SEATTLE CITY COUNCIL

Transportation and Utilities Committee

Agenda

Wednesday, March 3, 2021

9:30 AM

Public Hearing

Remote Meeting. Call 253-215-8782; Meeting ID: 586 416 9164; or Seattle Channel online.

Alex Pedersen, Chair
Dan Strauss, Vice-Chair
M. Lorena González, Member
Lisa Herbold, Member
Tammy J. Morales, Member
Debora Juarez, Alternate

Chair Info: 206-684-8804; Alex.Pedersen@seattle.gov

Watch Council Meetings Live **View Past Council Meetings**

Council Chamber Listen Line: 206-684-8566

For accessibility information and for accommodation requests, please call 206-684-8888 (TTY Relay 7-1-1), email CouncilAgenda@Seattle.gov, or visit http://seattle.gov/cityclerk/accommodations.

SEATTLE CITY COUNCIL

Transportation and Utilities Committee

Agenda

March 3, 2021 - 9:30 AM

Public Hearing

Meeting Location:
Remote Meeting. Call 253-215-8782; Meeting ID: 586 416 9164; or Seattle Channel online.

Committee Website:
http://www.seattle.gov/council/committees/transportation-and-utilities

---

This meeting also constitutes a meeting of the City Council, provided that the meeting shall be conducted as a committee meeting under the Council Rules and Procedures, and Council action shall be limited to committee business.

In-person attendance is currently prohibited per Washington State Governor's Proclamation 20-28.15, until the COVID-19 State of Emergency is terminated or Proclamation 20-28 is rescinded by the Governor or State legislature. Meeting participation is limited to access by telephone conference line and online by the Seattle Channel.

Register online to speak during the Public Comment period and the Public Hearing at the 9:30 a.m. Transportation and Utilities Committee meeting at http://www.seattle.gov/council/committees/public-comment.

Online registration to speak at the Transportation and Utilities Committee meeting will begin two hours before the 9:30 a.m. meeting start time, and registration will end at the conclusion of the Public Comment period and the Public Hearing during the meeting. Speakers must be registered in order to be recognized by the Chair.

Submit written comments to Councilmember Pedersen at Alex.Pedersen@seattle.gov.
Sign-up to provide Public Comment at the Meeting at http://www.seattle.gov/council/committees/public-comment
Watch live streaming video of the meeting at http://www.seattle.gov/council/watch-council-live
Listen to the meeting by calling the Council Chamber Listen Line at 253-215-8782 Meeting ID: 586 416 9164
One Tap Mobile No. US: +12532158782,,5864169164#

A. Call To Order

B. Approval of the Agenda

C. Public Comment

D. Items of Business

1. CB 120008 **AN ORDINANCE relating to the City Light Department; authorizing the General Manager and Chief Executive Officer to release a portion of an existing transmission corridor easement to the City of Kirkland; and accepting the payment of fair market value for the partial release of easement.**

Attachments: Att 1 – Partial Release of Easement

Supporting Documents: Summary and Fiscal Note
Summary Att 1 – Depiction of Easement Area to Be Released to City of Kirkland
Presentation

Public Hearing, Briefing, and Discussion

Presenters: Debra Smith, General Manager and CEO, Tom DeBoer, William Deveraux, Greg Sancewich, and Maura Brueger, Seattle City Light (SCL); Eric McConaghy, Council Central Staff

Register online to speak at the Public Hearing during the Transportation and Utilities Committee meeting at http://www.seattle.gov/council/committees/public-comment. Online registration will begin two hours before the 9:30 a.m. meeting start time, and registration will end at the conclusion of the Public Hearing during the meeting. Speakers must be registered in order to be recognized by the Chair. If you are unable to attend the remote meeting, please submit written comments to Councilmember Pedersen at Alex.Pedersen@seattle.gov.

2. Res 31988 **A RESOLUTION granting conceptual approval to construct, maintain, and operate a private parking area on East Howe Street, east of Fairview Avenue East; as proposed by BSOP 1, LLC, as part of developing a public plaza in unopened right-of-way in the Eastlake neighborhood.**

Supporting Documents:

Summary and Fiscal Note

Summary Att A - E Howe Steps Plaza Area Map

Central Staff Memo

Presentation

Briefing, Discussion, and Possible Vote

Presenters: Beverly Barnett and Amy Gray, Seattle Department of Transportation (SDOT); Juliet Vong, HBB Landscape Architecture; Detra Segar, East Howe Steering Committee; Ian Morrison, McCullough Hill Leary; Lish Whitson, Council Central Staff

3. CB 120009 **AN ORDINANCE relating to the City's 2021 Budget; amending Ordinance 126237, which adopted the 2021 Budget, including the 2021-2026 Capital Improvement Program (CIP); changing appropriations to the Seattle Department of Transportation in various budget control levels; and revising project allocations for certain projects in the 2021-2026 CIP; all by a 3/4 vote of the City Council.**

Attachments:
Att A - 23rd Avenue Corridor Improvements
Att B - BRT Concepts Design
Att C - Route 40 Transit-Plus Multimodal Corridor
Att D - Signal Major Maintenance
Att E - Transit Corridor Improvements

Supporting Documents:
Summary and Fiscal Note
Presentation
Central Staff Memo

Briefing, Discussion, and Possible Vote

Presenters: Candida Lorenzana and Domenico Martinucci, SDOT; Calvin Chow, Council Central Staff

4. CB 120002 **AN ORDINANCE relating to surveillance technology implementation; authorizing approval of uses and accepting surveillance impact reports for Seattle City Light's use of Current Diversion Technologies.**

Attachments:
Att 1 - Binoculars and Spotting Scope SIR
Att 2 - Check Meter Device SIR
Att 3 - SensorLink Amp Fork SIR
Att 4 - Current Diversion Technologies Executive Overview

Supporting Documents:
Summary and Fiscal Note
Central Staff Memo
Seattle IT Presentation
Central Staff Presentation

Briefing and Discussion

Presenters: Ginger Armbruster and Omari Stringer, Seattle Information Technology Department (Seattle IT); Michelle Vargo, SCL; Lise Kaye, Council Central Staff

5. CB 120003 **AN ORDINANCE relating to surveillance technology implementation; authorizing approval of uses and accepting the surveillance impact report for the Seattle Fire Department's use of Computer Aided Dispatch.**

Attachments: Att 1 - Computer-Aided Dispatch (CAD) SIR
Att 2 - Computer-Aided Dispatch (CAD) Executive Overview

Supporting Documents: Summary and Fiscal Note
Central Staff Memo
Seattle IT Presentation
Central Staff Presentation

Briefing and Discussion

Presenters: Ginger Armbruster and Omari Stringer, Seattle IT; Evan Ward, Seattle Fire Department; Lise Kaye, Council Central Staff

6. CB 120004 **AN ORDINANCE relating to surveillance technology implementation; authorizing approval of uses and accepting surveillance impact reports for the Seattle Police Department's use of surveillance technologies.**

Attachments:
Att 1 - 911 Logging Recorder SIR
Att 2 - Parking Enforcement Systems SIR
Att 3 - Automated License Plate Readers SIR
Att 4 - Computer-Aided Dispatch (CAD) SIR
Att 5 - CopLogic SIR
Att 6 - 911 Logging Recorder Executive Overview
Att 7 - Parking Enforcement Systems Executive Overview
Att 8 - Automated License Plate Readers Executive Overview
Att 9 - Computer-Aided Dispatch (CAD) Executive Overview
Att 10 - CopLogic Executive Overview

Supporting Documents:
Summary and Fiscal Note
Central Staff Memo
Seattle IT Presentation
Central Staff Presentation

Briefing and Discussion

Presenters: Ginger Armbruster and Omari Stringer, Seattle IT; Paul McDonagh, Seattle Police Department; Lise Kaye, Council Central Staff

E. Adjournment

File #: CB 120008, **Version:** 1

CITY OF SEATTLE

ORDINANCE _____

COUNCIL BILL _____

AN ORDINANCE relating to the City Light Department; authorizing the General Manager and Chief Executive Officer to release a portion of an existing transmission corridor easement to the City of Kirkland; and accepting the payment of fair market value for the partial release of easement.

WHEREAS, the City Light Department of The City of Seattle ("City Light") operates a public power system for The City of Seattle and surrounding communities, including a transmission corridor through the City of Kirkland ("Kirkland"); and

WHEREAS, City Light owns easement rights for an electric transmission corridor through a portion of Kirkland, which is a portion of City Light's larger electric transmission and distribution corridors; and

WHEREAS, City Light acquired an easement from William and Mary Ormsby on June 24, 1927, for the construction, operation, and maintenance of an electric transmission system consisting of three towers and the necessary wires, anchors, guys, and other appurtenances over, across, and through certain properties in what is now present-day Kirkland; and

WHEREAS, Kirkland owns the property located at 12307 NE Totem Lake Way, Kirkland, WA 98034, King County parcel number 866327-0060; and

WHEREAS, Kirkland operates and maintains the Cross Kirkland Corridor ("CKC") interim 5.75-mile crushed gravel trail that runs from the South Kirkland Park & Ride through the Totem Lake Business District; and

WHEREAS, Kirkland plans to construct the Totem Lake Connector ("TLC") bicycle and pedestrian bridge, which will connect the two ends of the 5.75-mile CKC currently severed by one of Kirkland's most

complicated intersections: Totem Lake Boulevard and Northeast 124th Street; and

WHEREAS, the TLC is one of a half-dozen public infrastructure projects that prepares Kirkland's only urban center for regional connectivity for community members and makes possible an alternative transportation corridor that will extend from Renton to Woodinville; and

WHEREAS, City Light's easement interests in the surface of the property are not necessary for continued operation and maintenance of the City Light facilities; and

WHEREAS, Kirkland wishes to purchase the necessary rights from City Light and City Light wishes to release the necessary rights to Kirkland while retaining the aerial easement interest, in perpetuity, for City Light transmission and distribution lines for operation, maintenance, and access to its electric transmission and distribution lines for the sum of $19,500, which represents the fair market value of the property to be released; NOW, THEREFORE,

BE IT ORDAINED BY THE CITY OF SEATTLE AS FOLLOWS:

Section 1. This real property transaction is exempt from the provisions of Seattle City Council Resolution 31424 regarding disposition of City Light surplus properties.

Section 2. Pursuant to the provisions of RCW 35.94.040 and after a public hearing, certain portions of the City Light easement are no longer needed for The City of Seattle's utility purposes and are declared surplus to City needs.

Section 3. The General Manager and Chief Executive Officer of the City Light Department, or the General Manager and Chief Executive Officer's designee, is authorized to enter into the necessary agreements with the City of Kirkland ("Kirkland") for the partial release of the easement in substantially the form as attached hereto as Attachment 1 to this ordinance.

Section 4. The General Manager and Chief Executive Officer of the City Light Department, or the General Manager and Chief Executive Officer's designee, is authorized to execute the Partial Release of Easement, which is in Attachment 1 to this ordinance, releasing certain portions of the City Light easement to

Kirkland and reserving the overhead easement rights for City Light's electric transmission and distribution lines, and to record the Partial Release of Easement with the King County Recorder.

Section 5. The General Manager and Chief Executive Officer of the City Light Department, or the General Manager and Chief Executive Officer's designee, is authorized to accept payment of $19,500 for the partial release of easement and deposit the payment into the City Light Fund.

Section 6. This ordinance shall take effect and be in force 30 days after its approval by the Mayor, but if not approved and returned by the Mayor within ten days after presentation, it shall take effect as provided by Seattle Municipal Code Section 1.04.020.

Passed by the City Council the _____ day of _____, 2021, and signed by me in open session in authentication of its passage this _____ day of _____, 2021.

_____

President _____ of the City Council

Approved / returned unsigned / vetoed

this _____ day of _____, 2021.

_____

Jenny A. Durkan, Mayor

Filed by me this _____ day of _____, 2021.

_____

Monica Martinez Simmons, City Clerk

(Seal)

Attachments:
Attachment 1 - Partial Release of Easement

Return to:
The City of Seattle
City Light Department
Real Estate Services SMT 3338
P.O. Box 34023
Seattle, WA 98124-4023

PARTIAL RELEASE OF EASEMENT

Reference Nos. (Released):	PM# 260528-3-103
Grantor:	The City of Seattle, acting by and through its City Light Department
Grantees:	The City of Kirkland, a Washington municipal corporation
Short Legal:	SW Quarter, Section 28, T-26N, R-5E.
Assessor's Tax Parcel No:	866327-0060

THIS PARTIAL RELEASE OF EASEMENTS AND AGREEMENT (this "Partial Release") is made and entered into by The City of Seattle, acting by and through its City Light Department ("Grantor"), for the benefit of the City of Kirkland ("Kirkland"), and all current and future owners of, and interest holders in, that certain parcel identified by King County Tax Parcel Numbers 866327-0060 located at 12307 NE Totem Lake Way, Kirkland, Washington (the "Property") and legally described in **Exhibit A** attached hereto and incorporated herein by this reference, with respect to the following facts:

WHEREAS, Grantor is the current beneficiary of that certain Easement dated as of June 24, 1927, (the "Easement") located on the Property; and

WHEREAS, Grantor has agreed to release certain rights arising pursuant to the Easement located across the Property, as more particularly described below.

NOW, THEREFORE, GRANTOR DOES HEREBY RELEASE the following rights acquired by way of the Easement within that portion of the Property legally described in **Exhibits B** attached hereto and depicted and labeled the "Release Area" on the diagram attached hereto as **Exhibit C,** which Exhibits are incorporated herein by this reference:

All surface rights to construct a tower(s).

The foregoing release shall not otherwise impair the rights of the Grantor acquired under the above described Easements, which rights, including but not limited to, all rights necessary to maintain safe and reliable electric transmission and all aerial rights, remain in full force and effect.

Grantor warrants to Grantees that (i) the Easement constitutes all of the easements and other rights in favor of Grantor within the Release Area legally described in **Exhibits B** and depicted in **Exhibit C;** (ii) Grantor is the current beneficiary of the Easement; and (iii) all necessary actions have been duly taken to permit Grantor to enter into this Partial Release. If any other electric transmission easements affecting the Release Area are found to exist, Grantor covenants and agrees to execute such additional releases and other instruments necessary in order to release and extinguish any other easement(s), right(s)-of-way, and/or other rights, consistent with this Partial Release and all exhibits attached hereto, in favor of Grantor within the Release Area.

[*exhibits on the following pages*]

Dated this ___ day of _____, 2021

SEATTLE CITY LIGHT
REAL ESTATE SERVICES

By: _____
Printed Name: _____
Manager, Real Estate Services

STATE OF WASHINGTON)
) ss.
COUNTY OF KING)

On this ___ day of _____, 2021, before me personally appeared _____ to me known to be the Manager of Real Estate at Seattle City Light, a department of the City of Seattle, the Washington municipal corporation that executed the within and foregoing instrument, and acknowledged that said instrument was the free and voluntary act and deed of said municipal corporation for the uses and purposes therein mentioned, and on oath stated that she/he was authorized to execute said instrument on behalf of the City of Seattle.

IN WITNESS WHEREOF, I have hereunto set my hand and affixed my official seal the day and year above written.

(notary seal)

Signature: _____

Print name: _____
Notary Public in and for the State of Washington
Residing at: _____
My commission expires: _____

CITY OF KIRKLAND

By: _____
Printed Name: _____
Its: _____

STATE OF WASHINGTON)
) ss.
COUNTY OF KING)

On this ___ day of _____, 2021, before me personally appeared _____ to me known to be the _____ for the City of Kirkland, the Washington municipal corporation that executed the within and foregoing instrument, and acknowledged that said instrument was the free and voluntary act and deed of said municipal corporation for the uses and purposes therein mentioned, and on oath stated that she/he was authorized to execute said instrument on behalf of the City of Kirkland.

IN WITNESS WHEREOF, I have hereunto set my hand and affixed my official seal the day and year above written.

(notary seal)

Signature: _____

Print name: _____
Notary Public in and for the State of Washington
Residing at: _____
My commission expires: _____

SUMMARY and FISCAL NOTE*

Department:	Dept. Contact/Phone:	CBO Contact/Phone:
Seattle City Light	Tom DeBoer/684-4185	Greg Shiring/386-4085

** Note that the Summary and Fiscal Note describes the version of the bill or resolution as introduced; final legislation including amendments may not be fully described.*

1. BILL SUMMARY

Legislation Title:
AN ORDINANCE relating to the City Light Department; authorizing the General Manager and Chief Executive Officer to release a portion of an existing transmission corridor easement to the City of Kirkland; and accepting the payment of fair market value for the partial release of easement.

Summary and background of the Legislation:
City Light owns an electrical transmission corridor through the City of Kirkland (Kirkland). A portion of the corridor utilizes easement rights to cross through property owned by Kirkland located at 12307 NE Totem Lake Way, Kirkland, WA 98034. Kirkland will use the area to build a bicycle and pedestrian bridge, referred to as the Totem Lake Connector, which will connect the Cross Kirkland Corridor and make possible an alternative transportation corridor that will extend from Renton to Woodinville.

The partial release of easement will ensure compatibility for long-term operations by City Light and the City of Kirkland. Kirkland will pay City Light the fair market value for the partial release of easement, which is $19,500.

Surface rights associated with the easement for City Light are not necessary for the continuing operation and maintenance of City Light electric transmission and distribution lines and City Light will retain all aerial easement rights above, over, across, and through the property to allow City Light to continue to construct, operate, and maintain its electric transmission and distribution lines in perpetuity.

2. CAPITAL IMPROVEMENT PROGRAM

Does this legislation create, fund, or amend a CIP Project? ___ **Yes** _X_ **No**

3. SUMMARY OF FINANCIAL IMPLICATIONS

Does this legislation amend the Adopted Budget? ___ **Yes** _X_ **No**

Does the legislation have other financial impacts to The City of Seattle that are not reflected in the above, including direct or indirect, short-term or long-term costs?
No.

Is there financial cost or other impacts of *not* implementing the legislation?
Loss of $19,500 in proceeds.

4. OTHER IMPLICATIONS

a. Does this legislation affect any departments besides the originating department?
No.

b. Is a public hearing required for this legislation?
Yes. A public hearing is required pursuant to RCW 35.94.040.

c. Is publication of notice with *The Daily Journal of Commerce* and/or *The Seattle Times* required for this legislation?
No.

d. Does this legislation affect a piece of property?
Yes. The easements are mapped in Seattle City Light's Real Property Geographic Information System (GIS).

e. Please describe any perceived implication for the principles of the Race and Social Justice Initiative. Does this legislation impact vulnerable or historically disadvantaged communities? What is the Language Access plan for any communications to the public?
There are no perceived impacts. No. Not applicable.

f. Climate Change Implications

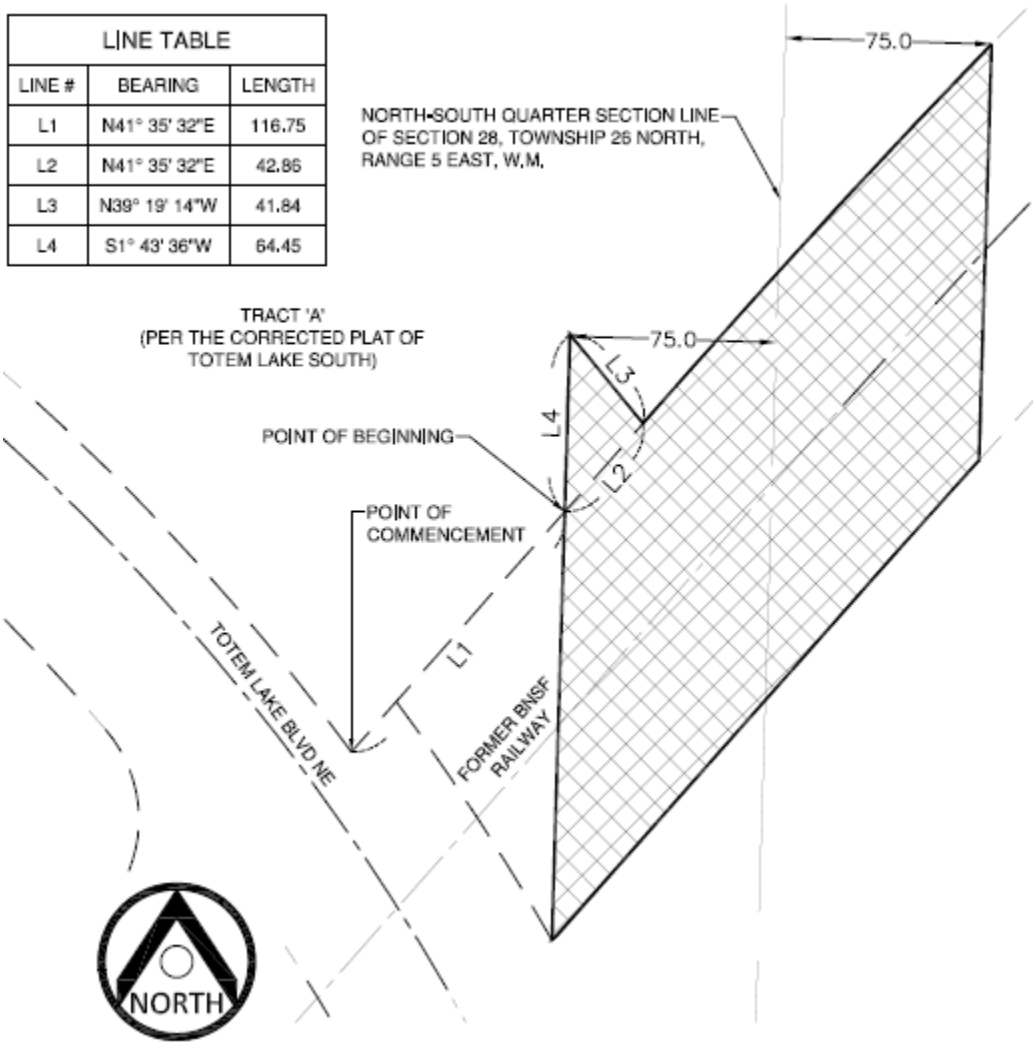
1. **Emissions: Is this legislation likely to increase or decrease carbon emissions in a material way?**
   Yes, the proposed connector bridge will make possible an alternative transportation corridor that will extend from Renton to Woodinville.

2. **Resiliency: Will the action(s) proposed by this legislation increase or decrease Seattle's resiliency (or ability to adapt) to climate change in a material way? If so, explain. If it is likely to decrease resiliency in a material way, describe what will or could be done to mitigate the effects.**
   This action will increase resiliency to climate change in the region with the alternative transportation corridor.

g. If this legislation includes a new initiative or a major programmatic expansion: What are the specific long-term and measurable goal(s) of the program? How will this legislation help achieve the program's desired goal(s).
Not applicable.

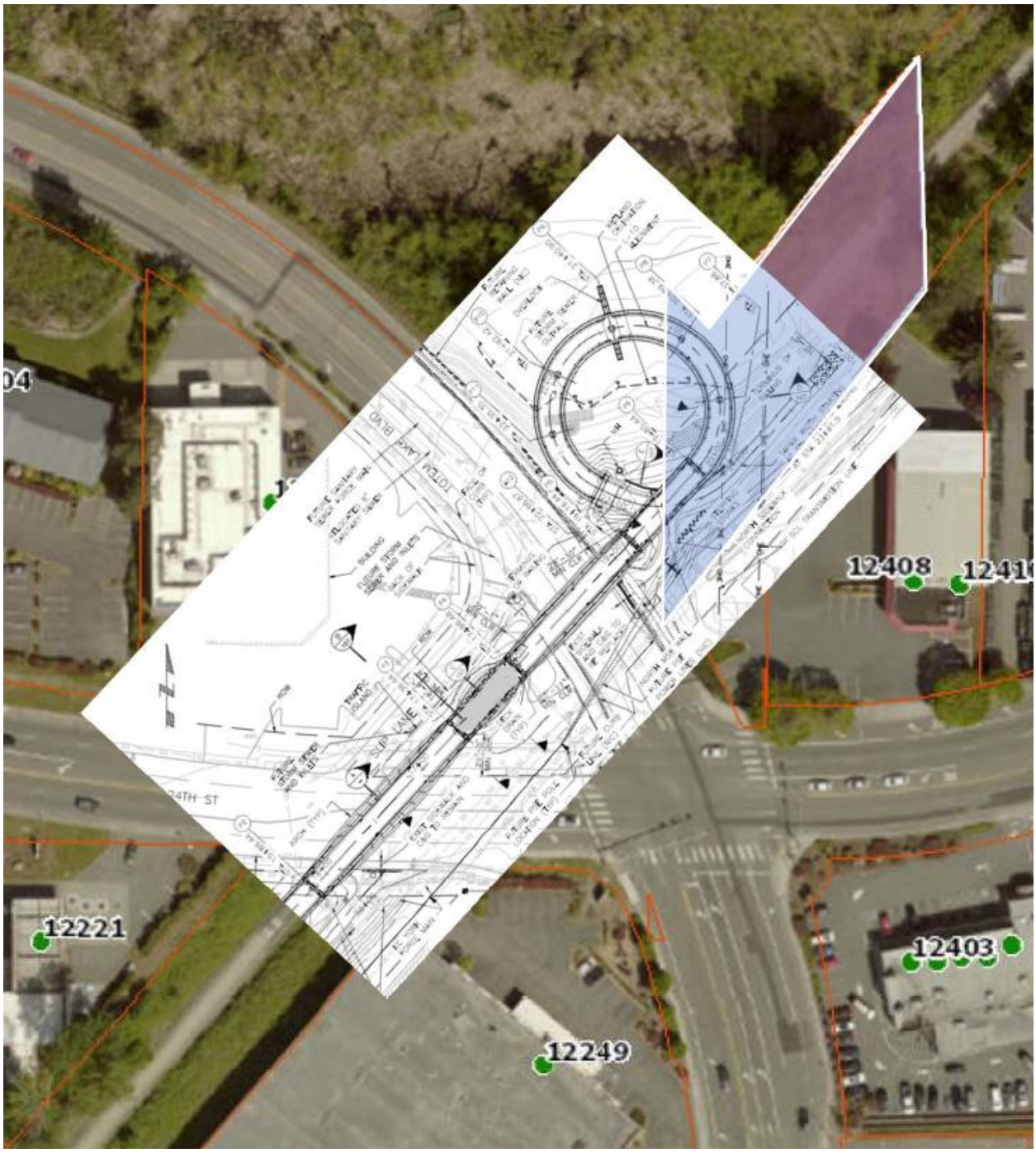
List attachments/exhibits below:
Summary Attachment 1 – Depiction of Easement Area to Be Released to City of Kirkland

Depiction of Easement Area to Be Released to City of Kirkland



Map is intended for illustrative or informational purposes only and is not intended to modify anything in the legislation.

Aerial Overlay of Site plan with Easement Area to Be Released to City of Kirkland



Map is intended for illustrative or informational purposes only and is not intended to modify anything in the legislation.

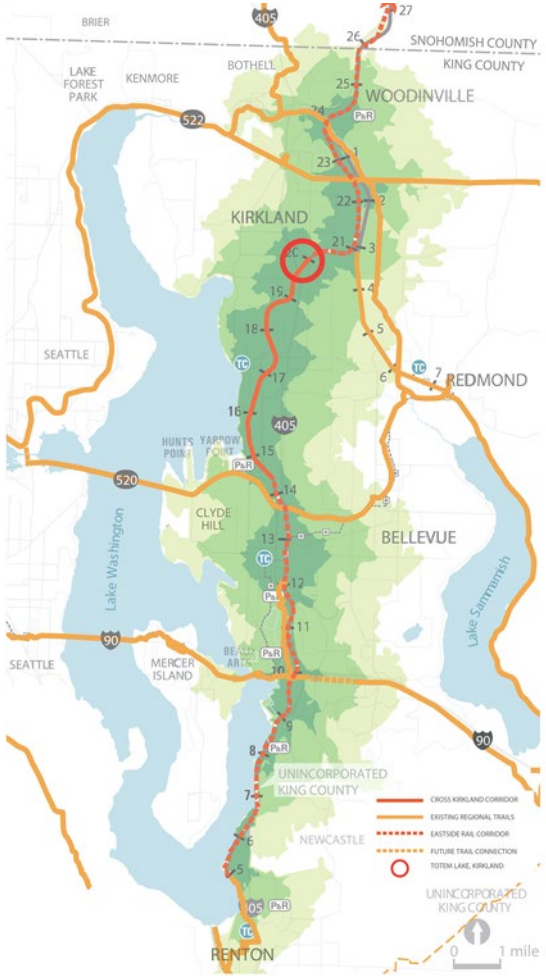
Kirkland Partial Release Ordinance

Partial Release of Easement to City of Kirkland

Seattle City Light

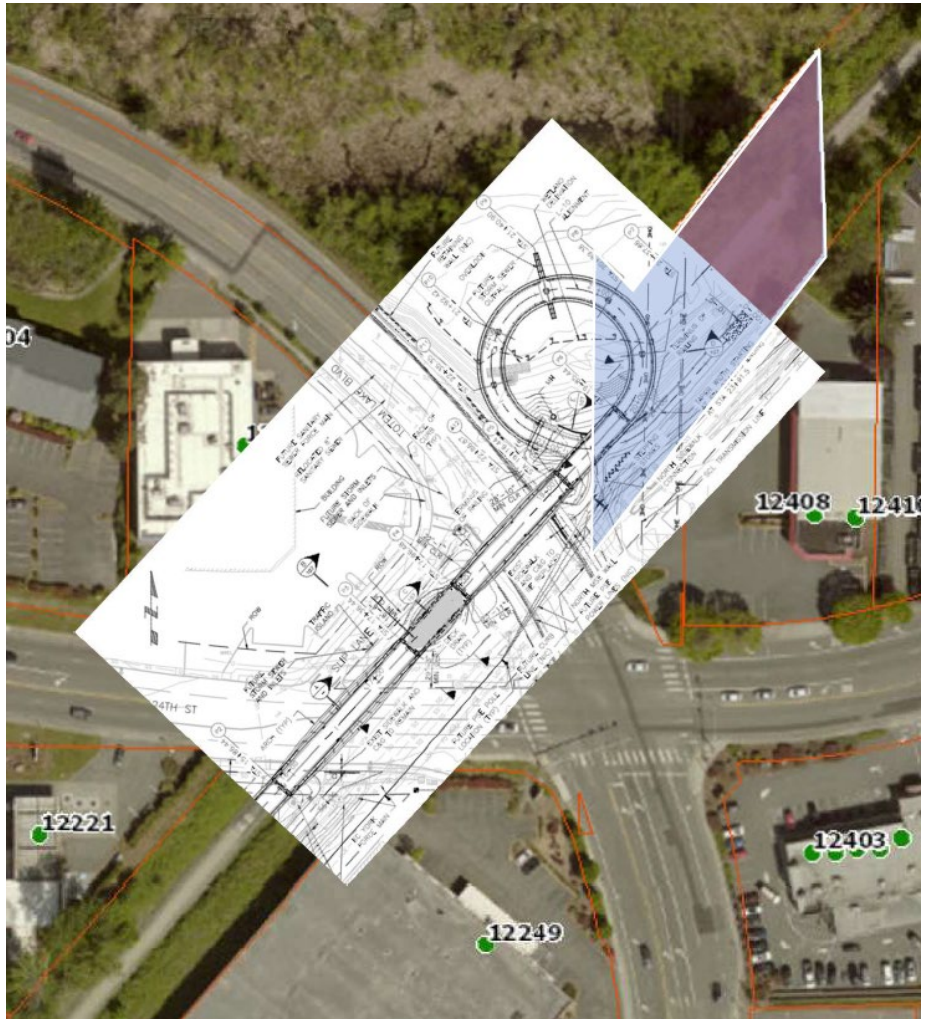
WE POWER SEATTLE

Cross Kirkland Corridor and Totem Lake Connector



Area to be Released

- Partial release of a portion of an existing transmission easement to the City of Kirkland
- Approximately 24,115 square feet
- City of Kirkland makes a one-time payment of $19,500 for the fair market value of the partial release
- Preserves City Light's rights necessary for safe and reliable transmission of electricity



Cross Kirkland Corridor and Totem Lake Connector

- Allows a grade-separated crossing for safe non-vehicular passage of NE 124th Street and Totem Lake Boulevard
- Part of the larger Eastside Rail Corridor
- Increases the functionality and connection of the regional trail system

POWER SEATTLE
Seattle City Light

File #: Res 31988, **Version:** 1

CITY OF SEATTLE

RESOLUTION _____

A RESOLUTION granting conceptual approval to construct, maintain, and operate a private parking area on East Howe Street, east of Fairview Avenue East; as proposed by BSOP 1, LLC, as part of developing a public plaza in unopened right-of-way in the Eastlake neighborhood.

WHEREAS, the East Howe Steps Plaza Steering Committee ("Steering Committee") secured City of Seattle funding to develop a design of a public plaza in an unopened portion of East Howe Street plaza, east of Fairview Avenue East, including a paved area for public plaza parking; and

WHEREAS, the Department of Neighborhoods led a community engagement process on the public plaza's design, and the design accommodates daytime restricted parking for the adjacent property owner; and

WHEREAS, the Steering Committee and BSOP 1, LLC, the adjacent property owner, entered into a Memorandum of Understanding agreeing that BSOP 1 LLC will contribute $500,000 for the construction of the public plaza, as supported by the Seattle Department of Neighborhoods, and BSOP 1, LLC will provide ongoing maintenance of the public plaza; and

WHEREAS, BSOP 1, LLC applied for permission to construct a private parking area for 16 vehicles in the unopened right-of-way in East Howe Street, east of Fairview Avenue East ("Private Parking Area"); and

WHEREAS, in making a recommendation, the Director of the Seattle Department of Transportation ("Director") considered the plans and application materials submitted by BSOP 1, LLC to construct the Private Parking Area and recommends that conceptual approval be granted; NOW, THEREFORE,

BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF SEATTLE, THE MAYOR CONCURRING, THAT:

Section 1. The City Council finds that the Private Parking Area across East Howe Street, east of

Fairview Avenue East, as proposed by BSOP 1, LLC and the funding for constructing the public plaza and the ongoing maintenance of a public plaza are in accordance with and in the public interest.

Section 2. As conditions for obtaining permission to construct the Private Parking Area in East Howe Street, east of Fairview Avenue East, and consistent with the Memorandum of Understanding, BSOP 1, LLC shall:

(1) Provide engineering and utility plans for additional review and permitting by the Seattle Department of Transportation (SDOT), which the Director will circulate to other City departments and any public and private utilities affected by the installation of the Private Parking Area;

(2) Continue to work with the Steering Committee to address the comments from the Seattle Design Commission and other City departments on the design and implementation of the public plaza, including signage for the Private Parking Area that is consistent with city policies on restricted parking areas;

(3) Provide a surety bond, covenant agreement, and public liability insurance naming the City as an additional insured or self-insurance, as approved by the City's Risk Manager;

(4) Pay all City permit fees;

(5) Obtain all necessary permits;

(6) Contribute $500,000 for the construction of the public plaza and provide ongoing maintenance of the public plaza for the duration of the Private Parking Area term permit and any subsequent Private Parking Area term permits;

(7) Maintain and inspect the Private Parking Area; and

(8) Remove the Private Parking Area and restore the right-of-way to in as good condition for public use as existed before constructing the Private Parking Area and in at least as good condition in all respects as the abutting portions of the public place as required by SDOT right-of-way restoration standards upon expiration of the term permit, or at the direction of the Director or City Council in accordance with the provisions of the term permit ordinance.

Section 3. After this resolution is adopted, SDOT will present to the Council a draft term permit ordinance identifying the conditions under which permission may be granted for the use of the right-of-way for the Private Parking Area. Permission to use the right-of-way is subject to the Council's decision to approve, deny, or modify the draft term permit ordinance presented by the Director.

Section 4. As recommended by the Director and the Mayor, conceptual approval for construction of the Private Parking Area on East Howe Street, east of Fairview Avenue East, is GRANTED.

Adopted by the City Council the _____ day of _____, 2021, and signed by me in open session in authentication of its adoption this _____ day of _____, 2021.

_____

President _____ of the City Council

The Mayor concurred the _____ day of _____, 2021.

_____

Jenny A. Durkan, Mayor

Filed by me this _____ day of _____, 2021.

_____

Monica Martinez Simmons, City Clerk

(Seal)

SUMMARY and FISCAL NOTE*

Department:	Dept. Contact/Phone:	CBO Contact/Phone:
Seattle Department of Transportation	Amy Gray/206-386-4638	Christie Parker/206-684-5211

1. BILL SUMMARY

Legislation Title: A RESOLUTION granting conceptual approval to construct, maintain, and operate a private parking area on East Howe Street, east of Fairview Avenue East; as proposed by BSOP 1, LLC, as part of developing a public plaza in unopened right-of-way in the Eastlake neighborhood.

Summary and background of the Legislation: The legislation would provide conceptual approval to BSOP 1, LLC to construct and maintain 16 private parking spaces in unopened right-of-way. In exchange, BSOP 1, LLC would contribute $500,000 to construct a public plaza in unopened right-of-way in the Eastlake neighborhood and be responsible for the plaza's on-going maintenance. The East Howe Steps Plaza Steering Committee has received $100,000 from the Department of Neighborhoods Neighborhood Matching Fund for designing and permitting the public plaza.

2. CAPITAL IMPROVEMENT PROGRAM

Does this legislation create, fund, or amend a CIP Project? ___ Yes _X_ No

3. SUMMARY OF FINANCIAL IMPLICATIONS

Does this legislation amend the Adopted Budget? ___ Yes _X_ No

Does the legislation have other financial impacts to The City of Seattle that are not reflected in the above, including direct or indirect, short-term or long-term costs?
No.

Is there financial cost or other impacts of *not* implementing the legislation?
If the resolution is not adopted, the East Howe Steps Plaza Steering Committee will not receive $500,000 from BSOP 1, LLC for constructing and maintaining the public plaza. The East Howe Steps Plaza Steering Committee would not be able to use the $100,000 grant from the Department of Neighborhoods for designing and permitting the public plaza.

Additionally, if the resolution is not adopted, the City would not receive an annual fee as a condition of the term permit ordinance.

4. OTHER IMPLICATIONS

a. Does this legislation affect any departments besides the originating department?
Yes, the Department of Neighborhoods has awarded the East Howe Steps Plaza Steering Committee a grant of $100,000 for designing and permitting the public plaza.

b. Is a public hearing required for this legislation?
No.

c. Is publication of notice with *The Daily Journal of Commerce* and/or *The Seattle Times* required for this legislation?
No.

d. Does this legislation affect a piece of property?
No.

e. Please describe any perceived implication for the principles of the Race and Social Justice Initiative. Does this legislation impact vulnerable or historically disadvantaged communities? What is the Language Access plan for any communications to the public?
There are no perceived implications on the principles of the Race and Social Justice Initiative. The $500,000 private contribution to the East Howe Steps construction will create additional public space in the Eastlake neighborhood.

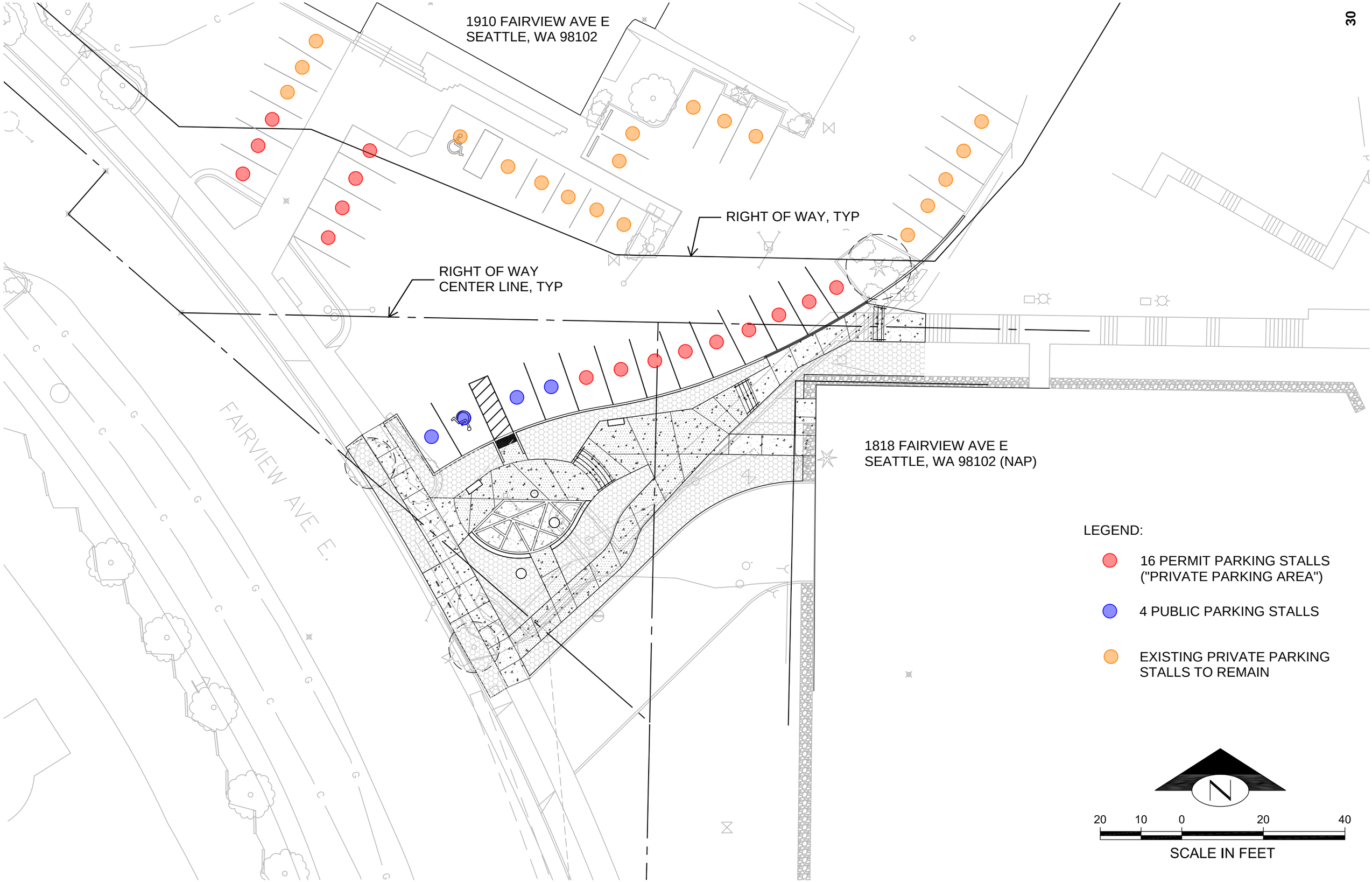
f. Climate Change Implications

1. **Emissions: Is this legislation likely to increase or decrease carbon emissions in a material way?**
   No.

2. **Resiliency: Will the action(s) proposed by this legislation increase or decrease Seattle's resiliency (or ability to adapt) to climate change in a material way? If so, explain. If it is likely to decrease resiliency in a material way, describe what will or could be done to mitigate the effects.**
   No.

g. If this legislation includes a new initiative or a major programmatic expansion: What are the specific long-term and measurable goal(s) of the program? How will this legislation help achieve the program's desired goal(s)?
N/A

List attachments/exhibits below:
Summary Attachment A - E Howe Steps Plaza Area Map


1910 FAIRVIEW AVE E
SEATTLE, WA 98102
RIGHT OF WAY, TYP
RIGHT OF WAY
CENTER LINE, TYP
FAIRVIEW AVE E.
1818 FAIRVIEW AVE E
SEATTLE, WA 98102 (NAP)
LEGEND:
16 PERMIT PARKING STALLS
("PRIVATE PARKING AREA")
4 PUBLIC PARKING STALLS
EXISTING PRIVATE PARKING
STALLS TO REMAIN
N
20 10 0 20 40
SCALE IN FEET

SEATTLE CITY COUNCIL
CENTRAL STAFF

February 24, 2021

MEMORANDUM

To: Transportation and Utilities Committee
From: Lish Whitson, Analyst
Subject: Resolution 31988: East Howe Street Parking Conceptual Approval

On Wednesday, March 3, 2021 the Transportation and Utilities Committee will consider Resolution 31988. This Resolution would grant conceptual approval for a new "significant structure" term permit to BSOP 1 LLC, allowing them to take steps to place private parking spaces on an unopened street right-of-way in the Eastlake neighborhood, Council District 4. As a condition of the resolution, BSOP will contribute toward the construction and long-term maintenance of a public plaza within the right-of-way adjacent to the parking.

Because these proposed parking spaces would occupy part of the city street, approval must be granted by the City Council pursuant to Seattle Municipal Code (SMC) Chapter 15.65 – Significant Structure Term Permits. Conditional conceptual approval of the term permit is the first step in approving the use of the street for private parking. Resolution 31988 would grant conceptual approval to BSOP for the construction of the parking and would direct the Seattle Department of Transportation (SDOT) to negotiate final approval of a term permit.

This memorandum summarizes the term permit approval process and describes the conditions of approval under Resolution 31988.

Significant Structure Term Permits

Significant structures are structures that have "a long-anticipated duration of encroachment, impede the City's or public's flexibility in the use of the public place, or are necessary for the functioning of other property of the permittee." Examples include tunnels below streets that provide utility, pedestrian, or vehicular access between private properties; public art placed in right-of-way; and overhead structures attached to buildings. SMC Chapter 15.65 establishes the procedures and criteria for approval of term permits for significant structures.

SMC 15.65.040.C identifies ten issues that are considered when reviewing whether to approve a significant structure:

1. Adequacy of horizontal, vertical, and other clearances.
2. View blockage and impacts due to reduction of natural light.
3. Construction permit review is at 60% conceptual approval.
4. Interruption or interference with existing streetscape or another street amenities.
5. Effect on pedestrian activity;

6. Effect on commerce and enjoyment of neighboring land uses;
7. Availability of reasonable alternatives;
8. Effect on traffic and pedestrian safety;
9. Accessibility for the elderly and handicapped; and
10. The public benefit mitigation elements provided by the proposal, to the extent required based on the nature of the structure.

Once the SDOT Director reviews a term permit petition, the director transmits a recommendation to the City Council for conceptual approval. The Council's review of the proposal considers the ten items noted above in order to determine whether the structure is in the public interest and no reasonable alternative to the structure exists. The Council may provide conceptual approval, conditional conceptual approval or deny the term permit through a resolution.

If SDOT determines that the construction plans are consistent with the Council's approval or conditional approval, SDOT forwards a bill to the City Council for its final decision to grant or deny the application for a proposed new structure permit. Generally, the City grants approval for a ten-year term, renewable two times for a total term of thirty years but the Council may approve a different term.

E Howe Street Private Parking

BSOP 1, LLC, the owners of an office building at 1910 Fairview Avenue E, propose to construct 16 private parking spaces and four public spaces in the E Howe Street right-of-way, east of Fairview Avenue. The private parking spaces would be used by the tenants of 1910 Fairview during the day and would be available to the public in the evening and weekends. In exchange for use of the right-of-way for parking, BSOP 1, LLC would contribute to the development and maintenance of a public plaza adjacent to the parking. The plaza is being designed and will be developed in coordination with the East Howe Street Plaza Steering Committee, a neighborhood organization.

E Howe Street between Fairview and Eastlake avenues is not developed for street purposes. Adjacent to Eastlake, the right-of-way has been developed with a pedestrian plaza in exchange for a subterranean street vacation. In the middle of the block, a set of stairs connects the Eastlake street grade with the Fairview street grade, 20 feet below Eastlake. A public plaza is proposed to be built connecting the bottom of the stairway to Fairview. The plaza would include a sloped walkway, small overlook, retaining wall, seat wall, railings and planted areas. A diagram showing the proposed locations of the parking spaces and plaza is attached to the fiscal note for Resolution 31988.

East of Eastlake, E Howe Street passes through the I-5 Colonnade Park and connects Eastlake to Capitol Hill. The proposed plaza would complete connections from Fairview Ave E to 15th Avenue E, at the north end of Lake View Cemetery.

Resolution 31988 would grant conditional conceptual approval for a term permit to BSOP for private parking in the E Howe Street right-of-way. BSOP would need to meet the following conditions outlined in the resolution before SDOT recommends approval and BSOP receives a term permit:

1. Provide engineering and utility plans for additional review and permitting by the Seattle Department of Transportation (SDOT), which the Director will circulate to other City departments and any public and private utilities affected by the installation of the Private Parking Area;
2. Continue to work with the [East Howe Street Plaza] Steering Committee to address the comments from the Seattle Design Commission and other City departments on the design and implementation of the public plaza, including signage for the Private Parking Area that is consistent with city policies on restricted parking areas;
3. Provide a surety bond, covenant agreement, and public liability insurance naming the City as an additional insured or self-insurance, as approved by the City's Risk Manager;
4. Pay all City permit fees;
5. Obtain all necessary permits;
6. Contribute $500,000 for the construction of the public plaza and provide ongoing maintenance of the public plaza for the duration of the Private Parking Area term permit and any subsequent Private Parking Area term permits;
7. Maintain and inspect the Private Parking Area; and
8. Remove the Private Parking Area and restore the right-of-way to in as good condition for public use as existed before constructing the Private Parking Area and in at least as good condition in all respects as the abutting portions of the public place as required by SDOT right-of-way restoration standards upon expiration of the term permit, or at the direction of the Director or City Council in accordance with the provisions of the term permit ordinance.

The resolution directs SDOT to draft a term permit bill that reflects these conditions for Council consideration. If Council approves the bill, BSOP would have the right to build and use the private parking spaces.

Next Steps

If the Committee recommends adoption of the resolution at its meeting on March 3, final adoption could occur as early as the City Council meeting on March 7. Once the resolution is

adopted and BSOP meets the conditions listed above, SDOT would begin to draft a bill to approve the term permit.

cc: Dan Eder, Interim Director
Aly Pennucci, Supervising Analyst

BSOP 1, LLC Term Permit

Council Transportation and Utilities Committee

Presentation overview

East Howe Steps Plaza Steering Committee (Steering Committee) and BSOP 1, LLC entered into a Memorandum of Understanding for the development of the E Howe Steps Plaza

- **BSOP 1, LLC will contribute $500,000 towards the development and maintenance of the new public plaza**
- **BSOP 1, LLC is seeking a new permit for private weekday parking in East Howe Street, east of Fairview Avenue East to implement the MOU**
- **The Steering Committee supports the private weekday parking**

SDOT recommends approval of the term permit

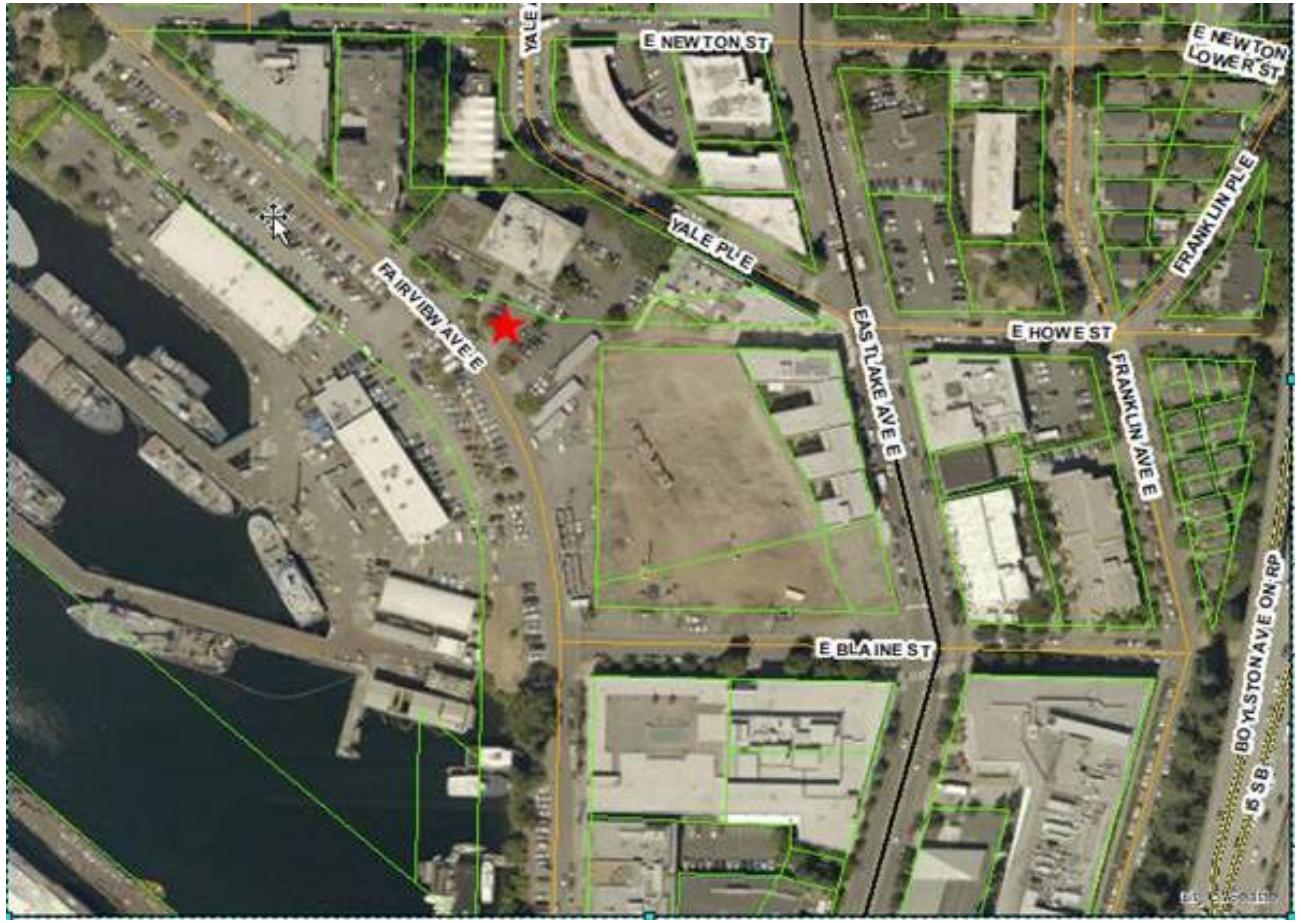
Property owner and community organization

- BSOP 1, LLC: property owner at 1910 Fairview Ave E, an existing office building with business parking located in the E Howe St right-of-way

- E Howe Steps Plaza Steering Committee: Eastlake community members who participated in the development of the MOU for the public improvements and the private parking area

Project area – Eastlake neighborhood

1910 Fairview Ave E



Term permit process

This term permit implements the agreement between the Steering Committee and BSOP 1, LLC for the development of the public plaza

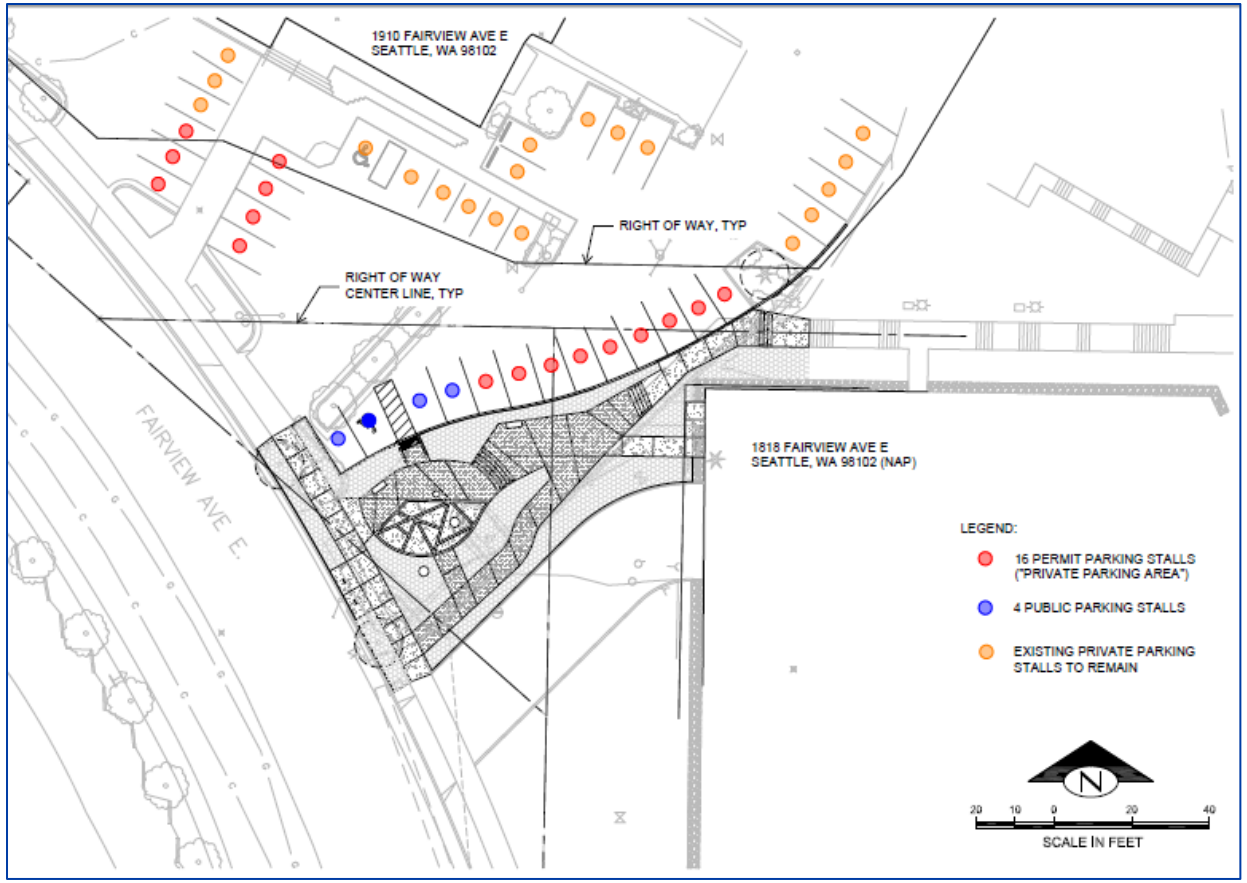
- Step 1: Resolution
  Adoption of the resolution provides conceptual approval for the private use in the right-of-way, subject to the terms and conditions to be established in the term permit ordinance.

- Step 2: Ordinance
  Passage of the ordinance details the terms and conditions of the permit, including annual fee, maintenance obligations, indemnification, insurance, and bond requirements.

Proposal

The Dept of Neighborhoods facilitated an MOU between the Steering Committee and BSOP 1, LLC

- The Steering Committee received a $100,000 Matching Fund grant from the Dept of Neighborhoods for designing and permitting the public plaza
- BSOP 1, LLC will contribute $500,000 to construct the public plaza in unopened right-of-way; BSOP 1 LLC will be responsible for the on-going maintenance of the plaza
- BSOP 1, LLC will accommodate up to 12 community events per year in the private weekday parking area
- The Steering Committee supports the private weekday parking term permit to support the agreement for the construction and on-going maintenance of the new plaza



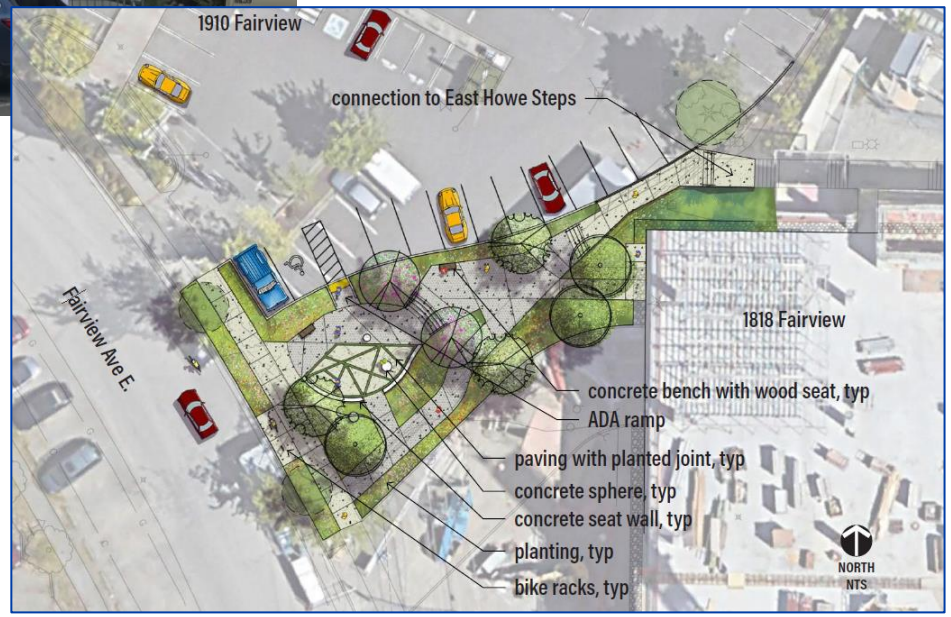
Proposal

Private weekday parking

- 16 signed private stalls
  - Available to the public on weekends and holidays
- 4 public parking stalls

Plaza:

- Landscaping and paver treatment
- Bike racks
- Protecting existing tree



Proposal

Existing conditions – E Howe ROW used as parking

Facing west

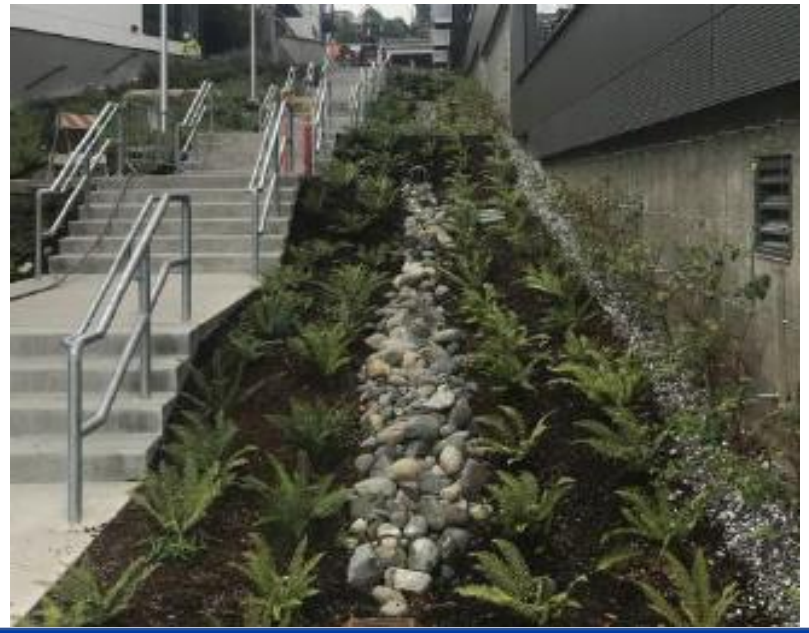
Facing east

Proposal

Existing Conditions – pedestrian stairs and sidewalk connecting Eastlake Ave E & Fairview Ave E, constructed as part of the development of the southern property

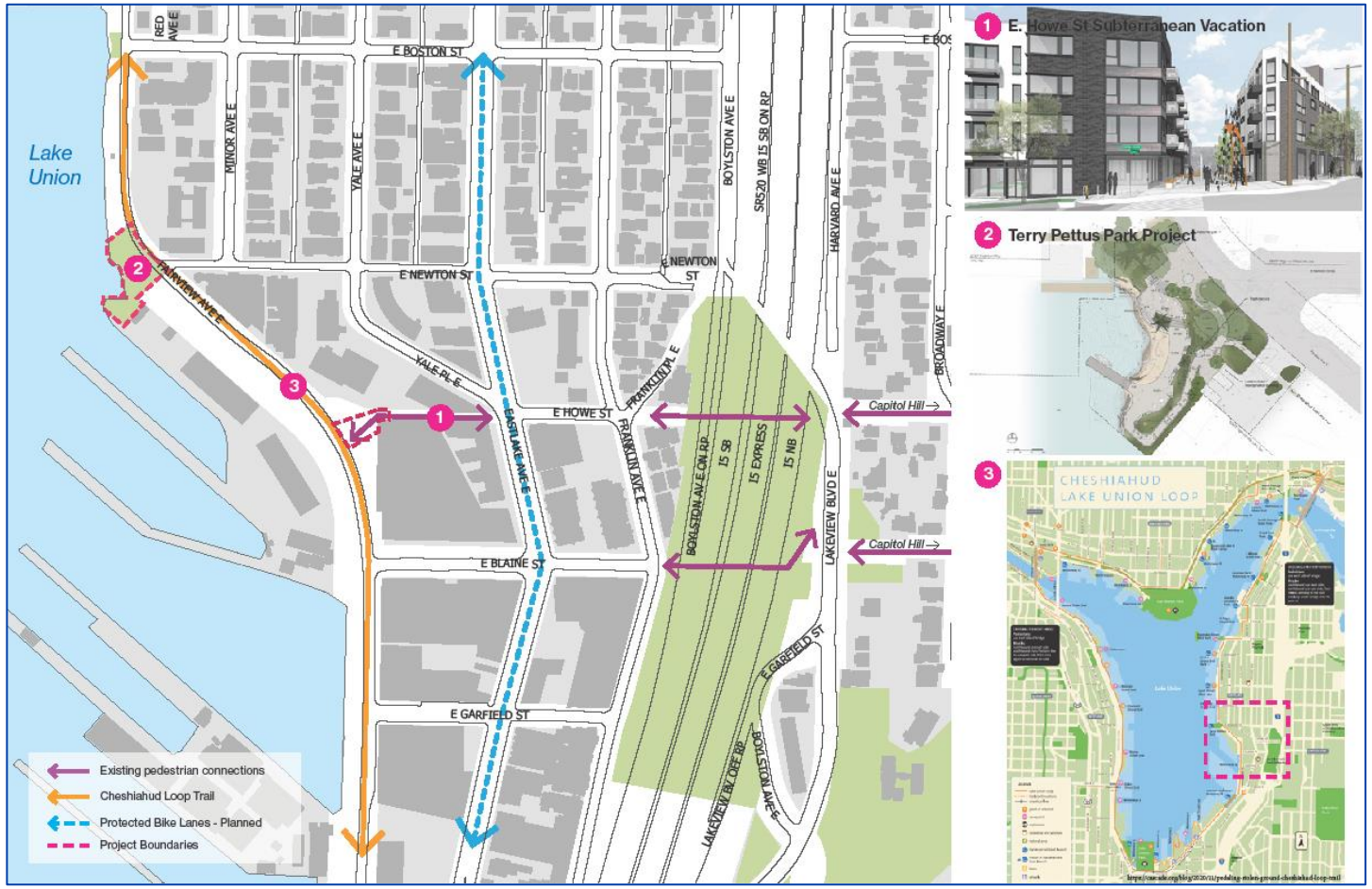
Facing west

Facing east



Facing east

Pedestrian connections



Requested action

- SDOT is seeking Council adoption of this resolution for conceptual approval for the private weekday parking by BSOP 1, LLC

- If the resolution is adopted, SDOT will prepare the term permit ordinance

- If the ordinance is approved, the permit will be in place for 15 years, with one renewable 15-year term

Questions?

amy.gray@seattle.gov | (206) 386-4638

www.seattle.gov/transportation

File #: CB 120009, **Version:** 1

CITY OF SEATTLE

ORDINANCE _____

COUNCIL BILL _____

AN ORDINANCE relating to the City's 2021 Budget; amending Ordinance 126237, which adopted the 2021 Budget, including the 2021-2026 Capital Improvement Program (CIP); changing appropriations to the Seattle Department of Transportation in various budget control levels; and revising project allocations for certain projects in the 2021-2026 CIP; all by a 3/4 vote of the City Council.

WHEREAS, the Seattle City Council formed a transportation benefit district in 2010 and imposed a $20 annual vehicle license fee that went into effect in 2011 for transportation purposes, which was increased to a total of $80 per year after Seattle voters approved a six-year measure called Proposition 1 in 2014; and

WHEREAS, in the 2019 general election, in spite of overwhelming rejection by Seattle voters, a majority of state voters approved Initiative 976, which, among multiple subjects, attempted to repeal statutory authority for local jurisdictions to impose vehicle license fees at an annual rate of up to $100; and

WHEREAS, after passage of I-976, the City joined King County and several other local transit agencies and jurisdictions from around the state in a filing a challenge in King County Superior Court against the constitutionality of I-976; and

WHEREAS, the Superior Court judge determined that Seattle and the other plaintiff jurisdictions had a reasonable likelihood of prevailing and being irreparably harmed if the initiative went into effect before its constitutionality could be determined and, therefore, issued an injunction preventing the initiative from going into effect; and

WHEREAS, the City held much of the Seattle Transportation Benefit District revenues in reserve pending the ultimate outcome of the constitutional challenge at the Washington State Supreme Court; and

WHEREAS, while the court case was being appealed to the Supreme Court, Seattle voters approved a new sales tax-based Proposition 1 for transit service to replace the 2014 measure that expired at the end of 2020; and

WHEREAS, on October 15, 2020 the Supreme Court held I-976 to be unconstitutional thereby freeing up $23 million in revenues that had been collected by the City and held in reserve; and

WHEREAS, after consulting with Seattle's Transit Advisory Board and Levy to Move Seattle Oversight Committee, the Seattle Department of Transportation (SDOT) has developed a detailed set of priority projects and service requiring minor amendments to budget provisions appropriating these funds; NOW, THEREFORE,

BE IT ORDAINED BY THE CITY OF SEATTLE AS FOLLOWS:

Section 1. In order to pay for necessary costs and expenses incurred or to be incurred in 2021, but for which insufficient appropriations were made due to causes that could not reasonably have been foreseen at the time of the making of the 2021 Budget, appropriations for the following items in the 2021 Budget are increased from the funds shown, as follows:

Item	**Department**	**Fund**	**Budget Summary Level/BCL Code**	**Amount**
1.1	Seattle Dept of Transportation	Seattle Transportation Benefit District (19900)	Mobility Operations (19000-BO-TR-17003)	$5,000,000
Total				**$5,000,000**

Section 2. Appropriations in the 2021 Budget and project allocations in the 2021-2026 Adopted Capital Improvement Program, which are backed by revenues, are modified as follows:

Item	**Department**	**Fund**	**Budget Summary Level/BCL Code**	**BCL Appropriation Change**	**CIP Project Name**	**2021 CIP Allocations**

2.1	Seattle Department of Transportation	Transportation Benefit District (19900)	Mobility Capital (19900-BC-TR-19003)	$4,350,000	Transit Corridor Improvements (BC-TR-19003)	((~~$1,928,000~~)) $6,278,000
2.2	Seattle Department of Transportation	Transportation Benefit District (19900)	Mobility Capital (19900-BC-TR-19003)	$300,000	Route 40 Transit-Plus Multimodal Corridor (MC-TR-C079)	((~~$833,000~~)) $1,133,000
2.3	Seattle Department of Transportation	Transportation Benefit District (19900)	Mobility Capital (19900-BC-TR-19003)	$400,000	BRT Concepts Design (MC-TR-C010)	((~~$239,000~~) $639,000
2.4	Seattle Department of Transportation	Transportation Benefit District (19900)	Major Maintenance/ Replacement (19900-BC-TR-19001)	$650,000	Signal Major Maintenance (MC-TR-C026)	((~~$1,436,000~~)) $2,086,000
2.5	Seattle Department of Transportation	Transportation Benefit District (19900)	Mobility Capital (19900-BC-TR-19003)	$4,300,000	23rd Avenue Corridor Improvements (MC-TR-C037)	((~~$0~~)) $4,300,000
Net Change				**$10,000,000**		

These modifications shall operate for the purposes of decreasing or increasing the basis for the limit imposed by subsection 4(c) of Ordinance 126237.

Section 3. The modifications to the 2021-2026 Adopted Capital Improvement Program for the above items are as reflected in Attachments A (Transit Corridor Improvements), B (Route 40 Transit-Plus Multimodal Corridor), C (BRT Concepts Design), D (Signal Major Maintenance) and E (23rd Avenue Corridor Improvements) to this ordinance.

Section 4. This ordinance shall take effect and be in force 30 days after its approval by the Mayor, but if not approved and returned by the Mayor within ten days after presentation, it shall take effect as provided by Seattle Municipal Code Section 1.04.020.

Passed by a 3/4 vote of all the members of the City Council the _____ day of _____, 2021, and signed by me in open session in authentication of its passage this _____ day of _____, 2021.

_____

President _____ of the City Council

Approved / returned unsigned / vetoed this _____ day of _____, 2021.

_____

Jenny A. Durkan, Mayor

Filed by me this _____ day of _____, 2021.

_____

Monica Martinez Simmons, City Clerk

(Seal)

Attachments:
Attachment A - 23rd Avenue Corridor Improvements
Attachment B - BRT Concepts Design
Attachment C - Route 40 Transit-Plus Multimodal Corridor

Attachment D - Signal Major Maintenance
Attachment E - Transit Corridor Improvements

23rd Avenue Corridor Improvements

Project No:	MC-TR-C037	**BSL Code:**	BC-TR-19003
Project Type:	Discrete	**BSL Name:**	Mobility-Capital
Project Category:	Improved Facility	**Location:**	23rd AVE S/E John ST/Rainier AVE S
Current Project Stage:	Stage 3 - Design	**Council District:**	Council District 3
Start/End Date:	2013 - 2022	**Neighborhood District:**	Central
Total Project Cost:	~~$58,096~~ $62,478	**Urban Village:**	23rd & Union-Jackson

This multi-phase project will reconstruct sidewalks, enhance the pedestrian environment, reconstruct pavement, upgrade signalized intersections, upgrade controller cabinets to meet transit signal priority (TSP) needs, and accommodate Intelligent Transportation Systems (ITS) upgrades. Activities include the following: install ITS to provide travel time information; install fiber communication as needed along the corridor to relay information back to the Traffic Management Center; and install poles for support of future trolley wires in two gap segments of the trolley network. The project will also include design and construction of a 3-lane cross section (with 4 lanes at isolated intersections) between John Street and Rainier Ave South, as well as a greenway facility on a parallel street to facilitate north-south bicycle travel. The project includes a Vision Zero element to construct new traffic signals; parking modifications; new curb ramps; traffic calming; speed reduction; pedestrian safety; and transit stop improvements. Phases I and II are substantially complete. The final Vision Zero phase is on hold and design is complete.

Resources	**LTD Actuals**	**2020 Revised**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**Total**
City Light Fund Revenues	3,062	9	-	-	-	-	-	-	3,071
Commercial Parking Tax	114	8	-	-	-	-	-	-	122
Federal Grant Funds	4,990	-	-	-	-	-	-	-	4,990
Interdepartmental Transfer	-	-	-	-	-	-	-	-	-
LTGO Bond Proceeds	14,517	27	-	-	-	-	-	-	14,544
Miscellaneous Grants or Donations	-	-	-	-	-	-	-	-	-
Private Funding/Donations	5	-	-	-	-	-	-	-	5
Real Estate Excise Tax II	4,806	159	-	-	-	-	-	-	4,964
State Grant Funds	10,734	276	-	-	-	-	-	-	11,010
Vehicle License Fees $60 & 0.1% Sales Tax	-	-	4,300	-	-	-	-	-	4,300
Transportation Funding Package - Lid Lift	11,730	-	-	-	-	-	-	-	11,730
Transportation Funding Package - Parking Tax	-	-	-	-	-	-	-	-	-
Transportation Move Seattle Levy - Lid Lift	7,099	633	-	-	-	-	-	-	7,731
Water Rates	10	-	-	-	-	-	-	-	10
Total:	**57,067**	**1,111**		**-**	**-**	**-**	**-**	**-**	~~58,178~~
Revised Total:	**57,067**	**1,111**	**4,300**	**-**	**-**	**-**	**-**	**-**	**62,478**

Fund Appropriations / Allocations[1]	**LTD Actuals**	**2020 Revised**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**Total**
2011 Multipurpose LTGO Bond Fund	5,622	-	-	-	-	-	-	-	5,622
2016 Multipurpose LTGO Bond Fund	7,920	25	-	-	-	-	-	-	7,945
2017 Multipurpose LTGO Bond Fund	975	2	-	-	-	-	-	-	977
Bridging The Gap Levy Fund	11,730	-	-	-	-	-	-	-	11,730
Move Seattle Levy Fund	6,895	633	-	-	-	-	-	-	7,527
REET II Capital Fund	4,806	159	-	-	-	-	-	-	4,964
Transportation Fund	19,120	293	-	-	-	-	-	-	19,412
Transportation Benefit District Fund	-	-	**4,300**	-	-	-	-	-	**4,300**
Total:	**57,067**	**1,111**		**-**	**-**	**-**	**-**	**-**	~~58,178~~
Revised Total:	**57,067**	**1,111**	**4,300**	**-**	**-**	**-**	**-**	**-**	**62,478**

[1]Funds are appropriated through the Adopted Budget at the Budget Summary Level. All Amounts shown above are in thousands of dollars

O&M Impacts: SDOT has individual project budgets for the maintenance of painted markings, signage, signals, bridges and roadway structures, urban forestry, and sidewalks and pavement; these budgets are constrained by the availability of transportation specific and general funds. The SDOT Asset Management website (https://www.seattle.gov/transportation/about-sdot/asset-management) provides unconstrained operational cost forecasting by asset type, typical lifecycle and average maintenance cost ranges.

[1]Funds are appropriated through the Adopted Budget at the Budget Summary Level. All Amounts shown above are in thousands of dollars

BRT Concepts Design

Project No:	MC-TR-C010	**BSL Code:**	BC-TR-19003
Project Type:	Discrete	**BSL Name:**	Mobility-Capital
Project Category:	Improved Facility	**Location:**	Citywide
Current Project Stage:	Stage 2 - Initiation, Project Definition, & Planning	**Council District:**	Multiple
Start/End Date:	2016 - 2021	**Neighborhood District:**	Multiple
Total Project Cost:	~~$2,091~~ **$2,441**	**Urban Village:**	Multiple

This project will advance the concept designs for Seattle's RapidRide and Transit-Plus Multimodal Corridor Expansion program. In order to deliver the corridor improvements, this work includes assessment and development of corridor design, detailed line and network ridership forecasting, capital cost estimates, traffic and environmental analysis, modal integration, and funding plans.

Resources	**LTD Actuals**	**2020 Revised**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**Total**
Transportation Move Seattle Levy - Lid Lift	1,451	350	239	-	-	-	-	-	2,041
Vehicle License Fees $60 & 0.1% Sales Tax	-	-	**400**	-	-	-	-	-	**400**
Total:	**1,451**	**350**	~~239~~	**-**	**-**	**-**	**-**	**-**	~~2,041~~
Revised Total:	**1,451**	**350**	**639**						**2,441**

Fund Appropriations / Allocations[1]	**LTD Actuals**	**2020 Revised**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**Total**
Move Seattle Levy Fund	1,451	350	239	-	-	-	-	-	2,041
Transportation Benefit District Fund	-	-	400	-	-	-	-	-	400
Total:	**1,451**	**350**	~~239~~	**-**	**-**	**-**	**-**	**-**	~~2,041~~
Revised Total:	**1,451**	**350**	**639**						**2,441**

O&M Impacts: Not applicable - does not create new assets.

[1]Funds are appropriated through the Adopted Budget at the Budget Summary Level. All Amounts shown above are in thousands of dollars

Route 40 Transit-Plus Multimodal Corridor

Project No:	MC-TR-C079	**BSL Code:**	BC-TR-19003
Project Type:	Discrete	**BSL Name:**	Mobility-Capital
Project Category:	Improved Facility	**Location:**	Various
Current Project Stage:	Stage 2 - Initiation, Project Definition, & Planning	**Council District:**	Multiple
Start/End Date:	2016 - 2024	**Neighborhood District:**	Multiple
Total Project Cost:	$21,132	**Urban Village:**	Multiple

This project will design and construct transit speed and reliability improvements and upgraded bus stop passenger facilities. Improvements to the route, which connects Downtown, South Lake Union, Fremont, Ballard, and Northgate, will support conversion to RapidRide service by partner agency King County Metro.

Resources	**LTD Actuals**	**2020 Revised**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**Total**
Federal Grant Funds	-	-	-	-	4,000	-	-	-	4,000
State Grant Funds	-	-	-	3,434	-	-	-	-	3,434
Transportation Move Seattle Levy - Lid Lift	390	755	833	1,999	3,675	80	-	-	7,732
Vehicle License Fees $60 & 0.1% Sales Tax	-	-	300	2,700	-	-	-	-	3,000
Total:	**390**	**755**	~~833~~	**~~5,433~~**	**7,675**	**80**	**-**	**-**	~~15,166~~
Revised Total:	**390**	**755**	**1,133**	**8,133**	**7,675**	**80**			**18,166**

Fund Appropriations / Allocations[1]	**LTD Actuals**	**2020 Revised**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**Total**
Move Seattle Levy Fund	390	755	833	1,999	3,675	80	-	-	7,732
Transportation Fund	-	-	-	3,434	4,000	-	-	-	7,434
Transportation Benefit District Fund	-	-	300	2,700	-	-	-	-	3,000
Total:	**390**	**755**	~~833~~	**~~5,433~~**	**7,675**	**80**	**-**	**-**	~~15,166~~
Revised Total:	**390**	**755**	**1,133**	**8,133**	**7,675**	**80**			**18,166**

Unsecured Funding:	**LTD Actuals**	**2020 Revised**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**Total**
To Be Determined	-	-	-	-	-	~~5,966~~ 2,966	-	-	~~5,966~~ 2,966
Total:	**-**	**-**	**-**	**-**	**-**	**~~5,966~~** **2,966**	**-**	**-**	**~~5,966~~** **2,966**

Unsecured Funding Strategy: SDOT plans to compete for FTA and WSDOT grants, as well as work with regional partners to secure funding.

O&M Impacts: SDOT has individual project budgets for the maintenance of painted markings, signage, signals, bridges and roadway structures, urban forestry, and sidewalks and pavement; these budgets are constrained by the availability of transportation specific and general funds. The SDOT Asset Management website (https://www.seattle.gov/transportation/about-sdot/asset-management) provides unconstrained operational cost forecasting by asset type, typical lifecycle and average maintenance cost ranges.

[1]Funds are appropriated through the Adopted Budget at the Budget Summary Level. All Amounts shown above are in thousands of dollars

Signal Major Maintenance

Project No:	MC-TR-C026	**BSL Code:**	BC-TR-19001
Project Type:	Ongoing	**BSL Name:**	Major Maintenance/Replacement
Project Category:	Rehabilitation or Restoration	**Location:**	Citywide
Current Project Stage:	N/A	**Council District:**	Multiple
Start/End Date:	N/A	**Neighborhood District:**	Multiple
Total Project Cost:	N/A	**Urban Village:**	Multiple

This project addresses major work related to the basic infrastructure at traffic signals such as poles, span wires, mast arms, wiring, equipment interconnectivity, video equipment and cabinets to improve and upgrade the traffic signal system. The project also is used for replacement of signal cabinets. The expected life of a signal is 30 years; currently there are more than 1,100 signals within the City.

Resources	**LTD Actuals**	**2020 Revised**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**Total**
Commercial Parking Tax	2,349	628	-	-	-	-	688	712	4,377
Developer Mitigation	-	240	-	-	-	-	-	-	240
Interdepartmental Transfer	-	-	1	2	-	-	-	-	3
Real Estate Excise Tax II	1,012	1	-	-	-	-	-	-	1,013
Transportation Move Seattle Levy - Lid Lift	3,352	1,358	1,435	1,413	1,762	1,801	132	-	11,254
Vehicle License Fees $60 & 0.1% Sales Tax	-	-	650	-	-	-	-	-	650
Total:	**6,714**	**2,227**	~~1,436~~	**1,414**	**1,762**	**1,801**	**820**	**712**	~~16,887~~
Revised Total:	**6,714**	**2,227**	**2,086**	**1,414**	**1,762**	**1,801**	**820**	**712**	**17,537**

Fund Appropriations / Allocations[1]	**LTD Actuals**	**2020 Revised**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**Total**
Move Seattle Levy Fund	3,352	1,358	1,435	1,413	1,762	1,801	132	-	11,254
REET II Capital Fund	1,012	1	-	-	-	-	-	-	1,013
Transportation Fund	2,349	868	1	2	-	-	688	712	4,620
Transportation Benefit District Fund	-	-	650	-	-	-	-	-	650
Total:	**6,714**	**2,227**	~~1,436~~	**1,414**	**1,762**	**1,801**	**820**	**712**	~~16,887~~
Revised Total:	**6,714**	**2,227**	**2,086**	**1,414**	**1,762**	**1,801**	**820**	**712**	**17,537**

Unsecured Funding:	**LTD Actuals**	**2020 Revised**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**Total**
To Be Determined	-	-	-	-	-	-	1,125	1,213	2,338
Total:	**-**	**-**	**-**	**-**	**-**	**-**	**1,125**	**1,213**	**2,338**

Unsecured Funding Strategy: Funding for this program beyond 2024 is dependent upon a future voter approved levy.

O&M Impacts: This is a capital maintenance project that reduces the need for O&M by improving asset condition.

[1]Funds are appropriated through the Adopted Budget at the Budget Summary Level. All Amounts shown above are in thousands of dollars

Transit Corridor Improvements

Project No:	MC-TR-C029	**BSL Code:**	BC-TR-19003
Project Type:	Ongoing	**BSL Name:**	Mobility-Capital
Project Category:	Improved Facility	**Location:**	Citywide
Current Project Stage:	N/A	**Council District:**	Multiple
Start/End Date:	N/A	**Neighborhood District:**	Multiple
Total Project Cost:	N/A	**Urban Village:**	Multiple

This program implements multimodal projects which improve transit speed, reliability, access, safety, and convenience. The program focuses on corridors and projects identified in the Transit Master Plan. Funding from Move Seattle Levy and other local funding sources are used to leverage partnership opportunities.

Resources	**LTD Actuals**	**2020 Revised**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**Total**
City Light Fund Revenues	7	-	-	-	-	-	-	-	7
Commercial Parking Tax	1,678	(13)	-	-	-	-	-	-	1,666
Developer Mitigation	-	704	-	-	-	-	-	-	704
Federal Grant Funds	3,546	-	-	-	-	-	-	-	3,546
King County Funds	1,596	470	-	-	-	-	-	-	2,066
LTGO Bond Proceeds	973	-	-	-	-	-	-	-	973
Private Funding/Donations	50	473	-	-	-	-	-	-	523
Sound Transit Funds	617	5,764	-	-	-	-	-	-	6,382
State Grant Funds	8,037	-	-	-	-	-	-	-	8,037
Transportation Funding Package - Lid Lift	18,908	-	-	-	-	-	-	-	18,908
Transportation Move Seattle Levy - Lid Lift	6,758	1,141	-	2,000	4,186	3,361	-	-	17,446
Vehicle License Fees $60 & 0.1% Sales Tax	1,869	1,835	4,350	-	-	-	-	-	~~3,704~~ **8,054**
Vehicle Licensing Fees	6,083	943	1,928	1,271	1,090	944	1,044	-	13,303
Total:	**50,124**	**11,317**	~~1,928~~	**3,271**	**5,276**	**4,305**	**1,044**	**-**	~~77,265~~
Revised Total:	**50,124**	**11,317**	**6,278**	**3,271**	**5,276**	**4,305**	**1,044**		**81,615**

Fund Appropriations / Allocations[1]	**LTD Actuals**	**2020 Revised**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**Total**
2016 Multipurpose LTGO Bond Fund	973	-	-	-	-	-	-	-	973
Bridging The Gap Levy Fund	18,908	-	-	-	-	-	-	-	18,908
Move Seattle Levy Fund	6,758	1,141	-	2,000	4,186	3,361	-	-	17,446
Transportation Benefit District Fund	7,953	2,778	~~1,928~~ **6,278**	1,271	1,090	944	1,044	-	~~17,007~~ **21,357**
Transportation Fund	15,532	7,398	-	-	-	-	-	-	22,930
Total:	**50,124**	**11,317**	~~1,928~~	**3,271**	**5,276**	**4,305**	**1,044**	**-**	~~77,265~~
Revised Total:	**50,124**	**11,317**	**6,278**	**3,271**	**5,276**	**4,305**	**1,044**		**81,615**

Unsecured Funding:	**LTD Actuals**	**2020 Revised**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**Total**
To Be Determined	-	-	-	-	-	-	2,900	4,010	6,910
Total:	**-**	**-**	**-**	**-**	**-**	**-**	**2,900**	**4,010**	**6,910**

Unsecured Funding Strategy: Funding for this program beyond 2024 is dependent upon a future voter approved levy.

O&M Impacts: SDOT has individual project budgets for the maintenance of painted markings, signage, signals, bridges and roadway structures, urban forestry, and sidewalks and pavement; these budgets are constrained by the availability of transportation specific and general funds. The SDOT Asset Management website (https://www.seattle.gov/transportation/about-sdot/asset-management) provides unconstrained operational cost forecasting by asset type, typical lifecycle and average maintenance cost ranges.

[1]Funds are appropriated through the Adopted Budget at the Budget Summary Level. All Amounts shown above are in thousands of dollars

[1]Funds are appropriated through the Adopted Budget at the Budget Summary Level. All Amounts shown above are in thousands of dollars

SUMMARY and FISCAL NOTE*

Department:	Dept. Contact/Phone:	CBO Contact/Phone:
SDOT	Susan Lund/206.615.1699	Christie Parker/206.684.5211

** Note that the Summary and Fiscal Note describes the version of the bill or resolution as introduced; final legislation including amendments may not be fully described.*

1. BILL SUMMARY

Legislation Title: AN ORDINANCE relating to the City's 2021 Budget; amending Ordinance 126237, which adopted the 2021 Budget, including the 2021-2026 Capital Improvement Program (CIP); changing appropriations to the Seattle Department of Transportation in various budget control levels; and revising project allocations for certain projects in the 2021-2026 CIP; all by a 3/4 vote of the City Council.

Summary and background of the Legislation: This legislation amends appropriations in the 2021 Adopted Budget for several programs and projects funded by Seattle Transportation Benefit District revenues that were held in reserve while the City litigated the constitutionality of Initiative 976 and determined whether Seattle voters would approve a new STBD transit funding measure in the 2020 general election. The total amount of reserved funds is $23.7 million. This legislation appropriates $15 million in 2021. An additional $2.7 million is anticipated to be spent in 2022, and the remaining $6 million will be held as a strategic reserve that can be used in the event of revenue declines and/or for program ramp-down in 2027 when the new 2020 STBD (0.15% sales tax) measure expires.

2. CAPITAL IMPROVEMENT PROGRAM

Does this legislation create, fund, or amend a CIP Project? _X__ Yes ____ No

Project Name:	Project I.D.:	Project Location:	Start Date:	End Date:	Total Project Cost Through 2026:
Transit Corridor Improvements	MC-TR-C029	Citywide	Ongoing	Ongoing	$81,615,000
Route 40 Transit-Plus Multimodal Corridor Project	MC-TR-C079	Various	2016	2024	$21,132,000
BRT Concepts Design	MC-TR-C010	Citywide	2016	2021	$2,441,000
Signal Major Maintenance	MC-TR-C026	Citywide	Ongoing	Ongoing	$17,537,000

23rd Avenue Corridor Improvements	MC-TR-C037	23rd Ave	2013	2022	$62,478,000

3. SUMMARY OF FINANCIAL IMPLICATIONS

Does this legislation amend the Adopted Budget? __X_ Yes ____ No

	General Fund $		Other $	
Appropriation change ($):	**2021**	**2022**	**2021**	**2022**
	$0	**$0**	**$15,000,000**	**$2,700,000**
	Revenue to General Fund		**Revenue to Other Funds**	
Estimated revenue change ($):	**2021**	**2022**	**2021**	**2022**
	$0	**$0**	**$0**	**$0**
	No. of Positions		**Total FTE Change**	
Positions affected:	**2021**	**2022**	**2021**	**2022**
	0	**0**	**0**	**0**

Does the legislation have other financial impacts to the City of Seattle that are not reflected in the above, including direct or indirect, short-term or long-term costs?
No

Is there financial cost or other impacts of *not* implementing the legislation?
Several STBD transit and Levy to Move Seattle needs would go unmet without these additional appropriations.

3.a. Appropriations

__X__ This legislation adds, changes, or deletes appropriations.

Fund Name and number	Dept	Budget Control Level Name/#*	2021 Appropriation Change	2022 Estimated Appropriation Change
Transp. Benefit District Fund/19900	SDOT	Mobility-Capital (BC-TR-19003)	$9,350,000	$2,700,000
Transp. Benefit District Fund/19900	SDOT	Major Maintenance /Replacement (BC-TR-19001)	$650,000	
Transp. Benefit District Fund/19900	SDOT	Mobility – Operations (BO-TR-17003)	$5,000,000	
TOTAL			**$15,000,000**	**$2,700,000**

See budget book to obtain the appropriate Budget Control Level for your department.

Is this change one-time or ongoing?
This is a one-time appropriation of the remaining 2014 voter approved STBD funding.

Appropriations Notes: In addition to the above items, the spending plan for the residual revenues from the 2014 STBD ballot measure also includes $6,000,000 for a strategic reserve. These reserves are not appropriated in this legislation; however, they will be reflected in the spending plan for the STBD Fund (19900).

3.b. Revenues/Reimbursements

____ **This legislation adds, changes, or deletes revenues or reimbursements.**

Revenue/Reimbursement Notes: Revenue was collected in prior years.

3.c. Positions

____ **This legislation adds, changes, or deletes positions.**

4. OTHER IMPLICATIONS

a. Does this legislation affect any departments besides the originating department?
No

b. Is a public hearing required for this legislation?
No

c. Is publication of notice with *The Daily Journal of Commerce* and/or *The Seattle Times* required for this legislation?
No

d. Does this legislation affect a piece of property?
No

e. Please describe any perceived implication for the principles of the Race and Social Justice Initiative. Does this legislation impact vulnerable or historically disadvantaged communities? What is the Language Access plan for any communications to the public?
People of color have lower rates of personal vehicle ownership and are more likely to fill essential worker roles and therefore continue to rely on transit service, and will benefit more from the transit speed and reliability and access projects funded through this legislation.

f. Climate Change Implications

1. **Emissions: Is this legislation likely to increase or decrease carbon emissions in a material way?**
   Personal transportation is the largest source of GHG emitted in Seattle. Transit service has less climate impact than traveling by personal vehicle or TNCs.

2. **Resiliency: Will the action(s) proposed by this legislation increase or decrease Seattle's resiliency (or ability to adapt) to climate change in a material way? If so,**

explain. If it is likely to decrease resiliency in a material way, describe what will or could be done to mitigate the effects.

The climate benefit of transit is more related to reduced or avoided GHG emissions than it is on adaptation.

g. If this legislation includes a new initiative or a major programmatic expansion: What are the specific long-term and measurable goal(s) of the program? How will this legislation help achieve the program's desired goal(s).

Delivery of the service and projects funded through this legislation is the most direct measure. Performance measures will be included in annual STBD reporting as required in STBD Resolution 12.

List attachments/exhibits below:

Seattle Transportation Benefit District (STBD)

Allocation of Reserves Due to I-976

Candida Lorenzana, Nico Martinucci
Transportation & Utilities Committee
March 3, 2021

City of Seattle

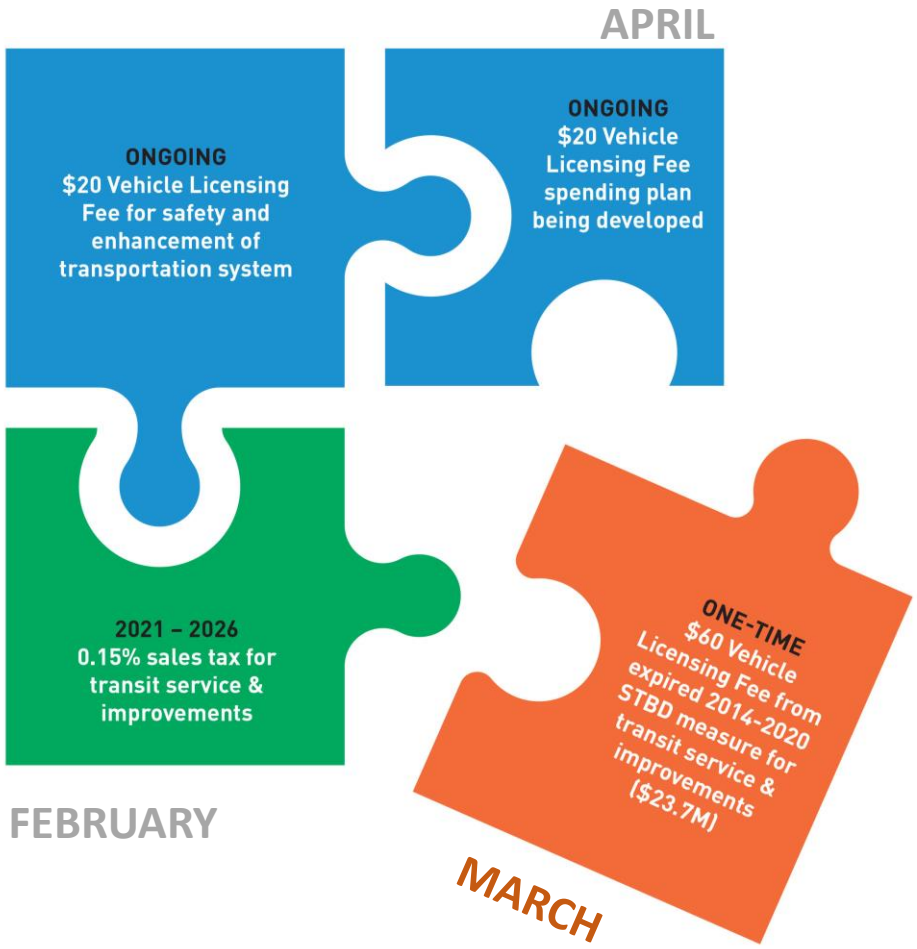
Presentation overview

Reserves from 2014 Measure due to I-976 – Spend Plan Proposal

- Implementation timeline
- Background – Revenues and $60 Vehicle License Fee
- Transit Advisory Board principles and priorities
- Proposed spend plan and project list

STBD Timeline

DATE	ACTION
February	Council and Mayor approve ordinance authorizing Metro/SDOT Transit Service Funding Agreement
Today	**Standalone supplemental budget legislation for reserves due to I-976 at TUC**
March 20	Metro service change; Transit Service Funding Agreement in effect
April 1	New $20 VLF proposed spending plan due to Council



Overview: Seattle Transportation Benefit District (STBD) Revenue Sources

- 2010 Councilmanic $20 VLF
  - Generated $8.6M in 2019; funds various capital & maintenance programs
  - Continues indefinitely
- 2014 Proposition 1 (expired end of 2020)
  - 0.1% sales tax ($30.4M in 2019) and $60 VLF ($25.8M in 2019); funded transit service and access improvements
- 2020 Proposition 1 (expires in 2027)
  - 0.15% sales tax (estimated $45.6M in 2022*); programmatic extension of 2014 Prop 1
- 2020 Additional Councilmanic $20 VLF
  - Estimated $7.4M in 2022*; funding priorities TBD
  - Continues indefinitely

*First full year of revenue collection

$60 Vehicle License Fee (VLF) Background

$60 VLF

Local News | Local Politics | Northwest | Traffic Lab

Washington Supreme Court strikes down I-976, which cut car-tab taxes

Oct. 15, 2020 at 8:53 am | *Updated Oct. 16, 2020 at 11:52 am*

From Seattle Times

- **~$23.7M** in $60 VLF revenue was put in jeopardy due to I-976 uncertainty; programmatic spending was reduced to reflect this
  - In the event of an unsuccessful legal challenge, these fees would need to be refunded
- With WA Supreme Court decision on October 15, these funds became available for programming

Reserves due to I-976 Programming – Engagement

$60 VLF

- Engaged Transit Advisory Board (TAB) and Move Seattle Levy Oversight Committee
- Coincided with COVID-19 Levy Reassessment and 2021-22 budget process
- TAB priorities:
  - Focus on restoring transit projects and those with clear transit nexus
  - Maintain intent of voter-approved measure
- TAB supportive of proposed plan

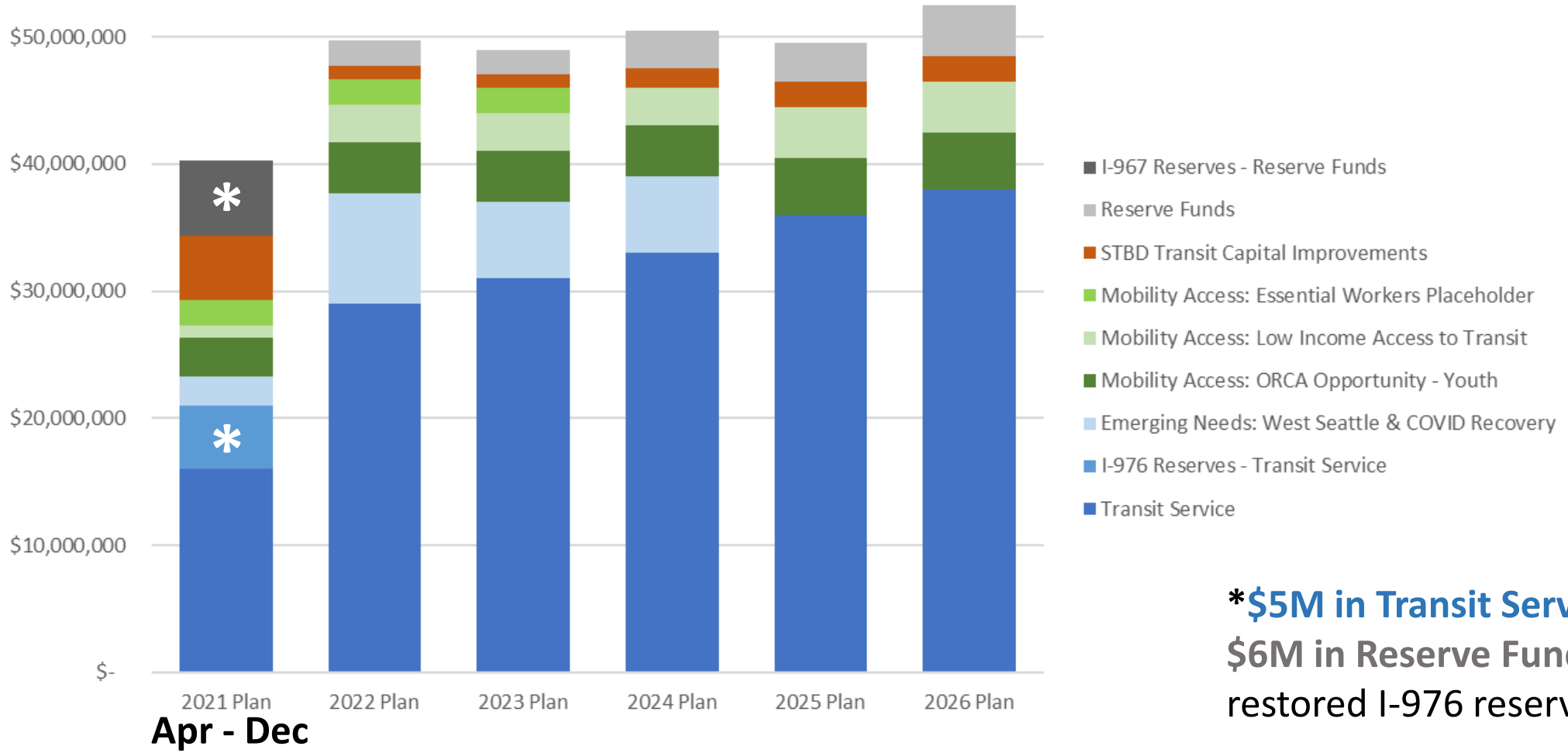
Overview: Proposed Spending of Reserves Related to I-976

$60 VLF

Category	Amount (M)	Description
Project Restoration	$12.7	Funds various transit and transit-related projects/programs, including bus stop improvements, Transit-Plus Multimodal Corridor delivery, crosswalk improvements, and more
Transit Service	$5.0	Allows for sustainable transit service funding and delivery in 2021 and beyond; helps fill gap in Q1 revenue collection
Strategic Reserves	$6.0	Provides contingency during uncertain times, and allows capacity for purchasing additional service in out years of the program
TOTAL:	**$23.7**	

STBD Prop 1 Draft Spend Plan (2021 – 2026)

$60 VLF



***$5M in Transit Service** and **$6M in Reserve Funds** from restored I-976 reserves

Key Project Restoration (1 of 2)

$60 VLF

Project/Program	Amount (M)	Description	Transit Nexus?
Gilman Ave Bus Safety Improvements; Lake City Way & NE 125th St Bus Stop Improvements	$1.75	Current projects that improve bus safety and operations along Gilman Ave (multimodal improvements) and Lake City Way & NE 125th St (bus bulb and stop expansion)	Yes
Transit Spot Improvement Program	$2.6	Restoration of programmatic budget reduction in 2021 budget as described in Move Seattle Levy Assessment Report; funds to install concrete bus zone improvements, red bus lanes, and rear-door bus pads	Yes
Route 40 Transit-Plus Multimodal Corridor Project	$0.3 (+$2.7 in 2022)	Allocation to fill expected gap in grant funding	Yes

Key Project Restoration (2 of 2)

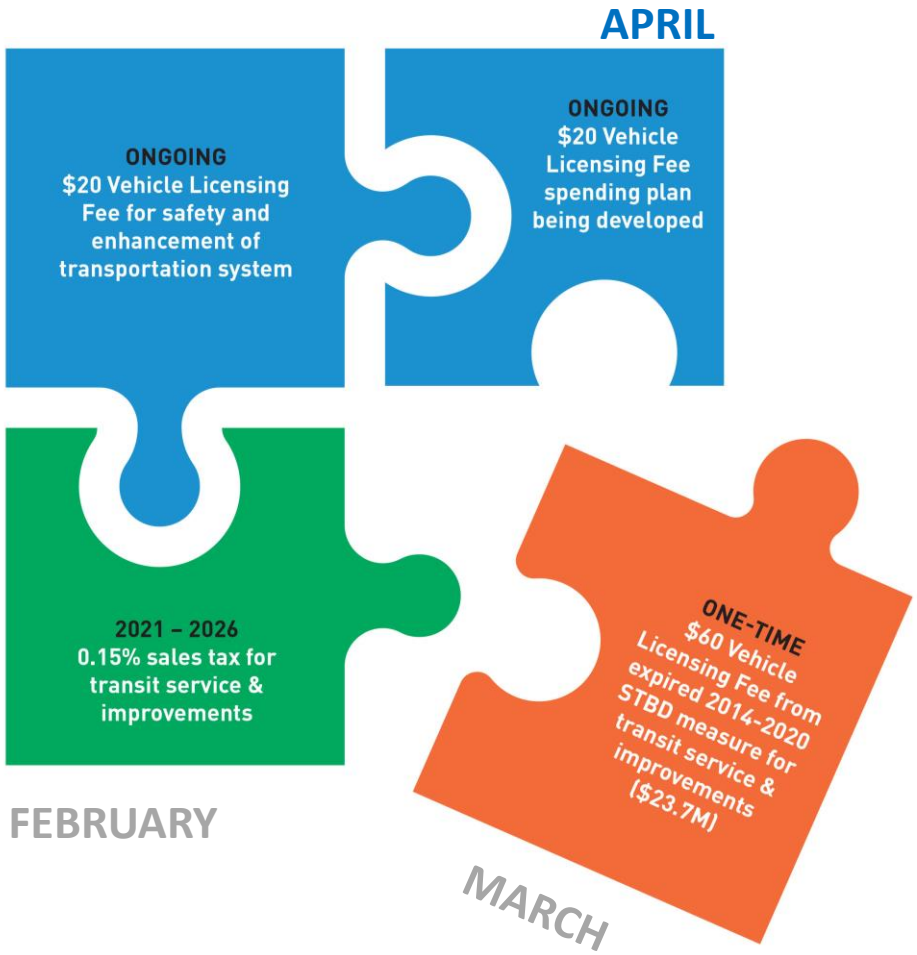
$60 VLF

Project/Program	Amount (M)	Description	Transit Nexus?
TPMC Program Support	$0.40	Restoration of fund gap created by budget reduction to BRT Concept Design CIP, which funds staff and technical resources to support Transit-Plus Multimodal Corridor Program	Yes
15th Ave NW & NW Market St Signal Improvements	$0.65	Restores funding removed due to 2021 budget reductions and supports transit signal priority enhancements (benefitting Route 44 and RapidRide D Line)	Yes
23rd Ave Phase 3	$4.3	Funds 12 bus zone improvements, signal upgrade at 23rd & John (transit improvement), and Vision Zero safety elements	Yes

TOTAL: $10.0M in 2021 spending /$2.7M in 2022

STBD Next Steps

DATE	ACTION
Today	Committee considers legislation for standalone supplemental budget legislation for one-time reserves related to I-976 at TUC
March 20	Metro service change; Transit Service Funding Agreement in effect
April 1	New $20 VLF proposed spending plan due to Council



Questions?

www.seattle.gov/transit/about-seattle-transportation-benefit-district

Candida.Lorenzana@seattle.gov | (206) 684.5907

www.seattle.gov/transportation

SEATTLE CITY COUNCIL
CENTRAL STAFF

February 26, 2021

MEMORANDUM

To: Transportation and Utilities Committee
From: Calvin Chow, Analyst
Subject: Authorizing Legislation for $60 Vehicle License Fee Reserves Spending Plan

On March 3, 2021, the Transportation and Utilities Committee will consider and possibly vote on Council Bill (CB) 120009,[1] which addresses the $23.7 million of Seattle Transportation Benefit District (STBD) Proposition 1 funds that had been held in reserve pending the outcome of legal challenges to Initiative 976. This legislation would authorize the Seattle Department of Transportation (SDOT) to spend $15 million of these funds in 2021. The legislation anticipates that a further $2.7 million would be proposed to be spent in the 2022 budget, and that the remaining $6 million would be held in reserve.

Background

In November 2014, Seattle voters approved STBD Proposition 1, which authorized a $60 vehicle license fee and a 0.1 percent sales tax to support transit service in Seattle. In November 2019, Washington voters approved Initiative 976, which eliminated Seattle's authority to collect vehicle license fees. The City of Seattle joined the legal challenge to Initiative 976 and received a temporary injunction to continue to collect the vehicle license fee while the case was before the courts. In October 2020, the Washington State Supreme Court ruled that Initiative 976 was unconstitutional and does not constrain Seattle's use of the vehicle license fee as authorized under state law.[2]

While SDOT continued to collect vehicle license fees under the temporary injunction, SDOT reserved a portion of this revenue ($23.7 million) in case Initiative 976 was upheld and vehicle license fees would have to be refunded. Because Initiative 976 was ruled unconstitutional, this remaining STBD Proposition 1 fund balance is now available to be spent.

Revenue collection under STBD Proposition 1 expired at the end of 2020,[3] but the authorizing legislation[4] still governs the allowable use of these funds. STBD Proposition 1 funds may be used to:

[1] CB 120009 will be included on the March 1, 2021 Introduction and Referral Calendar and referred to the Transportation and Utilities Committee.
[2] Separate from the STBD Proposition 1 funds under consideration in CB 120009, Council raised the councilmanic vehicle license fee from $20 to $40 (Ordinance 126234) as part of the 2021 Adopted Budget. Council directed SDOT to conduct a stakeholder process and recommend a spending plan for this revenue by April 2021.
[3] In November 2020, Seattle voters approved a new transit measure, Seattle Proposition 1, which authorized a 0.15 percent sales tax to continue to support transit service in Seattle.
[4] The allowable uses of STBD Proposition 1 funds were established in STBD Resolution 12 and amended by Ordinance 125606.

- Purchase Metro transit service hours on routes with at least 65 percent of all stops within the City of Seattle.
- Purchase Metro transit service hours on RapidRide lines that service the City of Seattle.
- Up to $7 million annually may be used to support transit use by children and youth.
- Up to $10 million annually may be used to support transit capital improvements.
- Up to $3 million annually may be used to support regional transit partnerships.
- Up to $2 million annually may be used to support access to transit for low-income riders.

Proposed Spending Plan

The proposed legislation is consistent with the allowable uses of STBD Proposition 1 funding. The legislation would authorize $15 million of spending in 2021, including $5 million for transit service and $10 million for transit capital projects, as follows:

- $5 million for the purchase of Metro transit service (Item 1.1).
- $4.35 million for Transit Corridor Improvements program (Item 2.1). This category of spending includes the Gilman Ave Bus Safety Improvements, the Lake City Way/NE 125th St Bus Stop Improvements, and the other transit spot improvements.
- $300,000 for the Route 40 Transit-Plus Multimodal Corridor project (Item 2.2).
- $400,000 for the Bus Rapid Transit Concepts Design project (Item 2.3).
- $650,000 for the Signal Major Maintenance program (Item 2.4). This category of spending includes the 15th Ave NW/NW Market St Signal Improvements.
- $4.3 million for the 23rd Ave Corridor Improvement project (Item 2.5).

In addition to the 2021 appropriations listed above, the proposed legislation anticipates:

- $2.7 million for the Route 40 Transit-Plus Multimodal Corridor project in 2022.
- $6 million of reserves against potential cost or revenue fluctuations in the delivery of transit service implementing the November 2020 Seattle Proposition 1 ballot measure.

In developing the proposed spending, SDOT engaged the Transit Advisory Board and the Move Seattle Levy Oversight Committee.

Considerations

The $23.7 million under consideration with this legislation is one-time funding. The proposed capital spending ($10 million in 2021 and $2.7 million in 2022) would restore funding for transit projects that had been paused as part of the 2020 Budget rebalancing in response to COVID-19. These projects had previously been identified and prioritized as part of the Transit Master Plan Implementation Plan and would be an appropriate use of one-time funding.

The proposed $5 million for transit service would help fill a funding gap in 2021 as the new 2020 Seattle Proposition 1 transit measure is implemented and begins collecting sales tax in April 2021.[5] This funding will also help smooth the transition in transit service levels[6] as the 2020 Seattle Proposition 1 measure will generate less annual revenue, and can afford fewer annual service hours, than the previous 2014 STBD Proposition 1 measure. While transit demand remains lower than pre-COVID-19 levels,[7] transit remains an essential service for many riders without access to other transportation alternatives.

The proposed $6 million for reserves would provide for some flexibility in the face of COVID-19 response and economic recovery. With depressed transit demand, the cost of transit service increases as less fare revenue to support the service. In addition, the pace of recovery in sales tax revenues (the source of revenue for the 2020 Seattle Proposition 1) remains uncertain. Maintaining some level of reserves would help address these uncertainties.

Council may wish to consider reallocating spending under the allowable uses of STBD Proposition 1 funds. Please contact me if you have any questions or concerns regarding this legislation.

cc: Dan Eder, Interim Director
Aly Pennucci, Policy and Budget Manager

---

[5] Implemented by Ordinance 126250.

[6] King County Metro makes transit service changes (incorporating Seattle transit service purchases) twice a year, in the Spring and Fall.

[7] The Washington State Department of Transportation (WSDOT) Covid-19 Transportation System Reporting Dashboard shows that King County Metro ridership has continued to fluctuate between -50 percent and -84 percent of baseline ridership in 2021.

File #: CB 120002, **Version:** 1

CITY OF SEATTLE

ORDINANCE _____

COUNCIL BILL _____

AN ORDINANCE relating to surveillance technology implementation; authorizing approval of uses and accepting surveillance impact reports for Seattle City Light's use of Current Diversion Technologies.

WHEREAS, Ordinance 125376 requires Council approval of surveillance impact reports (SIRs) related to approval of uses for certain technology, with existing/retroactive technology to be placed on a Master Technology List; and

WHEREAS, the ordinance provisions apply to the Current Diversion Technologies (Binoculars / Spotting Scope, Check Meter Device, SensorLink AmpFork) in use by Seattle City Light (SCL); and

WHEREAS, SCL conducted policy rule review and community review as part of the development of the SIRs; and

WHEREAS, Seattle Municipal Code Section 14.18.080, enacted by Ordinance 125679, also requires review of the SIRs by a Community Surveillance Working Group composed of relevant stakeholders and a statement from the Chief Technology Officer in response to the Working Group's recommendations; and

WHEREAS, development of the SIRs and review by the Working Group has been completed; NOW, THEREFORE,

BE IT ORDAINED BY THE CITY OF SEATTLE AS FOLLOWS:

Section 1. Pursuant to Ordinances 125376 and 125679, the City Council approves use of the Seattle City Light's Current Diversion Technologies and accepts the Surveillance Impact Reports (SIRs), for these technologies, attached to this ordinance as Attachment 1, 2, and 3 and the Executive Overview, for the same

technologies, attached to this ordinance as Attachment 4.

Section 2. This ordinance shall take effect and be in force 30 days after its approval by the Mayor, but if not approved and returned by the Mayor within ten days after presentation, it shall take effect as provided by Seattle Municipal Code Section 1.04.020.

Passed by the City Council the _____ day of _____, 2021, and signed by me in open session in authentication of its passage this _____ day of _____, 2021.

_____

President _____ of the City Council

Approved / returned unsigned / vetoed this _____ day of _____, 2021.

_____

Jenny A. Durkan, Mayor

Filed by me this _____ day of _____, 2021.

_____

Monica Martinez Simmons, City Clerk

(Seal)

Attachments:
Attachment 1 - Binoculars/Spotting Scope SIR

Attachment 2 - Check Meter Device SIR
Attachment 3 - SensorLink Amp Fork SIR
Attachment 4 - Current Diversion Technologies Executive Overview

City of Seattle

2019 Surveillance Impact Report

Current Diversion Team: Binoculars / Spotting Scope

Seattle City Light

Seattle City Light 1
Submitting Department Memo 3
Surveillance Impact Report ("SIR") overview 7
Privacy Impact Assessment 8
Financial Information 19
Expertise and References 20
Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet 21
Privacy and Civil Liberties Assessment 35
CTO Response 42
Appendix A: Glossary 49
Appendix B: Meeting Notice(s) 51
Appendix C: Meeting Sign-in Sheet(s) 59
Appendix D: Department of Neighborhood Focus Group Notes 84
Appendix E: All Comments Received from Members of the Public 116
Appendix F: Department Responses to Public Inquiries 124
Appendix G: Letters from Organizations or Commissions 126
Appendix H: Comment Analysis Methodology 150
Appendix I: Supporting Policy Documentation 153
Appendix J: CTO Notification of Surveillance Technology 154

City of Seattle

Submitting Department Memo

Seattle City Light

MEMO

APRIL 16, 2019

TO
Seattle City Council

FROM
Julie Moore, Public Information Officer

SUBJECT
Summary of Surveillance Impact Reports for Three Current Diversion Detection Technologies

---

Seattle City Light's three current diversion detection technologies are undergoing review pursuant to Seattle Municipal Code, Chapter 14.18, *Acquisition and Use of Surveillance Technologies*.

The utility's Current Diversion Team (CDT) is responsible for investigating when electricity is being used but unaccounted for by City Light's billing system, and hence, not paid for. The three technologies City Light's CDT employs are:

1. Standard, commercial-grade, unpowered binoculars.
2. The SensorLink Ampstik.
3. The SensorLink Transformer Meter System.

Formal policies and procedures governing current diversion activity are described in City Light's Department Policy and Procedure (DPP) P III-416*, Current Diversion*. The CDT manager is responsible for ensuring City Light staff comply with the DPP and all existing rules.

TECHNOLOGIES

The utility's CDT members are the only staff who use the three technologies to investigate current diversion, and always upon preexisting and/or reported suspicion and with the approval of the current diversion coordinator. Suspicion of current diversion can take a variety of forms, such as a neighbor's report of questionable circumstances, a meter reader's observation of a tampered meter, or a billing specialist's observation of unusual or zero consumption.

CDT members who investigate potential current diversions drive standard City Light-marked vehicles and can be identified by their City Light ID badge and a hard hat.

1) BINOCULARS

When distance is a barrier to close physical inspection, CDT members may use binoculars to examine meters in assessing if current diversion is taking place. Binoculars may also be used to determine if potentially dangerous alterations to City Light's electrical infrastructure exist. The binoculars do not collect data, and do not contain any special enhancements requiring power (e.g., night vision, video-recording capabilities). Data derived from observations via CDT binoculars are accessible only by CDT members.

When used, CDT members use the binoculars for approximately one minute at a time. CDT members view locations that are in public view and the binoculars do not digitally record anything. Furthermore, the CDT only investigates specific meters and other implicated electrical equipment where current diversion is suspected. Therefore, the risk of staff inadvertently capturing data related to other customers is extremely low.

Data obtained by means of binoculars—which consist of notes made by staff based on their binocular-facilitated observations—are stored in a secure folder on City Light's digital network drive. The data, as well as overall incident reports, are accessible only by CDT members and the current diversion coordinator. Data will be retained per City Light records retention schedules. The current diversion coordinator has responsibility for ensuring compliance with data retention requirements.

The limited number of binoculars and of CDT members makes the routine tracking of this equipment relatively straight forward. Binoculars are issued to CDT members and are stored in their official vehicles. These vehicles are operated, locked, and stored in accordance with utility security procedures.

2) SENSORLINK AMPSTIK

The SensorLink Ampstik ("Ampstik") is a hand-held tool used to detect instantaneous current flow through a service drop. Specifically, it is an electrical device mounted on an extensible pole (up to 40' to 50') that allows a circular clamp to be placed around a service-drop wire. The wire is the same wire that provides electrical service to a customer location via a City Light-provided meter. The device then displays instantaneous readings of the amount of electrical energy flow as measured in amperage or "amps." The CDT member may then compare those reads against the readings displayed on the electric meter, allowing staff to determine if current is presently being diverted. Because the device delivers a point-in-time reading, it is deployed by hand for approximately 10 minutes at a time. The Ampstik ultimately allows the utility to determine the valuation of the energy illegally diverted, which supports City Light's mission of recovering this value for the ratepayers via a process called "back-billing."

Risk of inadvertent or improper collection is low for two reasons. First, the CDT only investigates specific, metered locations previously identified as sites of suspected current diversion. Second, Ampstik devices are used only on those service-drop lines that are delivering electrical service to the suspected location.

The limited number of this equipment and of CDT members makes the routine tracking of the Ampstik devices relatively straight forward. Ampstiks are issued to CDT members and are stored

in their official vehicles. These vehicles are operated, locked, and stored in accordance with utility security procedures. City Light records Ampstik serial numbers and their assignments to CDT members, along with their deployment status.

CDT members who are journey-level electrical workers trained to use Ampstiks may collect and access this data. This data may be accessed only by CDT staff and the current diversion coordinator, and are stored in a secure folder on City Light's digital network drive. Data will be retained per City Light records retention schedules. The current diversion coordinator has responsibility for ensuring compliance with data retention requirements.

3) SENSORLINK TRANSFORMER METER SYSTEM (TMS)

The SensorLink Transformer Meter System ("TMS") is a device that measures the amount of electrical energy flowing through a service-drop wire over time. It digitally captures the instantaneous information for later retrieval by the CDT member(s) via a secure wireless protocol. TMS devices are housed in a black, weatherproof box of approximately four square inches, and have an external City Light inventory control number so that line workers know what function the device serves. These devices are typically installed on an electric pole adjacent to a transformer for a period of one week to one month depending on the specific case needs and crew availability. These units ultimately allow the utility to determine the valuation of the energy illegally diverted, which supports City Light's mission of recovering this value for the ratepayers via a process called "back-billing."

The CDT owns six TMS units, which are deployed on the basis of case number and need. Deployment level on a given case can vary from none (zero) to all (six). Once a case is properly opened, CDT members may check the devices out without prior additional authorization, although in nearly all circumstances, the current diversion coordinator is aware of deployment due to position responsibilities. City Light records TMS serial numbers and their assignments to CDT members, along with their deployment status.

Risk of inadvertent or improper collection is low for two reasons. First, the CDT member only investigates specific, metered locations previously identified and properly documented as a site of suspected current diversion. Second, TMS devices are used only on those service-drop lines that are delivering electrical service to a suspected location.

The SensorLink TMS device is not "visible to the public" in any conventional sense, although to a trained eye, it may be visible near a transformer on an electrical pole. CDT members, who are journey-level electrical workers trained in the placement, use, and removal of the device, may collect the data. The quantitative data – accumulated consumption (in kilowatt hours), average volts (current strength), average amps (current flow), and interval consumption (in kilowatt hours per a pre-defined time unit) – are accessed by CDT members remotely using a secure radio protocol and a specific, password-protected software program.

Data obtained by means of the TMS are stored in a secure folder on City Light's digital network drive, accessible only by CDT members and City Light management. Data stored in the TMS are deleted after its retrieval by the CDT staff and/or upon its removal from the electrical pole. In other words, no data remains in the TMS once its use for a specific current diversion case has

been completed. Data will be retained per City Light record retention schedules. The current diversion coordinator has responsibility for ensuring compliance with data retention requirements.

DATA SHARING & AUDITING

Data collected from the use of the three technologies may be shared with other government staff in two instances. When a determination is made that current diversion has taken place, a valuation of the stolen energy is shared with City Light's billing division so that the utility can "back-bill" and recover the diverted energy costs from the appropriate customer. Also, data is shared with police investigators and/or prosecutors for the purposes of law enforcement or legal action in complex or aggravated cases (e.g., when large sums of energy have been diverted/stolen, or where there is a safety risk to the public). This policy is formally laid out in City Light's DPP 500 P III-416. In both instances, data sharing is required for City Light to recover stolen energy costs. In the latter case (i.e., information sharing with police investigators) data sharing may also be required in order to protect public safety, since unauthorized alterations to the electrical system can pose a serious, and at times, lethal danger to the public.

To safeguard CDT data, the current diversion coordinator will request Seattle IT to provide audit data, so that City Light may complete an audit to ensure that access rights are assigned only to authorized staff.

IMPORTANCE OF TECHNOLOGIES – SUPPORTING CITY LIGHT'S MISSION

One of City Light's core missions as an electric utility is to recoup the costs of the energy provided to customers. This is required by Seattle Municipal Code 21.49.100, *Application and Contract Provisions*. Additionally, as a general rule the Washington State Constitution's Article VIII, Section 7 prohibits the gifting of public funds. Since all three technologies enable City Light to recover unaccounted for electricity costs, they contribute to the department's mission of being legally compliant. Translated into monetary value, the utility recovered over $1.6 million in 2017 using these technologies. This would otherwise be a substantial financial loss for the City.

Surveillance Impact Report ("SIR") overview

About the Surveillance Ordinance

The Seattle City Council passed Ordinance 125376, also referred to as the "Surveillance Ordinance," on September 1, 2017. SMC 14.18.020.b.1 charges the City's executive with developing a process to identify surveillance technologies subject to the ordinance. Seattle it, on behalf of the executive, developed and implemented a process through which a privacy and surveillance review is completed prior to the acquisition of new technologies. This requirement, and the criteria used in the review process, are documented in Seattle it policy pr-02, the "surveillance policy".

How this Document is Completed

This document is completed by the requesting department staff, support and coordinated by the Seattle information technology department ("Seattle it"). As Seattle it and department staff complete the document, they should keep the following in mind.

1. Responses to questions should be in the text or check boxes only; all other information (questions, descriptions, etc.) Should **not** be edited by the department staff completing this document.
2. All content in this report will be available externally to the public. With this in mind, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.

Surveillance Ordinance Review Process

The following is a high-level outline of the complete SIR review process.

Upcoming for Review	Initial Draft	Open Comment Period	Final Draft	Working Group	Council Review
The technology is upcoming for review, but the department has not begun drafting the surveillance impact report (SIR).	Work on the initial draft of the SIR is currently underway.	The initial draft of the SIR and supporting materials have been released for public review and comment. During this time, one or more public meetings will take place to solicit feedback.	During this stage the SIR, including collection of all public comments related to the specific technology, is being compiled and finalized.	The surveillance advisory working group will review each SIR's final draft and complete a civil liberties and privacy assessment, which will then be included with the SIR and submitted to Council.	City Council will decide on the use of the surveillance technology, by full Council vote.

Privacy Impact Assessment

Purpose

A Privacy Impact Assessment ("PIA") is a method for collecting and documenting detailed information collected in order to conduct an in-depth privacy review of a program or project. A PIA asks questions about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. It also requests information about policies, training and documentation that govern use of the technology. The PIA responses are used to determine privacy risks associated with a project and mitigations that may reduce some or all of those risks. In the interests of transparency about data collection and management, the City of Seattle has committed to publishing all PIAs on an outward facing website for public access.

When is a Privacy Impact Assessment Required?

A PIA may be required in two circumstances.

1. When a project, technology, or other review has been flagged as having a high privacy risk.
2. When a technology is required to complete the surveillance impact report process. This is one deliverable that comprises the report.

1.0 Abstract

1.1 Please provide a brief description (one paragraph) of the purpose and proposed use of the project/technology.

Seattle City Light's ("City Light") Current Diversion Team ("CDT") consists of a group of approximately five journey-level engineers who are dispatched to collect data to attempt to determine whether a suspected diversion of current (i.e., alterations to the City Light-owned electrical system by a third-party in order to consume electric power without its being registered by the City Light meter installed for that purpose) has in fact taken place. In support of this mission, the CDT crew uses standard, commercial-grade, unpowered binoculars ("binoculars") to inspect meters and other implicated electrical infrastructure at a distance. If a determination of diversion is sustained, data may be used to respond to lawful requests from the proper law enforcement authorities for evidence for recovering the value of the diverted energy.

In conjunction with this technology, two others – the SensorLink Ampstik device and the SensorLink TMS device – are used by the CDT. As a result, City Light's three retroactive Surveillance Impact Reports ("SIRs") may be, at times, duplicative, so that each report contains the necessary information.

1.2 Explain the reason the project/technology is being created or updated and why the PIA is required.

This technology is used in furtherance of a mission supported by ordinance and an existing City Light department policy procedure (DPP 500 P III-416, hereafter "DPP"). City Light provided the information in the Privacy Impact Assessment to fulfill requirements of the Surveillance Ordinance and so that the public may understand the nature of the CDT and the tools that are essential to its carrying out its mission for the benefit of ratepayers. The binoculars – unpowered, standard, commercial-grade – allow CDT crew members to observe meters and potentially dangerous alterations to the City Light electrical infrastructure.

2.0 Project / Technology Overview

Provide an overview of the project or technology. The overview gives the context and background necessary to understand the purpose, mission and justification for the project / technology proposed.

2.1 Describe the benefits of the project/technology.

As described in Section 1, the CDT utilizes binoculars in order to assess whether suspected diversions of current have occurred and/or are continuing to occur. They also allow City Light to determine the valuation of the energy illegally diverted, which supports City Light's mission of recovering this value for the ratepayers via a process called "back-billing."

2.2 Provide any data or research demonstrating anticipated benefits.

In 2017, the CDT's operations, via the use of binoculars (in combination with the two other technologies under review), City Light recovered $1.6 million. This would otherwise remain a substantial financial loss to the Utility.

2.3 Describe the technology involved.

The binoculars are standard, commercial-grade, unpowered binoculars. They do not contain any special enhancements requiring power (e.g., night-vision or video-recording capabilities). They are used to read a meter from a distance when the CDT is otherwise unable to access physically the meter for the purpose of inspection upon suspected current diversion. CDT crews may also, in the event they have a report of an aggravated case – where there is an electrical system alteration posing a present danger to the public or the electrical system's integrity – observe such alterations.

2.4 Describe how the project or use of technology relates to the department's mission.

The binoculars allow City Light to maintain the integrity of its electricity distribution system, to determine whether suspected current diversions have taken place, and to provide the valuation of the diverted energy to proper authorities for cost recovery. These are supported by ordinance (SMC 21.49.100) and Department Policy and Procedure (DPP).

2.5 Who will be involved with the deployment and use of the project / technology?

The CDT members are the only City Light staff who use the binoculars, and always upon pre-existing and/or reported suspicion of current diversion (e.g., neighbor report, unusual or no energy consumption detected upon a routine meter reading by City Light, visual observation of tampered-with meter or other City Light-owned or maintained electrical equipment). Data derived from observations via binoculars are accessible only by the CDT team.

3.0 Use Governance

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities contracting with the City are bound by restrictions specified in the surveillance ordinance and privacy principles and must provide written procedures for how the entity will comply with any restrictions identified.

3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

The limited number of this equipment and of CDT members makes the routine tracking of the binoculars relatively straight-forward. Binoculars are issued to CDT members, and stored in their official vehicles. These vehicles are operated, locked, and stored in accordance with Utility security procedures.

3.2 List the legal standards or conditions, if any, that must be met before the project / technology is used.

Routine use in support of making an internal determination as to current diversion is not subject to additional prior legal authorization.

3.3 Describe the policies and training required of all personnel operating the project / technology, and who has access to ensure compliance with use and management policies.

In addition to routine privacy and security training undergone by all City Light employees per Seattle IT policy, the CDT manager has responsibility for ensuring compliance with all existing rules and procedures.

4.0 Data Collection and Use

4.1 Provide details about what information is being collected from sources other than an individual, including other IT systems, systems of record, commercial data aggregators, publicly available data and/or other City departments.

No additional information is collected by the CDT in making its determinations, nor is any third-party or other aggregation taking place.

4.2 What measures are in place to minimize inadvertent or improper collection of data?

Risk of inadvertent or improper collection is low. The CDT only investigates specific meters and other implicated electrical equipment at locations previously identified and properly documented as sites of suspected current diversion.

4.3 How and when will the project / technology be deployed or used? By whom? Who will determine when the project / technology is deployed and used?

Binoculars are used throughout the year based on suspected cases of current diversion, by the CDT staff and with the approval of the Current Diversion Coordinator. As mentioned above, these can be triggered in several ways, for example neighbor report to the customer service bureau or other City Light representatives; recognition by billing specialists of highly out-of-the-ordinary meter readings; or observations by meter and other crews of tampering with metering or other electrical service provision equipment.

4.4 How often will the technology be in operation?

CDT crew members use the binoculars for approximately one minute at a time in those cases where an initial investigation has been authorized by the Current Diversion Coordinator, in order to carry out the task of observing a meter and any other implicated electrical equipment.

4.5 What is the permanence of the installation? Is it installed permanently, or temporarily?

Binoculars are not “installed” as they are hand-held and used for approximately one minute at a time.

4.6 Is a physical object collecting data or images visible to the public? What are the markings to indicate that it is in use? What signage is used to determine department ownership and contact information?

Binoculars are not installed, as they are used by hand for approximately one minute at a time. CDT crew members who operate them are deployed in standard City Light-marked vehicles and wear identifying gear. No special notification is made to the public, as doing so may risk defeating its purpose of detecting a diversion of current on a single, previously-suspected service-drop location. As such, the risk of inadvertent capturing of data related to other customers is extremely low.

4.7 How will data that is collected be accessed and by whom?

CDT members, who are journey-level electrical workers trained in the proper use this equipment, may collect these data. These consist of meter reads and, in certain instances, other implicated electrical equipment that poses a present danger to the public or the electrical system integrity.

4.8 If operated or used by another entity on behalf of the City, provide details about access, and applicable protocols.

City Light is the only entity operating or using the technology.

4.9 What are acceptable reasons for access to the equipment and/or data collected?

As described above, binoculars are used only to make determinations about whether a current diversion is likely to be taking place, and, in certain instances, to view implicated and potentially dangerous electrical equipment.

4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

Data obtained by means of binoculars (which consist of notes made by staff based on their binocular-facilitated observations) are stored in a private folder on City Light's digital file locations. The data, as well as overall incident reports, are accessible only by CDT members and its Current Diversion Coordinator.

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

Records of inspections facilitated by use of binoculars are stored in a private folder on City Light's digital file locations, accessible only by CDT members and management.

5.2 How will the owner allow for departmental and other entities, to audit for compliance with legal deletion requirements?

City Light will make CDT file locations and staff available for properly authorized entities wishing to ensure compliance. Data will be retained per City Light records retention schedules.

5.3 What measures will be used to destroy improperly collected data?

Any improperly collected data will be deleted from City Light's digital file locations.

5.4 Which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

The Current Diversion Coordinator has responsibility for this function.

6.0 Data Sharing and Accuracy

6.1 Which entity or entities inside and external to the City will be data sharing partners?

Reports from observations facilitated by the use of binoculars may be shared with other parties in two instances, both of which are public entities. These are (1) when a determination is made that current diversion has taken place, in which case a valuation of the stolen energy is sent to the customer billing division of City Light for "back-billing" to the customer for cost recovery, and (2) when police investigators and/or prosecutors require evidence for further proceedings in complex or aggravated cases, as when large sums of energy have been diverted/stolen, or where there is a safety risk to the public.

6.2 Why is data sharing necessary?

In both cases, this is required for City Light to recoup stolen energy costs. In the second case (information sharing with police investigators) it may also be required to protect public safety, since unauthorized alterations to the electrical system can pose a serious and at times lethal danger to the public.

6.3 Are there any restrictions on non-City data use?

Yes ☒ No ☐

6.3.1 If you answered yes, provide a copy of the department's procedures and policies for ensuring compliance with these restrictions.

Data are collected and maintained for Seattle City Light use and may only be shared with outside entities for the purposes of law enforcement or legal action by the relevant jurisdictional authority. This policy is formally laid out in Seattle City Light Department Policy & Procedure DPP 500 P III-416.

6.4 How does the project/technology review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?

City Light anticipates no additional data-sharing, as the CDT's mission is fixed. Additional changes would require review the Current Diversion Coordinator. Law enforcement, as mentioned in 6.3, may request these data and findings but only pursuant to a subpoena or a request pursuant to the Public Disclosure Law (based upon probable cause, see RCW 42.56.335).

6.5 Explain how the project/technology checks the accuracy of the information collected. If accuracy is not checked, please explain why.

As the binoculars are unpowered, standard binoculars, this section does not apply.

6.6 Describe any procedures that allow individuals to access their information and correct inaccurate or erroneous information.

Upon a proper finding of current diversion, customers are back-billed to recoup these losses. DPP 500 P III-416 provides that "all customers shall receive uniform consideration and courtesy in all matters involving actual or suspected current diversion." Customers are notified of findings and offered opportunities to respond and/or object.

7.0 Legal Obligations, Risks and Compliance

7.1 What specific legal authorities and/or agreements permit and define the collection of information by the project/technology?

One of City Light's core missions as an electric utility is to recoup the costs of the energy it provides to its customers as part of its operations, as required in SMC 21.49.100.

7.2 Describe what privacy training is provided to users either generally or specifically relevant to the project/technology.

CDT members are trained in how to store information in private folders on City Light's digital storage locations, in addition to the general privacy and security training required by Seattle IT.

7.3 Given the specific data elements collected, describe the privacy risks identified and for each risk, explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

With binoculars, crews observe meters and other equipment that may indicate current diversion. Although there is some risk that crews may observe individuals or other customers' equipment, these locations (1) are in public view and (2) are not digitally recorded.

7.4 Is there any aspect of the project/technology that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?

City Light has considered but does not anticipate such objections, since the data collected are used for one purpose only.

8.0 Monitoring and Enforcement

8.1 Describe how the project/technology maintains a record of any disclosures outside of the department.

When a report is sent to law enforcement, it does not include power consumption information. Law enforcement then relies upon the Public Disclosure Law to request power records, if they decide to do so, and City Light would provide that information pursuant to that request. This may be effectuated either by a subpoena or by a request from law enforcement based upon probable cause and pursuant to the Washington Public Disclosure Law (see RCW 42.56.335).

8.2 What auditing measures are in place to safeguard the information, and policies that pertain to them, as well as who has access to the audit data? Explain whether the project/technology conducts self-audits, third party audits or reviews.

To safeguard the information, the Current Diversion Coordinator will request Seattle IT to provide audit data, so that City Light may complete an audit to ensure that access rights are assigned only those who should have access to the shared drive containing customer/current-diversion data.

Financial Information

Purpose

This section provides a description of the fiscal impact of the surveillance technology, as required by the surveillance ordinance.

1.0 Fiscal Impact

Provide a description of the fiscal impact of the project/technology by answering the questions below.

1.1 Current or potential sources of funding: initial acquisition costs.

Current ☒ potential ☐

Date of initial acquisition	Date of go live	Direct initial acquisition cost	Professional services for acquisition	Other acquisition costs	Initial acquisition funding source
2014	Same	N/A	None	None	City Light

Notes:

None.

1.2 Current or potential sources of funding: on-going operating costs, including maintenance, licensing, personnel, legal/compliance use auditing, data retention and security costs.

Current ☒ potential ☐

Annual maintenance and licensing	Legal/compliance, audit, data retention and other security costs	Department overhead	IT overhead	Annual funding source
N/A	N/A	N/A	N/A	N/A

Notes:

None.

1.3 Cost savings potential through use of the technology

In 2017, through the use of the Current Diversion Team's technologies – including binoculars – City Light was able to recover $1.6 million in stolen energy costs.

1.4 Current or potential sources of funding including subsidies or free products offered by vendors or governmental entities

None identified.

Expertise and References

Purpose

The following information is provided to ensure that Council has a group of experts to reference while reviewing the completed surveillance impact report ("SIR"). Any individuals or agencies referenced must be made aware ahead of publication that their information has been included. All materials must be available for Council to access or review, without requiring additional purchase or contract.

1.0 Other Government References

Please list any other government bodies that have implemented this technology and can speak to the implementation of this technology.

Agency, municipality, etc.	Primary contact	Description of current use
N/A	N/A	N/A

2.0 Academics, Consultants, and Other Experts

Please list any experts in the technology under consideration, or in the technical completion of the service or function the technology is responsible for.

Agency, municipality, etc.	Primary contact	Description of current use
N/A	N/A	N/A

3.0 White Papers or Other Documents

Please list any authoritative publication, report or guide that is relevant to the use of this technology or this type of technology.

Title	Publication	Link
N/A	N/A	N/A

Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet

Purpose

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit ("RET") in order to:

- Provide a framework for the mindful completion of the SIR in a way that is sensitive to the historic exclusion of vulnerable and historically underrepresented communities. Particularly, to inform the public engagement efforts departments will complete as part of the surveillance impact report.
- Highlight and mitigate any impacts on racial equity from the adoption and the use of the technology.
- Highlight and mitigate any disparate impacts on individuals or vulnerable communities.
- Fulfill the public engagement requirements of the surveillance impact report.

Adaptation of the RET for Surveillance Impact Reports

The RET was adapted for the specific use by the Seattle Information Technology Departments' ("Seattle IT") Privacy Team, the Office of Civil Rights ("OCR"), and Change Team members from Seattle IT, Seattle City Light, Seattle Fire Department, Seattle Police Department, and Seattle Department of Transportation.

Racial Equity Toolkit Overview

The vision of the Seattle Race and Social Justice Initiative ("RSJI") is to eliminate racial inequity in the community. To do this requires ending individual racism, institutional racism and structural racism. The RET lays out a process and a set of questions to guide the development, implementation and evaluation of policies, initiatives, programs, and budget issues to address the impacts on racial equity.

1.0 Set Outcomes

1.1. Seattle City Council has defined the following inclusion criteria in the surveillance ordinance, and they serve as important touchstones for the risks departments are being asked to resolve and/or mitigate. Which of the following inclusion criteria apply to this technology?

☐ The technology disparately impacts disadvantaged groups.

☐ There is a high likelihood that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service.

☒ The technology collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection.

☐ The technology raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice.

1.2 What are the potential impacts on civil liberties through the implementation of this technology? How is the department mitigating these risks?

Because the binoculars, in conjunction with the other two diversion technologies being reviewed, are designed to measure electric current at one connection point assigned to one customer, no impacts on civil liberties are anticipated from the technologies themselves. At the same time, City Light is aware that the methods and procedures surrounding the use or installation of an otherwise non-offensive technology is just as important. For that reason, we ensure that our staff are clearly identified as Seattle City Light employees when in the field; there is no surreptitious operation in the field.

1.3 What are the risks for racial or ethnicity-based bias through each use or deployment of this technology? How is the department mitigating these risks?

Include a description of any issues that may arise such as algorithmic bias or the possibility for ethnic bias to emerge in people and/or system decision-making.

City Light is committed to equitable enforcement of all its legal mandates, in the same way that it is committed to equity in its provision of clean, affordable, and reliable power for its customers. City Light aims to ensure that the enforcement mechanisms similarly equitable, in that they should be not only unbiased but also equitably enforced. For that reason, City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible.

1.4 Where in the City is the technology used or deployed?

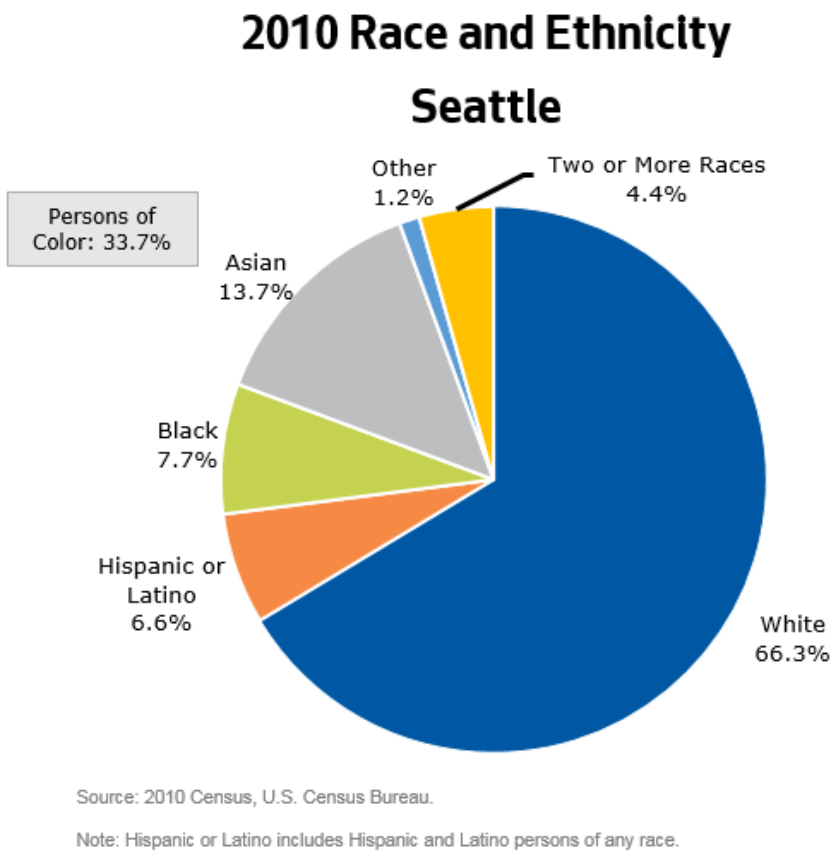
☒ all Seattle neighborhoods

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County.

If possible, please include any maps or visualizations of historical deployments / use.

Seattle City Light's service territory extends beyond the boundary of the City of Seattle. Other areas include: Burien, Lake Forest Park, Normandy Park, Renton, SeaTac, Shoreline, Tukwila, and areas of unincorporated King County.

1.4.1 What are the racial demographics of those living in this area or impacted by these issues?



1.4.2 How does the Department to ensure diverse neighborhoods, communities, or individuals are not specifically targeted through the use or deployment of this technology?

DPP 500 P III-416 provides that "all customers shall receive uniform consideration and courtesy in all matters involving actual or suspected current diversion." City Light aims to ensure that the enforcement mechanisms are equitable, in that they should be not only unbiased but also equitably enforced. For that reason, City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible.

1.5 How do decisions around data sharing have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

Data is collected for Seattle City Light use and may only be shared with outside entities for the purposes of law enforcement or legal action by the relevant jurisdictional authority. This policy is formally laid out in Seattle City Light Department Policy & Procedure DPP 500 P III-416. As stated previously, City Light aims to ensure that the enforcement mechanisms are equitable, in that they should be not only unbiased but also equitably enforced. For that reason, City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible.

1.6 How do decisions around data storage and retention have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

Data is maintained for Seattle City Light use and may only be shared with outside entities for the purposes of law enforcement or legal action by the relevant jurisdictional authority. This policy is formally laid out in Seattle City Light Department Policy & Procedure DPP 500 P III-416. As stated previously, City Light aims to ensure that the enforcement mechanisms are equitable, in that they should be not only unbiased but also equitably enforced. For that reason, City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible.

1.7 What are potential unintended consequences (both negative and positive potential impact)? What proactive steps can you can / have you taken to ensure these consequences do not occur.

One of City Light's core missions as an electric utility is to recoup the costs of the energy it provides to its customers as part of its operations (as required in SMC 21.49.100 and the general rule against gifts of public funds found in the Washington State Constitution at Article VIII, Section 7). Per DPP 500 P III-416,"all customers shall receive uniform consideration and courtesy in all matters involving actual or suspected current diversion." As stated previously, City Light aims to ensure that the enforcement mechanisms are equitable, in that they should be not only unbiased but also equitably enforced. For that reason, City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible.

2.0 Public Outreach

2.1 Organizations who received a personal invitation to participate.

Please include a list of all organizations specifically invited to provide feedback on this technology.

1. ACLU of Washington	2. Ethiopian Community Center	3. Planned Parenthood Votes Northwest and Hawaii
4. ACRS (Asian Counselling and Referral Service)	5. Faith Action Network	6. PROVAIL
7. API Chaya	8. Filipino Advisory Council (SPD)	9. Real Change
10. API Coalition of King County	11. Friends of Little Saigon	12. SCIPDA
13. API Coalition of Pierce County	14. Full Life Care	15. Seattle Japanese American Citizens League (JACL)
16. CAIR	17. Garinagu HounGua	18. Seattle Neighborhood Group
19. CARE	20. Helping Link	21. Senior Center of West Seattle
22. Central International District Business Improvement District	23. Horn of Africa	24. Seniors in Action
25. Church Council of Greater Seattle	26. International ImCDA	27. Somali Family Safety Task Force
28. City of Seattle Community Police Commission (CPC)	29. John T. Williams Organizing Committee	30. South East Effective Development
31. City of Seattle Community Technology Advisory Board	32. Kin On Community Health Care	33. South Park Information and Resource Center SPIARC
34. City of Seattle Human Rights Commission	35. Korean Advisory Council (SPD)	36. STEMPaths Innovation Network
37. Coalition for Refugees from Burma	38. Latina/o Bar Association of Washington	39. University of Washington Women's Center
40. Community Passageways	41. Latino Civic Alliance	42. United Indians of All Tribes Foundation
43. Council of American Islamic Relations - Washington	44. LELO (Legacy of Equality, Leadership, and Organizing)	45. Urban League
46. East African Advisory Council (SPD)	47. Literacy Source	48. Wallingford Boys & Girls Club
49. East African Community Services	50. Millionair Club Charity	51. Washington Association of Criminal Defense Lawyers
52. Education for All	53. Native American Advisory Council (SPD)	54. Washington Hall
55. El Centro de la Raza	56. Northwest Immigrant Rights Project	57. West African Community Council
58. Entre Hermanos	59. OneAmerica	60. YouthCare
61. US Transportation expertise	62. Local 27	63. Local 2898
64. (SPD) Demographic Advisory Council	65. South Seattle Crime Prevention Coalition (SSCPC)	66. CWAC
67. NAAC		

2.2 Additional Outreach Efforts

Department	Outreach Area	Description
ITD	Social Media Outreach Plan: Twitter	Directed Tweets and Posts related to Open Public Comment Period for Group 2 Technologies, as well as the BKL event.
SPD, SFD, OPCD, OCR, SPL, SDOT, SPR, SDCI, SCL, OLS, Seattle City Council	Social Media Outreach Plan: Twitter	Tweets and Retweets regarding Group 2 comment period and/or BKL event.
ITD	Press Release	Press release sent to several Seattle media outlets.
ITD	Ethnic Media Press Release	Press Release sent to specific ethnic media publications.
ITD	Social Media Outreach Plan: Facebook Event Post	Seattle IT paid for boosted Facebook posts for their BKL event.
ITD	CTAB	Presented and utilized the Community Technology Advisory Board (CTAB) network and listserv for engaging with interested members of the public
ITD	Blog	Wrote and published a Tech Talk blog post for Group 2 technologies, noting the open public comment period, BKL event, and links to the online survey/comment form.
ITD	Technology Videos	Seattle IT worked with the Seattle Channel to produce several short informational/high level introductory videos on group 2 technologies, which were posted on seattle.gov/privacy. And used at a number of Department of Neighborhoods-led focus groups.

2.3 Scheduled public meeting(s).

Meeting notes, sign-in sheets, all comments received, and questions from the public will be included in Appendix B, C, D, E, F, G, H and I. Comment analysis will be summarized in section 3.0 Public Comment Analysis.

Location	Bertha Knight Landes Room, 1st Floor City Hall 600 4th Avenue, Seattle, WA 98104
Time	February 27, 2018; 6 p.m. – 8 p.m.
Capacity	100+
Link to URL Invite	BKL Event Invitation

2.4 Scheduled focus Group Meeting(s)

Meeting 1

Community Engaged	Council on American-Islamic Relations - Washington (CAIR-WA)
Date	Thursday, February 21, 2019

Meeting 2

Community Engaged	Entre Hermanos
Date	Thursday, February 28, 2019

Meeting 3

Community Engaged	Byrd Barr Place
Date	Thursday, February 28, 2019

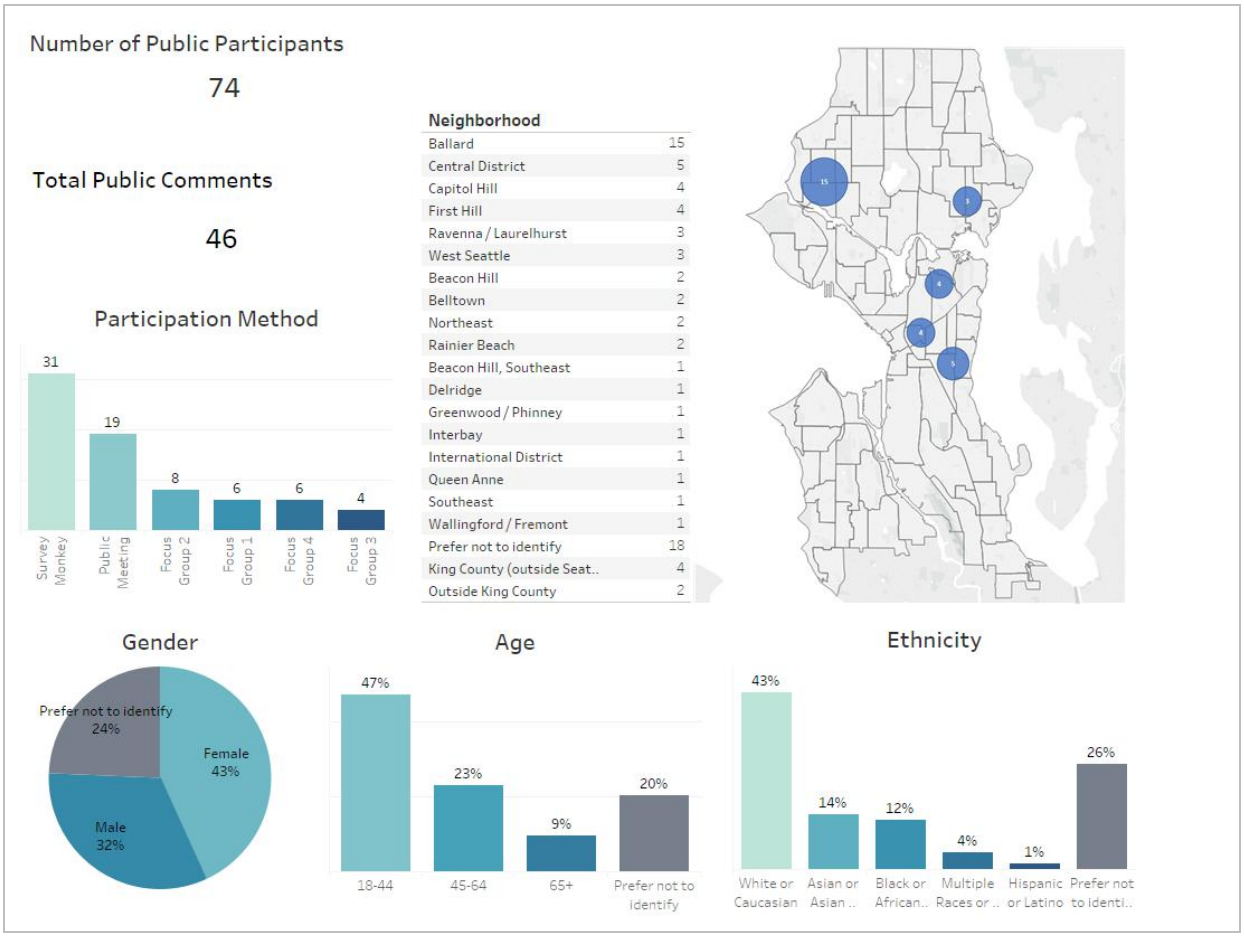
Meeting 4

Community Engaged	Friends of Little Saigon
Date	Wednesday, February 27, 2019

3.0 Public Comment Analysis

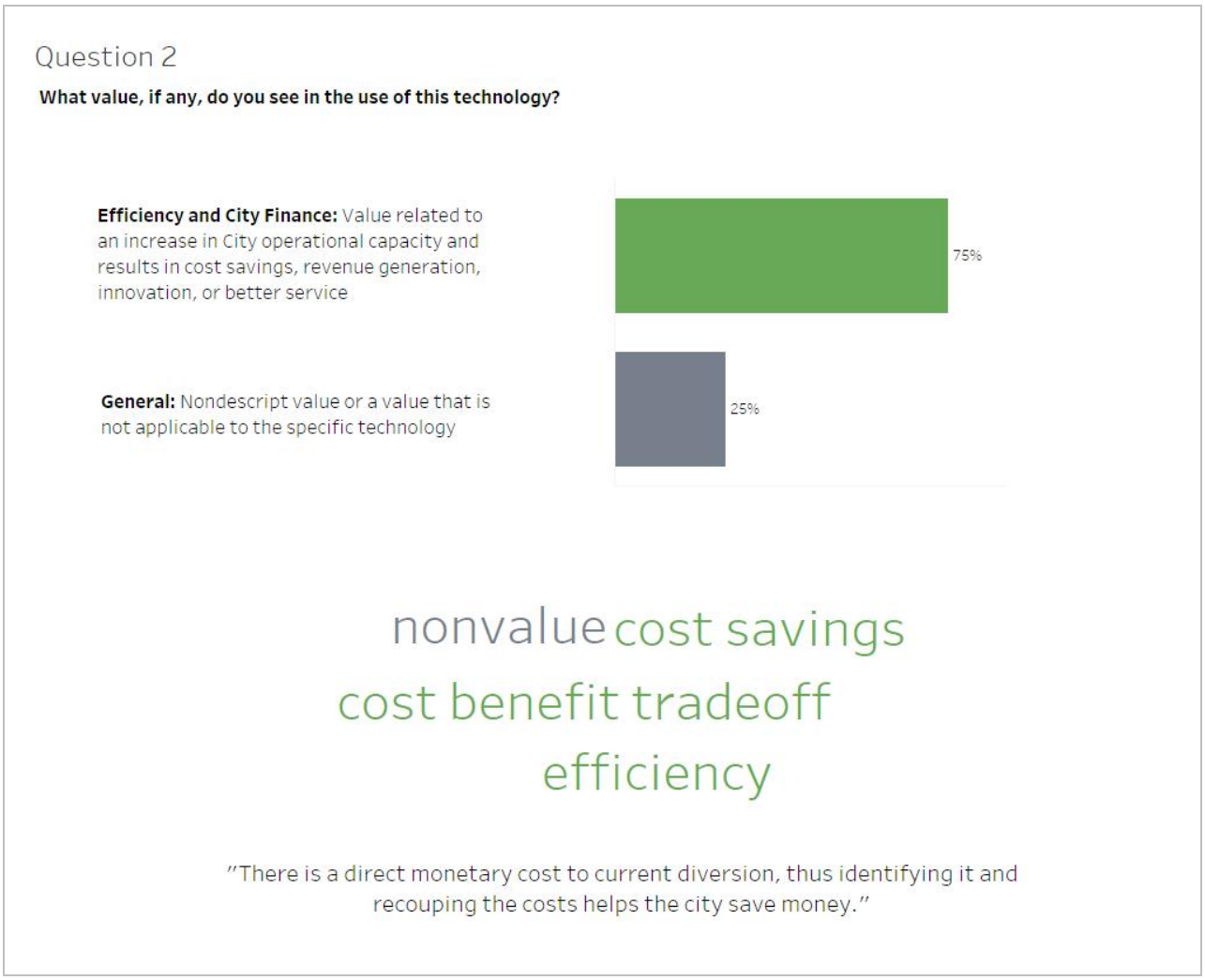
Please note, due to the nature of the comments received and the related purpose of the Seattle City Light technologies, this comment analysis reflects comments received for the SCL Binoculars/Spotting Scope, SensorLink Amp Fork, and Check Meter Device.

3.1 Summary of Response Volume



3.2 Question One: What concerns, if any, do you have about the use of this technology?

3.3 Question Two: What value, if any, do you see in the use of this technology?



3.4 Question Three: What do you want City leadership to consider about the use of this technology?

Question 3

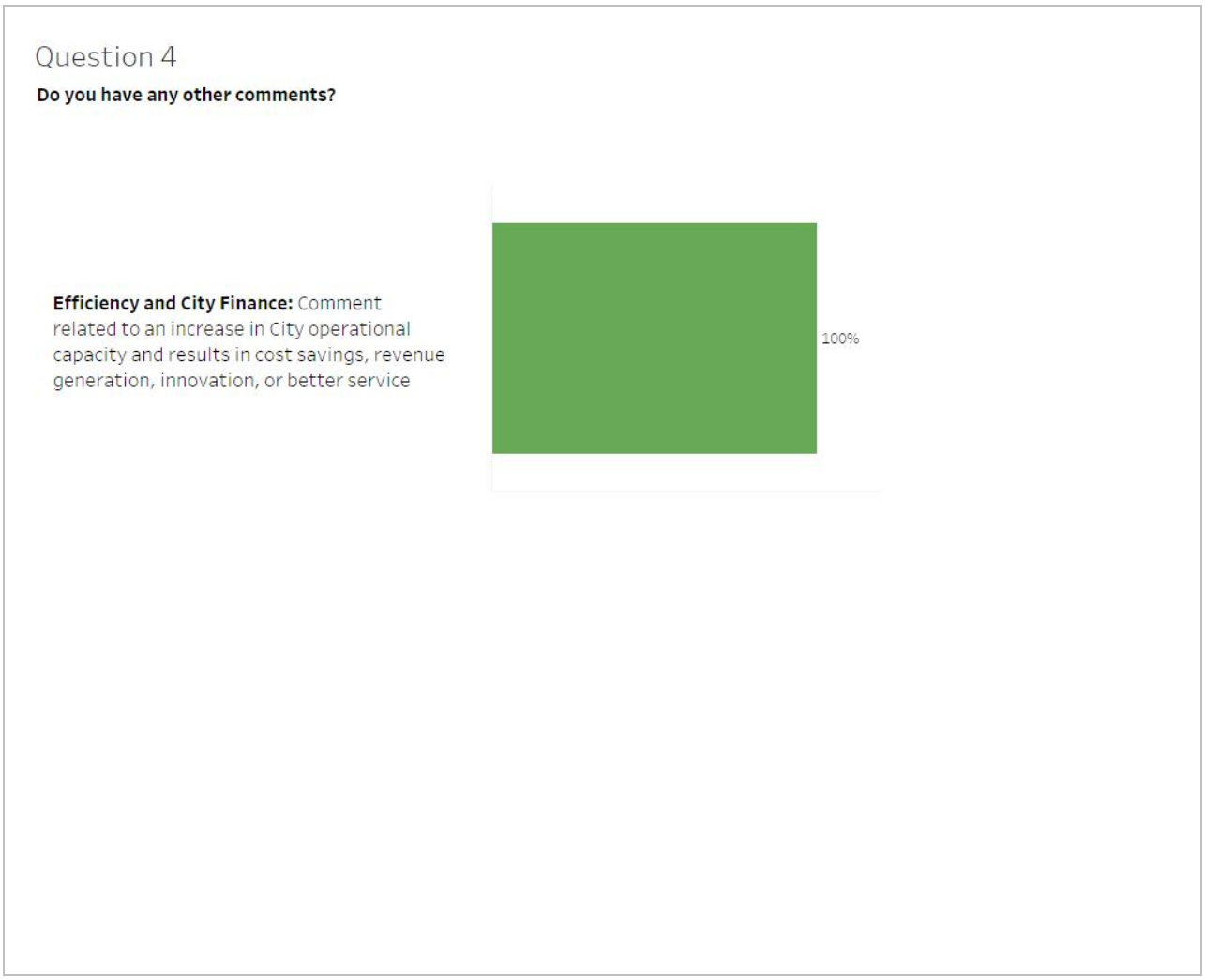
What do you want City leadership to consider about the use of this technology?

Increase policy, enforcement, and oversight: Recommendations related to department and City policy, oversight, accountability, transparency, audit, and policy enforcement.

oversight
reporting statisticscease use

"City leadership should specifically inquire as to what percentage of people/households that were enforcement locations would also be considered low-income. If that percentage is high, then that likely means SCL may cause people to be jailed for effectively being poor (and resourceful); and SCL may have inadequate support offerings for people who are low-income."

3.5 Question Four: Do you have any other comments?



4.0 Equity Annual Reporting

4.1 What metrics for this technology be reported to the CTO for the annual equity assessments?

Seattle City Light is currently working to finalize these metrics.

Privacy and Civil Liberties Assessment

Purpose

This section shall be completed after public engagement has concluded and the department has completed the racial equity toolkit section above. The privacy and civil liberties assessment is completed by the community surveillance working group ("working group"), per the surveillance ordinance which states that the working group shall:

"Provide to the executive and the City Council a privacy and civil liberties impact assessment for each SIR that must be included with any departmental request for surveillance technology acquisition or in-use approval. The impact assessment shall include a description of the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities. The CTO shall share with the working group a copy of the SIR that shall also be posted during the period of public engagement. At the conclusion of the public engagement period, the CTO shall share the final proposed SIR with the working group at least six weeks prior to submittal of the SIR to Council for approval. The working group shall provide its impact assessment in writing to the executive and the City Council for inclusion in the SIR within six weeks of receiving the final proposed SIR. If the working group does not provide the impact assessment before such time, the working group must ask for a two-week extension of time to City Council in writing. If the working group fails to submit an impact statement within eight weeks of receiving the SIR, the department and City Council may proceed with ordinance approval without the impact statement."

Working Group Privacy and Civil Liberties Assessment

The Working Group's Privacy and Civil Liberties Impact Assessment for this technology is below, and is also included in the Ordinance submission package, available as an attachment.

From: Seattle Community Surveillance Working Group (CSWG) To: Seattle City Council

Date: June 4, 2019

Re: Privacy and Civil Liberties Impact Assessment for Check Meter Device, SensorLink Amp Fork, and Binoculars/Spotting Scope (Current Diversion Technologies, SDOT)

Executive Summary

On April 25, 2019, the CSWG received the Surveillance Impact Reports (SIRs) on three Current Diversion Technologies (Check Meter Device, SensorLink Amp Fork, and Binoculars/Spotting Scope) used by Seattle City Light (SCL) included in Group 2 of the Seattle Surveillance Ordinance technology review process. This document is CSWG's Privacy and Civil Liberties Impact Assessment for these technologies as set forth in SMC 14.18.080(B)(1), which we provide for inclusion in the final SIRs submitted to the City Council.

This document first provides recommendations in this executive summary, then provides background information, key concerns, and outstanding questions on the current diversion technologies.

Our assessment of the three current diversion technologies (Check Meter Device, SensorLink Amp Fork, and Binoculars/Spotting Scope) focuses on two key issues:

(1) The use of these systems and the data collected by them for purposes other than those intended;
(2) Over-collection and over-retention of data.

While the stated purposes of the three current diversion technologies may be relatively innocuous, it is important to note that these technologies may be used to gather identifying information about individuals. Particularly in the absence of written, explicit policies governing what these technologies can and cannot be used for, the data collected by these technologies may compromise the privacy of individuals and may be misused to target individuals and communities. It is important that these technologies have explicit protections limiting the use of these tools to their intended purpose.

Recommendations

We recommend that the Council and SCL adopt clear and enforceable rules that ensure, at a minimum, the following:

(1) Define purpose of use for each technology and restrict its use to that purpose.
(2) Ensure there are clear data protection policies to safeguard stored data.
(3) Ensure the deletion of data collected by the technology immediately after the relevant current diversion investigation has closed.

Background on the Three Current Diversion Technologies

The Check Meter Device, the SensorLink Amp Fork, and the Binoculars/Spotting Scope are technologies used by SCL's Current Diversion Team to investigate when electricity is being used without being paid for.

The Check Meter Device is a device that measures the amount of electrical energy flowing through a service-drop wire over time. It digitally captures the information for later retrieval by the Current Diversion Team member(s) via a wireless protocol. These devices are typically installed on an electric pole adjacent to a transformer for a period of one week to one month. The stated purpose of this technology is to determine the valuation of the energy illegally diverted.

The SensorLink Amp Fork is a hand-held electrical device used to detect current flow. It is mounted on an extensible pole (up to 40' to 50') that allows a circular clamp to be placed around a wire. The device then displays instantaneous readings of the amount of electrical energy flow. The Current Diversion Team member may then compare those reads against the readings displayed on the electric meter, allowing staff to determine if current is being diverted.

The Binoculars/Spotting Scope is a device used to determine if current diversion is taking place when distance is a barrier to physical inspection. Binoculars may also be used to determine if potentially dangerous alterations to City Light's electrical infrastructure exist. The relevant SIR states that the binoculars do not collect data, and do not contain any special enhancements requiring power (e.g., night vision or video-recording capabilities).[1]

Key Concerns Regarding all Three Current Diversion Technologies

Seattle City Light's policy:

(1) **Does not include explicit, written restrictions on use.** An April 3, 2019 email from Seattle City Light to the ACLU stated that "Seattle City Light does not have any formal, explicit, written policies on what the technologies can be used for."[2] The email states that Section 3.0 (Use Governance) of the SIRs describes SCL's standards, but this section does not contain meaningful restrictions on use. The absence of written, specific policies increases the risk of misuse.

(2) **Does not include specific data protection provisions.** For example, the draft SIR for the Check Meter Device (SensorLink Transformer Meter System) says that the data is retrieved from the device "via secure radio protocol," but the SIR does not explain further. Radio frequencies are not inherently secure, so the policy should define how this data is secured, including when it is on the Check Meter Device and once it is stored off the device.

(3) **Includes an unjustifiably long data retention period.** According to Seattle City Light, the retention period for current diversion data collected is at least 6 years.[3] Such a lengthy retention period for electricity diversion investigation records is unnecessary. Data should be deleted as soon as an investigation is closed.

In addition, all three SIRs state: "City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible." This equity analysis should be provided for public review.

[1] 2019 Surveillance Impact Report SCL Check Meter Device, pages 3-6.

[2] See pages 3-4 for Seattle City Light Response to ACLU-WA on April 3, 2019.

[3] Ibid.

City of Seattle

Seattle City Light

700 5th Ave. | P.O. Box 34023 | Seattle WA 98124-4023
TEL (206) 684-3000 TTY/TDD (206) 684-3225 FAX (206) 625-3709
seattle.gov/light
twitter.com/SEACityLight facebook.com/SeattleCityLight

April 3, 2019

Shankar Narayan, Technology and Liberty Project Director
Jennifer Lee, Technology and Liberty Project Advocate
American Civil Liberties Union – Washington
901 Fifth Ave, Suite 630
Seattle, WA 98164

Dear Shankar and Jennifer,

We have received your letter dated March 20, 2019 with comments on the three Seattle City Light technologies included in Group 2 of the Seattle Surveillance Ordinance process. We appreciate your feedback, which will be considered as the Surveillance Impact Reports (SIRs) are finalized.

In the meantime, I can offer the below information related to your two questions:

What enforceable policies, if any, apply to use of these three technologies?

Current Diversion Detection Technology Policies: Seattle City Light does not have any formal, explicit, written policies on what the technologies can be used for. However, City Light's draft 2019 Surveillance Impact Reports (SIRs) outline the non-written standards for use of the technologies. Please refer to Section 3.0, "Use Governance," of the attached SIRs for the three current diversion technologies, as they describe City Light's standards.

Also, please know that City Light has formally adopted a Department Policy & Procedure (DPP P III-416, "Current Diversion") governing the prevention, detection, reporting, investigation, and correction of illegal, unauthorized, or inadvertent diversions of electric current, and the recovery of associated lost revenues and costs. Please see the attached DPP.

What is Seattle City Light's data retention schedule?

City Light follows the record retention period presented in the following chart.

An equal employment opportunity, affirmative action employer. Accommodations for people with disabilities provided upon request.

Retention Schedule	Series Title and Description	DAN #	Retention and Disposition Action (Primary Record Copy)	Designation
Utility Services Power Distribution	ELECTRICITY DIVERSION INVESTIGATION RECORDS Inquiry regarding problems or discrepancies with meters, either from meter reader or other parties. Investigation records may include: site visit dates, notes regarding location, pictures of meter or surrounding area, consumption history, special meter read, and service order for technical support.	UT55-05G-07 Rev. 0	Investigation closed plus 6 years	Non-Archival Non-Essential OPR

Please let me know if you have additional questions.

Sincerely,

Julie Moore
Public Information Officer
Seattle City Light

City of Seattle

CTO Response

Memo

Date: 11/17/2020

To: Seattle City Council, Transportation and Utilities Committee

From: Saad Bashir

Subject: CTO Response to the Surveillance Working Group SCL Current Diversion Technologies SIR Review

---

To the Council Transportation and Utilities Committee,

I look forward to continuing to work together with Council and City departments to ensure transparency about the use of surveillance technologies and finding a mutually agreeable means to use technology to improve City services while protecting the privacy and civil rights of the residents we serve. Specific concerns in the Working Group comments about SCL's Current Diversion Technologies are addressed in the attached document.

As provided in the Surveillance Ordinance, SMC 14.18.080, this memo outlines the Chief Technology Officer's (CTO's) response to the Surveillance Working Group assessment on the Surveillance Impact Report for Seattle City Light's Current Diversion Technologies, including the Check Meter Device, SensorLink Amp Fork, and Binoculars/Spotting Scope.

Background

The Information Technology Department (ITD) is dedicated to the Privacy Principles and Surveillance Ordinance objectives to provide oversight and transparency about the use and acquisition of specialized technologies with potential privacy and civil liberties impacts. All City departments have a shared mission to protect lives and property while balancing technology use and data collection with negative impacts to individuals. This requires ensuring the appropriate use of privacy invasive technologies through technology limitations, policy, training and departmental oversight.

The CTO's role in the SIR process has been to ensure that all City departments are compliant with the Surveillance Ordinance requirements. As part of the review work for surveillance technologies, ITD's Privacy Office has facilitated the creation of the Surveillance Impact Report documentation, including collecting comments and suggestions from the Working Group and members of the public about these technologies. IT and City departments have also worked collaboratively with the Working Group to answer additional questions that came up during their review process.

Technology Purpose

Seattle City Light's Current Diversion Team (CDT) consists of a group of approximately five journey-level engineers who are dispatched to collect data to attempt to determine whether a suspected diversion of current (i.e., alterations to the City Light-owned electrical system by a third-party in order to consume electric power without it being registered by the City Light meter installed for that purpose) has taken

place. Diversion alterations can result in injury to people and can damage SCL equipment and Infrastructure. Further, SCL is required by law (SMC 21.49.100) to collect payment for utility use and so investigates and remediates any loss of payment created by such situations.

In support of this mission, the CDT crew uses a Check Meter Device, SensorLink Amp Fork, and Binoculars/Spotting Scope. If a determination of diversion is sustained, data may be used to respond to lawful requests from the proper law enforcement authorities for evidence for recovering the value of the diverted energy.

Working Group Concerns

In their review, the Working Group has raised concerns about these Current Diversion Technologies being used in a privacy impacting way, including use of these systems for other than their stated purpose, and over-collection and over-retention of the data collected.

1) The use of these systems and the data collected by them for purposes other than those intended.
2) Over-collection and over-retention of data.

The policy and training enacted by SCL and limitations from the technologies themselves provide adequate mitigation for the potential privacy and civil liberties concerns raised by the Working Group about the use of this important operational technology.

Response to Specific Concerns: SCL Current Diversion Technologies

Concern: Use of these systems and the data collected by them for purposes other than those intended.

CTO Assessment: SCL's Department Policy & Procedure, DPP P III-416 outlines the process for determining why and how the department investigates suspected current diversion. This policy includes how evidence (such as data collected from current diversion technologies) must be handled and who is authorized to receive a report. Some of the technologies are not capable of sharing data outside of additional manual observations, and any data as a part of the investigation is securely stored and only accessible by members of the Current Diversion Team. This body of policy and operational documentation provides detail about how the technology is used and how any data collected is managed, and it is our assessment that the documentation provides adequate protections.

SIR Response:
Check Meter Device
Section 3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

"The CDT owns six SensorLink TMS units, which are deployed on the basis of case number and need. Deployment level on a given case can vary from none (zero) to all (six). Once a case is properly opened, CDT crew members may check them out without prior additional authorization, though the Current Diversion Coordinator is under nearly all circumstances aware of deployment due to position

responsibilities. Serial numbers are recorded and the CDT member to whom they are assigned, as well as their deployment status, are logged."

Section 4.2 What measures are in place to minimize inadvertent or improper collection of data?

"Risk of inadvertent or improper collection is low for two reasons. First, the CDT only investigates specific, metered locations previously identified and properly documented as sites of suspected current diversion. And second, SensorLink TMS devices are used only on those service-drop lines that are delivering electrical service to the suspected location."

Amp Fork

Section 3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

"The limited number of this equipment and of CDT members makes the routine tracking of the Ampstik devices relatively straight-forward. Ampstiks are issued to CDT members, and stored in their official vehicles. These vehicles are operated, locked, and stored in accordance with Utility security procedures. Ampstiks' serial numbers are recorded and the CDT member to whom they are assigned, as well as their deployment status, are logged."

Section 4.2 What measures are in place to minimize inadvertent or improper collection of data?

"Risk of inadvertent or improper collection is low for two reasons. First, the CDT only investigates specific, metered locations previously identified as sites of suspected current diversion. And second, Ampstik devices are used only on those service-drop lines that are delivering electrical service to the suspected location."

Binoculars

Section 3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

"The limited number of this equipment and of CDT members makes the routine tracking of the binoculars relatively straight-forward. Binoculars are issued to CDT members, and stored in their official vehicles. These vehicles are operated, locked, and stored in accordance with Utility security procedures."

Section 4.2 What measures are in place to minimize inadvertent or improper collection of data?

"Risk of inadvertent or improper collection is low. The CDT only investigates specific meters and other implicated electrical equipment at locations previously identified and properly documented as sites of suspected current diversion."

Concern: Data Protection Policies

CTO Assessment: The data storage location and access controls are adequate for protecting information collected by these technologies during current diversion investigations. All users that have access to this data have an authorized and specified use for the data. For those devices that are capable of collecting data, none is retained on the device, and any data stored would be kept in line with the department retention policy.

SIR Response:

Check Meter Device

Section 4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

"Data obtained by means of the SensorLink TMS device are stored in a private folder on City Light's digital file locations, accessible only by CDT members and management. Data stored in the SensorLink TMS device itself are deleted after its observations are retrieved by the CDT and/or upon its removal from the electrical pole (i.e., no data remain on the SensorLink TMS once its use for a given determination of current diversion has been completed and before it is therefore made available to other CDT staff for subsequent deployment)."

Amp Fork

Section 4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

"Data obtained by means of the Ampstik are stored in a private folder on City Light's digital file locations. The data, as well as incident reports, are accessible only by CDT members and its Current Diversion Coordinator."

Binoculars

Section 4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

"Data obtained by means of binoculars (which consist of notes made by staff based on their binocular-facilitated observations) are stored in a private folder on City Light's digital file locations. The data, as well as overall incident reports, are accessible only by CDT members and its Current Diversion Coordinator."

Concern: Overcollection and over retention of data

CTO Assessment: SCL follows legally required retention periods that ensure that only data that is necessary to complete an investigation is preserved after the investigation in case of any dispute. The data is protected and only accessible by those who are related to the investigation

SIR Response:
Check Meter Device
Section 4.7 How will data that is collected be accessed and by whom?

"CDT members, who are journey-level electrical workers trained in the placement, use, and removal of the SensorLink TMS device, may collect this data. The quantitative data – accumulated consumption (in kilowatt-hours), average volts (current strength), average amps (current flow), and interval consumption (in kilowatt-hours per a pre-defined time-unit) – are accessed by CDT crew members remotely using a secure radio protocol and a specific, password-protected software program, known as Steelhead."

Section 4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

"Data obtained by means of the SensorLink TMS device are stored in a private folder on City Light's digital file locations, accessible only by CDT members and management. Data stored in the SensorLink TMS device itself are deleted after its observations are retrieved by the CDT and/or upon its removal from the electrical pole (i.e., no data remain on the SensorLink TMS once its use for a given determination of current diversion has been completed and before it is therefore made available to other CDT staff for subsequent deployment)."

Amp Fork
Section 4.7 How will data that is collected be accessed and by whom?

"CDT members, who are journey-level electrical workers trained in the use of the Ampstik, may collect and access this data. Additionally, the Current Diversion Coordinator may access the data."

Section 4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

"Data obtained by means of the Ampstik are stored in a private folder on City Light's digital file locations. The data, as well as incident reports, are accessible only by CDT members and its Current Diversion Coordinator."

Binoculars
Section 4.7 How will data that is collected be accessed and by whom?

"CDT members, who are journey-level electrical workers trained in the proper use this equipment, may collect these data. These consist of meter reads and, in certain instances, other implicated electrical equipment that poses a present danger to the public or the electrical system integrity."

Section 4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

"Data obtained by means of binoculars (which consist of notes made by staff based on their binocular-facilitated observations) are stored in a private folder on City Light's digital file locations. The data, as well as overall incident reports, are accessible only by CDT members and its Current Diversion Coordinator."

SCL's Required Retention period

Retention Schedule	**Series Title and Description**	**DAN #**	**Retention and Disposition Action (Primary Record Copy)**	**Designation**
Utility Services Power Distribution	ELECTRICITY DIVERSION INVESTIGATION RECORDS Inquiry regarding problems or discrepancies with meters, either from meter reader or other parties. Investigation records may include: site visit dates, notes regarding location, pictures of meter or surrounding area, consumption history, special meter read, and service order for technical support.	UT55-05G-07 Rev. 0	Investigation closed plus 6 years	Non-Archival Non-Essential OPR

Appendix A: Glossary

Accountable: (taken from the racial equity toolkit.) Responsive to the needs and concerns of those most impacted by the issues you are working on, particularly to communities of color and those historically underrepresented in the civic process.

Community outcomes: (taken from the racial equity toolkit.) The specific result you are seeking to achieve that advances racial equity.

Contracting equity: (taken from the racial equity toolkit.) Efforts to achieve equitable racial outcomes in the way the City spends resources, including goods and services, consultants and contracting.

DON: "department of neighborhoods."

Immigrant and refugee access to services: (taken from the racial equity toolkit.) Government services and resources are easily available and understandable to all Seattle residents, including non-native English speakers. Full and active participation of immigrant and refugee communities exists in Seattle's civic, economic and cultural life.

Inclusive outreach and public engagement: (taken from the racial equity toolkit.) Processes inclusive of people of diverse races, cultures, gender identities, sexual orientations and socio-economic status. Access to information, resources and civic processes so community members can effectively engage in the design and delivery of public services.

Individual racism: (taken from the racial equity toolkit.) Pre-judgment, bias, stereotypes about an individual or group based on race. The impacts of racism on individuals including white people internalizing privilege, and people of color internalizing oppression.

Institutional racism: (taken from the racial equity toolkit.) Organizational programs, policies or procedures that work to the benefit of white people and to the detriment of people of color, usually unintentionally or inadvertently.

OCR: "Office of Civil Rights."

Opportunity areas: (taken from the racial equity toolkit.) One of seven issue areas the City of Seattle is working on in partnership with the community to eliminate racial disparities and create racial equity. They include: education, health, community development, criminal justice, jobs, housing, and the environment.

Racial equity: (taken from the racial equity toolkit.) When social, economic and political opportunities are not predicted based upon a person's race.

Racial inequity: (taken from the racial equity toolkit.) When a person's race can predict their social, economic, and political opportunities and outcomes.

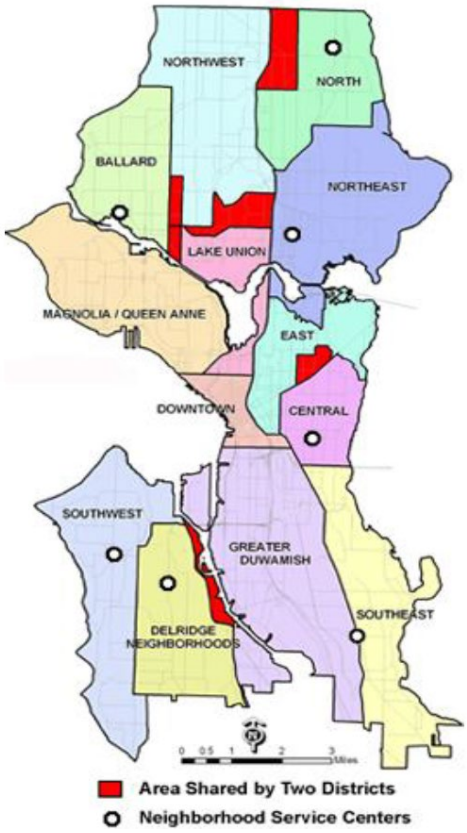
RET: "racial equity toolkit"

Seattle neighborhoods: (taken from the racial equity toolkit neighborhood.) Boundaries defined for the purpose of understanding geographic areas in Seattle.

Stakeholders: (taken from the racial equity toolkit.) Those impacted by proposed policy, program, or budget issue who have potential concerns or issue expertise. Examples might include: specific racial/ethnic groups, other institutions like Seattle housing authority, schools, community-based organizations, change teams, City employees, unions, etc.

Structural racism: (taken from the racial equity toolkit.) The interplay of policies, practices and programs of multiple institutions which leads to adverse outcomes and conditions for communities of color compared to white communities that occurs within the context of racialized historical and cultural conditions.

Surveillance ordinance: Seattle City Council passed ordinance 125376, also referred to as the "surveillance ordinance."



SIR: "surveillance impact report", a document which captures the fulfillment of the Council-defined surveillance technology review process, as required by ordinance 125376.

Workforce equity: (taken from the racial equity toolkit.) Ensure the City's workforce diversity reflects the diversity of Seattle.

City of Seattle

Appendix B: Meeting Notice(s)

City Surveillance Technology Fair

February 27, 2018

6:00 p.m. – 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Join us for a public meeting to comment on a few of the City's surveillance technologies:

Seattle City Light
- Binoculars
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation
- Acyclica

Seattle Fire Department
- Computer Aided Dispatch

Seattle Police Department
- 911 Call Logging Recorder
- Computer Aided Dispatch
- CopLogic

Can't join us in person?

Visit www.seattle.gov/privacy to leave an online comment or send your comment to **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** The Open Comment period is from **February 5 - March 5, 2019.**

Please let us know at Surveillance@seattle.gov if you need any accommodations. For more information, visit Seattle.gov/privacy.

Surveys, sign-in sheets and photos taken at this event are considered a public record and may be subject to public disclosure. For more information see the Public Records Act RCW Chapter 42.56 or visit Seattle.gov/privacy. All comments submitted will be included in the Surveillance Impact Report.

City of Seattle

Giám Sát Thành Phố
Hội Chợ Công Nghệ

ngày 27 tháng 2 năm 2019
6 :00 giờ chiều – 8:00 giờ chiều
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Hãy tham gia cuộc họp công cộng cùng chúng tôi để nhận xét về một số công nghệ giám sát của Thành phố:

Seattle City Light
- Ống nhòm quan sát
- Sensorlink Ampstik
- Đồng hồ đo máy biến áp của Sensorlink

Seattle Department of Transportation (Sở Giao Thông Vận Tải Seattle)
- Acyclica

Seattle Fire Department (Sở Phòng Cháy Chữa Cháy Seattle)
- Hệ Thống Thông Tin Điều Vận Có Máy Tính Trợ Giúp

Seattle Police Department (Sở Cảnh Sát Seattle)
- Hệ Thống Ghi Âm Cuộc Gọi 911
- Hệ Thống Thông Tin Điều Vận Có Máy Tính Trợ Giúp
- CopLogic

Quý vị không thể tới tham dự trực tiếp cùng chúng tôi?

Hãy truy cập www.seattle.gov/privacy và để lại nhận xét trực tuyến hoặc gửi ý kiến của quý vị tới **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** Giai đoạn Góp Ý Mở từ **Ngày 5 tháng 2 - Ngày 5 tháng 3 năm 2019.**

Vui lòng thông báo cho chúng tôi tại Surveillance@seattle.gov nếu quý vị cần bất kỳ điều chỉnh nào. Để có thêm thông tin, hãy truy cập Seattle.gov/privacy.

Các khảo sát, danh sách đăng ký và ảnh chụp tại sự kiện này được coi là thông tin công cộng và có thể được tiết lộ công khai. Để biết thêm thông tin, hãy tham khảo Public Records Act (Đạo Luật Hồ Sơ Công Cộng) RCW Chương 42.56 hoặc truy cập Seattle.gov/privacy. Tất cả các ý kiến đóng góp mà quý vị gửi đến sẽ được đưa vào Báo Cáo Tác Động Giám Sát.

City of Seattle

Eksibisyon ng Teknolohiya Sa Pagmamatyag sa Lungsod

Pebrero 27, 2019

6:00 p.m. - 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Samahan kami para sa isang pampublikong pagpupulong upang magbigay ng komento sa ilan sa mga teknolohiya sa pagmamanman ng Lungsod:

Seattle City Light
- Mga Binocular
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation (Departamento ng Transportasyon ng Seattle)
- Acyclica

Seattle Fire Department (Departamento para sa Sunog ng Seattle)
- Pagdispatsa sa Tulong ng Computer

Seattle Police Department (Departamento ng Pulisya ng Seattle)
- Rekorder ng Pagtawag sa 911
- Pagdispatsa sa Tulong ng Computer
- CopLogic

Hindi kami masasamahan nang personal?

Bumisita sa www.seattle.gov/privacy upang mag-iwan ng online na komento o ipadala ang iyong komento sa **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** Ang panahon ng Bukas na Pagkomento ay sa **Pebrero 5 - Marso 5, 2019.**

Mangyaring ipaalam sa amin sa Surveillance@seattle.gov kung kailangan mo ng anumang tulong. Para sa higit pang impormasyon, bumisita sa Seattle.gov/privacy.

Itinuturing na pampublikong rekord ang mga survey, papel sa pag-sign-in at mga larawan na makukuha sa pangyayaring ito at maaaring mapasailalim sa paghahayag sa publiko. Para sa higit pang impormasyon, tingnan ang Public Records Act (Batas sa Mga Pampublikong Rekord) RCW Kabanata 42.56 o bumisita sa Seattle.gov/privacy. Isasama ang lahat ng isinumiteng komento sa Surveillance Impact Report (Ulat sa Epekto ng Pagmamanman).

City of Seattle

Feria de tecnología de vigilancia ciudadana

27 febrero de 2019

De 6:00 p. m. a 8:00 p. m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Acompáñenos en la reunión pública para dar su opinión sobre algunas de las tecnologías de vigilancia de la ciudad:

Seattle City Light
- Binoculars
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation (Departamento de Transporte de Seattle)
- Acyclica

Seattle Fire Department (Departamento de Bomberos de Seattle)
- Computer Aided Dispatch

Seattle Police Department (Departamento de Policía de Seattle)
- 911 Call Logging Recorder
- Computer Aided Dispatch
- CopLogic

¿No puede asistir en persona?

Visite www.seattle.gov/privacy para dejar un comentario en línea o enviar sus comentarios a **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** El período de comentarios abiertos es desde el **5 de febrero al 5 de marzo de 2019.**

Avísenos en Surveillance@seattle.gov si necesita adaptaciones especiales. Para obtener más información, visite seattle.gov/privacy.

Las encuestas, las planillas de asistencia y las fotos que se tomen en este evento se consideran de dominio público y pueden estar sujetas a la difusión pública. Para obtener más información, consulte la Public Records Act (Ley de Registros Públicos), RCW capítulo 42.56, o visite Seattle.gov/privacy. Todos los comentarios enviados se incluirán en el Informe del efecto de la vigilancia.

City of Seattle

Kormeerida Bandhigga Tiknoolajiyada ee Magaalada

Feebaraayo 27, 2019
6:00 p.m. - 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Nagulasoo biir bandhigga dadweynaha si fikir looga dhiibto dhawr kamid ah aaladaha tiknoolajiyada ee City surveillance:

Seattle City Light
- Binoculars
- Sensorlink Ampstik
- Sensorlink Cabiraha mitirka Gudbiyaha

Seattle Department of Transportation
(Waaxda Gaadiidka ee Seattle)
- Acyclica

Seattle Fire Department
(Waaxda Dab damiska ee Seattle)
- Adeeg Qaybinta Kumbuyuutarka loo adeegsado

Seattle Police Department
(Waaxda Booliiska ee Seattle)
- Qalabka Duuba Wicitaanada 911
- Computer Aided Dispatch
- CopLogic

Nooguma imaan kartid miyaa si toos ah?

Booqo barta www.seattle.gov/privacy si aad fikirkaaga oonleen ahaan uga dhiibato **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.**
Mudada Fikrad Dhiibashadu furantahay waxay kabilaabanaysaa **Feebaraayo 5 - Maarso 5, 2019.**

Fadlan noogusoo gudbi ciwaankaan Surveillance@seattle.gov hadaad ubaahantahay hooy laguusii qabto. Wixii macluumaad dheeri ah, booqo Seattle.gov/privacy.

Xog aruurinada, waraaqaha lasaxixaayo iyo sawirada lagu qaado munaasabadaan waxaa loo aqoonsanayaa diiwaan bulsho waxaana suuragal ah in bulshada lagu dhex faafiyo. Wixii macluumaad dheeri ah kafiiri Public Records Act (Sharciga Diiwaanada Bulshada) RCW Cutubkiisa 42.56 ama booqo Seattle.gov/privacy. Dhammaan fikradaha ladhiibto waxaa lagusoo darayaa Warbixinta ugu danbaysa ee Saamaynta Qalabka Muraaqabada.

City of Seattle

城市监控技术博览会

2019 年 2 月 27 日
下午 6:00 至下午 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 9810

加入我们的公众会议，留下您对纽约市监控技术的意见：

Seattle City Light
- 望远镜
- Sensorlink Ampstik
- Sensorlink 变压器表

Seattle Department of Transportation（西雅图交通局）
- Acyclica

Seattle Fire Department（西雅图消防局）
- 计算机辅助调度

Seattle Police Department（西雅图警察局）
- 911 通话记录录音器
- 计算机辅助调度
- CopLogic

无法亲自前来？

访问 www.seattle.gov/privacy 发表在线评论或将您的意见发送至 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124。开放评论期：2019 年 2 月 5 日至 3 月 5 日。

如果您需要任何住宿服务，请通过 Surveillance@seattle.gov 联系我们。要获得更多信息，请访问 Seattle.gov/privacy。

此次活动中的调查、签到表和照片被视为公共记录，可能会被公开披露。有关更多信息，请参阅 Public Records Act（信息公开法）RCW 第 42.56 章或访问 Seattle.gov/privacy。提交的所有意见都将包含在监控影响报告内。

City of Seattle

도시 감시 기술 박람회

2019 년 2 월 27 일
오후 6:00 – 오후 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

공개모임에 참여하시고, 도시 감시 기술과 관련한 의견을 공유해 주십시오.

Seattle City Light
- 쌍안경
- Sensorlink Ampstik
- Sensorlink 변압기 미터

Seattle Department of Transportation(시애틀 교통국)
- Acyclica

Seattle Fire Department(시애틀 소방국)
- 컴퓨터 지원 출동 지시

Seattle Police Department(시애틀 경찰국)
- 911 전화 기록 녹음기
- 컴퓨터 지원 출동 지시
- CopLogic

현장 참여가 어려우신가요?

www.seattle.gov/privacy 를 방문하셔서 온라인 의견을 남기시거나 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124 로 의견을 송부해 주시기 바랍니다. 공개 의견 수렴 기간은 2019 년 2 월 5 일 – 3 월 5 일입니다.

편의사항이 필요하신 경우 Surveillance@seattle.gov 로 문의해 주시기 바랍니다.
자세한 정보는 Seattle.gov/privacy 를 참조해 주십시오.

본 행사에서 수집된 설문 조사, 참가 신청서 및 사진은 공개 기록으로 간주되며 일반에 공개될 수 있습니다. 자세한 사항은 Public Records Act(공공기록물법) RCW 챕터 42.56 을 참조하시거나, Seattle.gov/privacy 를 방문하시기 바랍니다. 제출된 모든 의견은 감시 영향 보고서에 수록됩니다.

City of Seattle

城市監視技術展覽會

2019 年 2 月 27 日
下午 6:00 至下午 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

加入我們的公眾會議，留下您對紐約市監視技術的意見：

Seattle City Light
- 望遠鏡
- Sensorlink Ampstik
- Sensorlink 變壓器表

Seattle Department of Transportation（西雅圖交通局）
- Acyclica

Seattle Fire Department（西雅圖消防局）
- 電腦輔助發送

Seattle Police Department（西雅圖警察局）
- 911 通話紀錄錄音機
- 電腦輔助發送
- CopLogic

無法親自前來？

造訪 www.seattle.gov/privacy 發表線上評論或將您的意見傳送至 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124。開放評論期：2019 年 2 月 5 日至 3 月 5 日。

如果您需要任何便利服務，請透過 Surveillance@seattle.gov 聯絡我們。要獲得更多資訊，請造訪 Seattle.gov/privacy。

此次活動中的調查、簽入表和照片被視為公共紀錄，可能會被公開披露。有關更多資訊，請查閱 Public Records Act（資訊公開法）RCW 第 42.56 章或造訪 Seattle.gov/privacy。提交的所有意見都將包含在監視影響報告內。

Appendix C: Meeting Sign-in Sheet(s)

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☒ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☒ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

☐ include Middle Eastern

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☒ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☒ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☒ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☑ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☑ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☒ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☒ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☑ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☒ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☒ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☑ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☑ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☑ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Queen Anne

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☑ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☑ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☒ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☒ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☒ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☑ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☑ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

X

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☒ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☒ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☒ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☒ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☒ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☒ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☑ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

leighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
] Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☒ 18-44
☐ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☒ Female
☐ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☑ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
] Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☐ 45-64
☑ 65+
☐ Prefer not to identify

Gender

☐ Female
☑ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

☑ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
] Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☑ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☑ Female
☐ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney
SE KING COUNTY

☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☑ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
✓ Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☑ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☐ Female
☑ Male
☐ Transgender
☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☒ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☒ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☒ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☒ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☒ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☑ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☑ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☑ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☑ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☑ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☑ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Appendix D: Department of Neighborhood Focus Group Notes

Friends of Little Saigon (FOLS)

Please select which technology you wish to comment on:

☐SCL: Binoculars ☐SCL: Sensorlink Transformer Meter (TMS) ☐SFD: Computer-Aided Dispatch ☐SPD:9-11 Call Recorder

☐SCL: Sensorlink Ampstik ☐SDOT: Acyclica ☐SPD: Computer-Aided Dispatch ☒SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

- Will they keep the data safe on coplogic?
- Can it be hacked?
- What if you report your neighbour and your neighbour hacks the system and find out?
- What is the money amount limit for coplogic / Why is there a limit for coplogic?: (a community member says that she believes that the limit $500 or under, but it's hard to have a limit because a lot of packages cost more than $500 such as electronics get stolen and you won't be able to report it online)
- The departement is having all these technologies being used but not letting the public aware of it
- Coplogic is not clear and is confusing to use (what you can report and what you can't report)
- If coplogic is known by the community would they use it ? (Community members agreed that no one would use coplogic because it's not in Vietnamese. Not even people who speak english fluently even use it.
- Many community members don't trust the system)

What value, if any, do you see in the use of this technology?

- Coplogic has been going on for a few years it's not very effective. The only effective thing is that coplogic is doing saving police hours and time.

What do you want City leadership to consider about the use of this technology?

- Most of the time, our community don't report things because they don't trust the system, they often tell someone that they trust a friend. Is there an option that someone and report a crime for someone else?

Other comments:

- The government should be more transparent with the technology system with the public.

- The translation is much far removed from the actual Vietnamese language.
- The translation is very hard to understand, the language is out of context (The flyer is poorly translate)
- Is there resources to support these technologies? Is there translations so that it is accessible for everyone? Will this accommodate everyone?
- Police should have a software that connects them to translation and interpretation right away instead of having to call a translator
- How will other people know of the technology if they can't come to focus group meetings? Such as flyers? Social media? Etc.
- Besides face to face meetings, are there plans to execute this information of the technology and surveillance to the community?
- Will the City of Seattle go to community events, temple, the church to reach out to the community and explain the technologies?
- These technologies are taking a part of our taxes, so everyone should know. It should be for everyone to know, not only catered to one group or population.

Are there any questions you have, or areas you would like more clarification?

- How effective are the tools/technology?
- How many people know of these technologies? Provide statistics
- What are the statistics of the coplogic?
- What is the data and statistics for coplogic and what are people reporting?
- What is the most common crime that they are reporting?
- And how effective is coplogic based on the statistics and data?

Friends of Little Saigon (FOLS)

Please select which technology you wish to comment on:

☐SCL: Binoculars	☐SCL: Sensorlink Transformer Meter (TMS)	☐SFD: Computer-Aided Dispatch	☒SPD:9-11 Call Recorder
☐SCL: Sensorlink Ampstik	☐SDOT: Acyclica	☒SPD: Computer-Aided Dispatch	☐SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

- CAD did not work from experience. A community member said that they reported that they needed assistance at 10:00pm and no one showed up, then had to call 911 at 12:00am and someone finally showed up at 4:30am
- Why create more options and technologies if the police department and government can not support it? It's a waste of time and money (taxes). Should have enough personals before they implement technology.
- Government should have enough personals to support translation if they choose to translate.

What do you want City leadership to consider about the use of this technology?

- The city should focus on having the community review the technologies that are yet to be implemented.
- The Vietnamese community is not getting the information we need to report crimes

Other comments:

- Engagement is very important. Engaging the community and engaging different demographics.
- Friday night, Saturdays, and Sunday afternoon work the best for the Vietnamese community.
- If the city wants to involve the vietnamese community and engage the Vietnamese community, it is important to accommodate with our community It is important to proofread the translation, have 3 people proofread. Someone
  pre 1975, post 1975 and current Vietnamese language. The government clearly does not proofread the translation.

Council on American Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington
Thursday, Feb. 21, 2019
Technology Discussed: CopLogic

1. Do you have concerns about this specific technology or how it's used?
    - Having used the system myself the one thing I noted was the type of report you can file, they ask questions like if you knew the suspect, and if you're saying no I don't know who did it. and you check a box that says I understand that no one is going to investigate this
        - What is the point of having a system in place than If no one is going to investigate it
        - It is for common things like my car is broken into and stuff was taken out of my car, you can file it if you need a report for insurance. But if you were to call that and report to the police, they wouldn't come for days
    - So for example if I can be a straight up Islamophobe and I can see a Muslim woman and make a bunch of false reports online, and how long would it take for someone to say I see you making all these reports. Because people can make so many different reports, how do you deal with that
        - There are very limited types of reports that it will accept. So if someone wanted to report graffiti and they were reporting more hate crime related graffiti an officer will review the report
        - So I think the review process would be really important
    - Another barrier is that it's an online system so we need to think about wifi access and there is this assumption that everyone has access to internet and computers. And what I'm hearing is that people can just file a report at a click of their finger. And if these people can do that on their computer what stops them from being able to file all these cases about certain groups and individuals.
    - Additional there have been cases in the past where people are abusing reporting system. This one doesn't allow you to report against known suspect but I could see that happening in the future so I wanted that to be mentioned. The other thing under protection is says all activity can be stored and the data Is monitored by lexis nexus… and this company does a lot of research on crime mapping which brings up some of the concerns on like CVE
        - But what you are saying is that lexis nexus does other mapping that it can use this information for
        - Yes, because I want to clarify what is the technological ambition of SPD because I don't think this would work well in the communities that SPD is supposed to served. And I would want a contract review of what lexis nexus does. Will the info stay on the data and server of lexis nexus, what happens to it
    - Another thing is has SPD given Lexis nexus to use this in any of the research data they do, because they put out a lot of information regarding mapping, and crime control. And what information are they allowed to take
    - We have seen recently people doing interesting things when reporting crimes. I think its important to realize that when reporting crime people have a different perception when

reporting crime. People will see you in a certain neighborhood and might think they stole that car, or are doing something bad here. So when we give people the ability to report online we need to be concerned with accessibility about people being able to report freely… and we saw for a year that if an African American person came to use a swimming pool someone can call and say they don't live here. I think SPD is trying alleviate some of those calls they are getting, but I don't think this is the solution to the problem

- What is the logic behind this overall, because is seems like it presents more cons than pros, and what is analytics database you use to look at these reports. Because when I am using government data base I can see where I need more surveillance etc. so we are getting all these open wholes in the system. Is this a right wing Donald trump agenda to watch neighbors of color and surveillance
- I think im more concerned with where does this information end up and how is it used
- What is the usefulness of the information that is not followed up on. And how does it help the people it's actually serving? So for example someone works for an anti-Muslim white supremacy group and they have people in different areas report issues about different Muslim groups in Seattle how do you prove the validity of these information and make sure they aren't just causing harm

2. What value do you think this brings to our city?
    - I think technology saves time, money, makes filing a report easy, I had to do that once it takes a lot of time.
    - I appreciate that it is easier so something like a hit or run or a car breaking in, that's fine.
3. What worries you about how this is used?
    - The only issues I can think of right now is it seems like it would be very easy to make a fraudulent report or a report that is for a small thing that you can make into a big thing, like the things you see go viral on the internet. So now it seems like the barrier to making a police report is smaller
    - I agree I think the bar is lowered and different people are perceived differently. And we have seen how SPD criminalizes different communities for behaviors that don't need to be criminalizing
    - A lot of different kinds of reports have to do with peoples perceived notion, so my concern comes from how do we make sure that this kind of technology isn't used to map our where Muslims live/are, and there types of religious belief. Or isn't being used to monitor them. How do we ensure that this isn't used to map our communities
    - The only comment I have that in the forms I have filled out is it won't allow you to fill out the form if you are naming a specific individual, you can name a group, but a not a person. The following criteria is there no known suspects, it happens in Seattle, so things like thefts. So you can report, graffiti, identity theft, credit card fraud, simple shop lift. So when I click report it says if you have a suspect it says please call. And when I press report it allows me to report anonymously, so I could report against a community with no follow up
        - Well that doesn't stop them from targeting al-Noor masjid, or Safeway in new holly, or new holly gathering hall, and it can target the people in that

community. And people don't feel comfortable with increase police presences, so it targets area if not targeting people

- When I was buying the house in Dallas (participant currently still lives/works/plays in Seattle) one of the first things I did was looking at a crime map and based off of that if someone is making a lot of reports can that be used for crime mapping because than that can lower the property value. And if the police isn't following up then how is it being used
- Its definitely possible for people to report inaccurate information

4. What recommendations would you give policy makers at the City about this technology?
    a. But my concern is reporting someone that can really target people of color. And that happens much more threatening to people. So the concept of an upset black women is more intimidating than an upset women that is another race and how many times will behavior like that be reported. Or how many times will a black man be reported against because it seems scary. So I think it lowers the bar when you don't have to talk to an individual when you don't have to talk to a police
    b. My questions are, how accessible are cop logic to people who don't read or speak English. How is SPD going to do what they can to make sure that this doesn't negatively impact communities they are already having issues with like the Sea Tac community that already feels threaten and criminalized by communities.

5. Can you imagine another way to solve the problem this technology solves?
    - So the SPD is very data driven these days and the one thing we repeat is report report report, call 911 and report online whatever you thinking is happening because all of that goes into their data base and is used for them to use resources and put police based off of where there is more crime. The report report report mentality assumes there are good relationships between the community and police, so even if someone doesn't do something bad, I don't know that they would feel comfortable reporting, even if online
    - From the community I have come from I am almost certain that they haven't even used online reporting so how do we make sure that we are giving everyone access to use online reporting. And there are certain crimes that are so common in areas that they don't even report it because they think the police should already know about it
    - I think the department should solely rely on the technology only as a way of collecting info they should still use in personal resources to actively participant in local community and make connections you can't rely only on this technology alone to do this

6. Other comments
    a. Also in this day in age we need to consider that immigration is a issue, and this administrative has blended the different agencies so people have a hard time knowing where SPD starts and ICE starts and those lines have been blurred and that is a real concern for many families

Council on Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington

Thursday, Feb. 21, 2019

Technology Discussed: Binoculars/Spotting Scope

1. Do you have concerns about this specific technology or how it's used?
    . People in our community don't have the access to say or be apart of these conversation. A lot of these people are literate, and might not have the same cultural values. For Muslim women there are a type of consent that you have when you walk outside and are covered in a certain away versus when you are in the privacy of your own home. And people might not have that cultural and religious awareness
    a. I had one quick concerns, as far as the data that is collected using these binoculars, who has access to it
        - Seattle City Light: Information goes into the billing system, which customers can access if they have the automated reader but do not have access to under the current system
    - I know the focus is on binoculars but my mind is on new technologies and when people who are consumers and feel like I am overcharged how do I follow up and get those issues resolved. For systems that are completed based off of technologies how will I know if that data is being altered.
    b.
2. What value do you think this brings to our city?
    . I would just add this is more my general comments I think its good that Seattle city lights is providing notifications to people when this is happening. Are they wearing something visible that show people they are from Seattle city lights? And is there a way for people to complain?
        - Yes they are wearing vests that are very visible. Yes we have a couple different avenues the easiest is to call the customer service line and to submit a complaint there
3. What worries you about how this is used?
    . My primary concerns on my end is if someone is looking into my home with binoculars its a privacy concern. Most Muslim women wear hijab and I don't feel comfortable if someone is using binoculars looking from the outside when we are not wearing the hijab. My concern is that it is a huge invasion of privacy
    a. I have a question as the women expressed the feeling of people reading the meters with binoculars, if the meter has abnormal behavior or is in a different place of the house. Have there been situations where someone sees the person looking at someone house with binoculars, and they might not have gotten

notified. Or the meter might be on the opposite side of where they are looking. Are they getting background checks? Or are complaints being followed up

- Seattle City Light: Yes all city employees have background checks, and if a complaint gets called in they will go through disciplinary actions
- What are the average times for disciplinary actions. How long is the process for a full investigation
- Seattle City Light: It's a multiple step process in terms of different levels. There are warnings, and if there was undo actions. Timeline really depends, I'm not sure
- Cause I think that people who go through the different nuances of how privacy can be breach that is just the end all be all of how privacy can breach so I think there needs to be policy put in place so that people don't have their privacy breach and they are being monitored by a pedophile

4. What recommendations would you give policy makers at the City about this technology?
   . When I look at the Seattle city of light they do a lot of estimated guesses and as a consumer they might give you a $500 fee based off of the estimated guesses so I think it is important to have some sort of device that better clearly shows how much you use

5. Can you imagine another way to solve the problem this technology solves?
   . My other question is if its actually not efficient why do you get the option to opt out (of the new automated system). If there is an old school way of doing it that involves a breach of privacy because these are human beings using the binoculars, so If this other option is better why are people having the ability to opt out.
6. Other comments: (Many comments were discussed over Seattle City Light's upcoming change from binocular use to automated meter readers)
   . Who opted out was it home owners?
   a. When we go to a place with 12 tenements do all 12 of them have the ability to opt out or in, or just the owners of the building?
   b. Each home owner has a schedule provided to them and it is a 3 day period which they can come in and look at the system
   c. Is there a cost to them to have the new meter.
      - Seattle City Light: There is no cost with getting the new meter, but there is still a cost If we have to send someone out there to read it
      - What I don't understand is why the new practice is not to just use the new system since that is more accurate and it is doesn't require binoculars
      - What is the cost of opting out

    - Seattle City Light: There is a flat rate
- I was gonna reiterate when we talk about equity and equitable practices. You can opt out (of the automated system) but there is a fee. And it makes me think how much of It is a choose if one of these you have to pay for and the other one is free. So that sounds a little problematic when looking at choices of equity. I think choices are great, but also people need to be well informed. Like people within the community need to have more clear information to make the best decision for themselves
- Going back to people who make the decision. I want the person who are living in the house to know what decision is being made. So not just the person who owns the house, but the person living in the home. And not everyone it literate and not everyone speaks English. And its really important that you are giving them information they can actually consume. Instead of giving them notices they cant read

Council on Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington
Thursday, Feb. 21, 2019
Technology Discussed: Acyclica

1. Do you have concerns about this specific technology or how it's used?
    - Where does this data go? Does it go to SDOT? Google maps?
    - My other question is, it said whatever is being transferred is encrypted. All encrypted means to me is getting data from one device to another will be transferred without it being intercepted. What I don't know is, how much information are people getting
    - My concern is related to data, yeah we like to use gps. But what is the perimeter, what is the breach of access. Where is the data being used, and what can that turn into. we might be okay if the data is only being used for traffic related updates, but they might use it for more
    - I also would like to see how acyclica actually does what they do. They are using a lot of words that normally don't know. So I want to know how exactly they are hashing and salting. So for them to be clear about how they doing it. like when whatsapp encrypted they didn't give us the exact code but told us how they are doing it
    - Asking for a greater transparency for how they are doing this
    - I think the purpose of it is really important but the biggest concern is collecting all of this information without consent of passersby.
    - So the specific identifier that acyclica uses it mac addresses? You could potentially use that number to track that phone for the lifetime of the phone, for as long as that phone is on and being used. And that is very concerning.
    - Also I want to understand more where is this data going, and I want to know if this data is going to be used for future projects.
    - I want to ask is this something people opt into
    - People don't even know this is being used

2. What value do you think this brings to our city?
    - I like getting places and I like getting traffic information.
3. What worries you about how this is used?
    - What I don't like is you using my phone to get that information. I want whatever is in my cellphone to be protected. And I wanna know what you can access
    - I think based on Seattle and Seatac's higher up wanting to monitor and map out Muslims and where they are, and I don't like people being able to use our phone to track our location or actions they might think is violent. So based off of Seattle's track record and law enforcement agencies I don't like it
    - People who live outside of Seattle are also being impacted by it anytime they drive in Seattle
    - Could someone "opt out" by having wifi disabled on their device? I don't know if this covers cell towers. Because if it covers cell towers the only thing you could is having your phone on airplane mode

4. What recommendations would you give policy makers at the City about this technology?
    - I think the big question is why aren't we using other vendors, like I mentioned google maps, or waze, in fact komo 4 uses ways. Where other options we're looked at, and what were the trade off there's. And I want to see some transparency between the decision-making processes
    - I don't think this data should be shared with other private agencies, or other interagency programs
    - If all you're looking at is traffic flow, why are you not using the sensors in the road to give traffic flow updates.
    -
5. Can you imagine another way to solve the problem this technology solves?
    - I don't know if this already exists but something that makes it that data can't be used from one technology and use it for a different purposes
    - I think speaking from an industry perspective that is really important to have a processes for. Because all of this data is being used regardless of if you live in Seattle, or people live in different countries even who are visiting. That data is being collected. My understanding is that SDOT doesn't get the data directly. So my concern is how long can acyclica keep this data, use this data. Why wasn't a different option used, one in which some sort of consent can be used, so something like waze, google maps where people can opt in can get that information.
    - Road sensors or ways to count cars
    - I think its better to count cars than phones, because there is some expectation that your car will be monitored.
    - Using vehicle level granularity

Entre Hermanos

Please select which technology you wish to comment on:

☐SCL: Binoculars	☐SCL: Sensorlink Transformer Meter (TMS)	☐SFD: Computer-Aided Dispatch	☐SPD:9-11 Call Recorder
☐SCL: Sensorlink Ampstik	☒SDOT: Acyclica	☐SPD: Computer-Aided Dispatch	☐SPD: CopLogic

1) What concerns, if any, do you have about the use of this technology?

El uso de wifi en Acyclica porque pueden obtener toda la información de los teléfonos.

Si vale la pena la inversión

Enfocando al grupo: La tecnología ya está instalada. que les preocupa de su uso?

El tráfico sigue igual.

Quien usa o almacena la información.

La preocupación es la colección de data.

Colección y almacenamiento de información es la mayor preocupación.

No es la colección de data lo alarmante sino los recursos (dinero utilizado) ya que o la tecnología no están funcionando porque el tráfico sigue igual. No hay cambio con la nueva tecnología, esos gastos no son válidos ya que no hay resultados. Esos gastos pudieran ser utilizados para la comunidad.

También tienen que ver si la tecnología emite radiación o alguna otra cosa dañina; perjudicial a la salud.

El gobierno tiene todos los datos.

No necesitan esta tecnología para tener los datos porque ya existen métodos para eso, incluso aplicaciones o alguna otra cosa.

La otra preocupación del grupo es que no haya un cambio al problema que se quiere resolver. En el caso de Acrylica sería el mejorar el tráfico.

- Tecnologías como esta necesitan recolectar más opiniones de expertos.
- Sería bueno que la información sea compartida con la comunidad. (Transparencia en fines y objetivos de la tecnología y datos guardados, tácticas implementadas.)

2) What do you want City leadership to consider about the use of this technology?

Hay lugares donde no se necesitan. En algunas partes de Magnolia, Queen Anne, Northgate, no se ocupan.

Seguimiento de pregunta: En las comunidades donde viven los latinos que tanto se ocupa Acyclica?

Participante no cree que allí se ocupan.

Hablaron sobre la necesitad de puntos estratégicos y calles con más necesidad de ayuda por causa del tráfico.

What do you think about this technology in particular ?

Bien, la tecnología ayuda con la velocidad o el movimiento de los coches.

La información se guarda y analizan por donde viajas o cuantas veces cruzas este rastreo.

Si es solo para ver el tráfico está bien.

Está bien en algunas partes. Puede que sea algo bueno. Pero puede que esta tecnología pueda compartir información personal que puede ser utilizada de otra forma en especial si hay Hacking (forma negativa, uso de datos).

La tecnología en sí no es tan grande (de tamaño) para ser algo visualmente desagradable. La información captada a través de estos medios puede que ayude a conducir el tráfico de mejor manera pero también puede que tome información personal.

Are there any questions you have, or areas you would like more clarification? ●

La tecnología no es un router, sino colección de data para planeaciones urbanas.

Participante: “quiero creer” “convencerme” que los sensores están allí para ayudar con el tráfico.

No se sabe cuándo las instalaron, los resultados deberían de ser públicos. Si la tecnología es para aliviar el flujo de tráfico entonces por qué no extienden el programa? O por qué no hay mejoramiento del tráfico?

Alternatives to this technology

- Alguna pantalla que indique cuáles vías son alternativas puede reemplazar esto.
- Cambios al límite de velocidad puede que alivie el flujo del tráfico.
- Dejar de construir tanto.
- Rediseño de calles ayudaría flujo de tráfico.
- El rediseñar las vías servirá para las futuras generaciones.

Entre Hermanos

Please select which technology you wish to comment on:

☒SCL: Binoculars	☒SCL: Sensorlink Transformer Meter (TMS)	☐SFD: Computer-Aided Dispatch	☐SPD:9-11 Call Recorder
☐SCL: Sensorlink Ampstik	☐SDOT: Acyclica	☐SPD: Computer-Aided Dispatch	☐SPD: CopLogic

1) What concerns, if any, do you have about the use of this technology?

Los binoculares son preocupantes si la persona no tiene ética. Es preocupante que una persona vea a través de binoculares a que una tecnología mida el uso de la electricidad

Al grupo le incomoda el uso de binoculares

Sensorlynk específicamente la preocupación sería que le quita el trabajo a una persona.

Si es para detectar robo el grupo cree que hay otras maneras de saber quien roba

que no tan solo será para leer la electricidad sino para obtener otros tipos de información si cámaras fueran usadas

2) What value, if any, do you see in the use of this technology?

Ahorro de energía

Record y datos mas precisos

Oportunidad de trabajo a quien utiliza los binoculares

Estabiliza los precios de la electricidad

3) What do you want City leadership to consider about the use of this technology?

: Usar background check, uso de uniforme por trabajadores, cámara en binoculares.

What do you think about this technology in particular ?

Sensorlink Si

Binoculares son invasivos

Are there any questions you have, or areas you would like more clarification? ●

La confianza en estos medidores serán confiables? Serán efectivos?

El uso de binoculares se puede acompañar de una cámara añadida

Alternatives to this technology

Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad

City of Seattle

Entre Hermanos

Please select which technology you wish to comment on:

☐SCL: Binoculars ☐SCL: Sensorlink Transformer Meter (TMS) ☐SFD: Computer-Aided Dispatch ☐SPD:9-11 Call Recorder

☐SCL: Sensorlink Ampstik ☐SDOT: Acyclica ☐SPD: Computer-Aided Dispatch ☒SPD: CopLogic

1) What concerns, if any, do you have about the use of this technology?

Las fallas electrónicas son preocupantes especialmente en reportes policiacos.

Las preocupaciones es que el reporte no salió, no llegó por cualquier razón.

No todos podrán o saben usar las computadoras.

Fallas de los algoritmos de cada demanda es alarmante.

Que y cuando determina la urgencia de respuesta

Las personas le temen a los policías. Y este medio puede ayudar a que el miedo disminuya.

La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

2) What value, if any, do you see in the use of this technology?

La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

El uso de computadora está bien para las denuncias.

Si personas usan esta tecnología y es analizada en tiempo real por otras personas no hay problema.

Es otro método para denunciar

Está de acuerdo con el uso de computadoras para denunciar solo que no todos son capaz de usar este método/tecnología.

3) What do you want City leadership to consider about the use of this technology?
Que sea multi-idioma, implementar audio, implementar sistemas que ayuden a múltiples personas con diversas capacidades/necesidades

Si es usada de manera adecuada y como han dicho está bien.

El uso de la tecnología es bueno para dar respuesta para todas las cosas y personas

What do you think about this technology in particular ?

Grupo están de acuerdo con su uso.

Puede salvar una vida.

Los riesgos y acciones determinan la urgencia de la intermisión policiaca.

Alguna gente se siente más capaz de presentar una queja a través de este sistema, la tecnología en uso tiene validez.

Bueno para la violencia doméstica.

Are there any questions you have, or areas you would like more clarification?

La computadora decidirá la importancia/urgencia del reporte/emergencia dando a llevar acciones de emergencia.

Gravedad de emergencia es determina por tecnología.

La definición de emergencia es diferente con cada persona.

Cada uno tiene la definición de vigilancia, pero ¿que tal la definición de emergencia?

SITUATIONS TO APPLY ITS USE

Una pelea en la calle, un malestar corporal, cuestiones de vida, abuso doméstico

Si nos basamos en la definición de emergencia sólo en cuanto estemos en peligro inmediato o en tiempos mínimos/ de transcurrencia alarmante/peligrosa el uso de será implementado o limitado solo a instantes inmediatos de peligro.

Para reportar algo que ya sucedió o que son recurrentes.

Basado en el concepto de emergencia, las personas pueden tomar el método adecuado para reportar su caso y a través del medio necesario.

Los reportes no son anónimos.

Los datos son recolectados aun, a pesar de la opción escogida.

Alternatives to this technology

Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad

Entre Hermanos

City of Seattle
Surveillance

Inicio

Resumen: El departamento de vecindarios quiere saber la opinión de este grupo. Ellos verán videos de un minuto y medio y encontrarán folletos en sus mesas donde encontraran más información sobre lo visto.

Demográficos:

Ocho personas participaron, una de West Seattle, una de First Hill, dos de Ravenna/Laurelhurst y cuatro de King County (outside Seattle).

Cuatro personas se consideraron hispano o latino, una como india americana o nativa de Alaska, y tres no opinaron.

Cinco personas marcaron 18-44 como su rango de edad, dos marcaron 45-64 como el suyo y una no opinó.

Cinco personas marcaron masculino como género, una como transgénero, una como femenino, y otra no opinó.

Otra Información Importante:

- Preguntas serán hechas.
- Habrá una hoja para poder conversar sobre videos de interés
- Se les agradeció por venir.
- El concepto de vigilancia será manejado como la ciudad de Seattle lo maneja.
- Tom: Agradeció a los invitados por venir

Surveillance. In 2017 city council passed an ordinance to see what technology fit the definition of surveillance. The information gathered by these surveillance technologies are as follows: to “observe or analyze the movements, behaviors, or actions of identifiable individuals in a manner” which "is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice.”

Presentador: Preguntó si la conversación en inglés fue entendida.

Grupo: Concordó.

Tom: Do not let information on videos stop you from making comments or raising questions.

Presentador: Dio a entender el concepto de vigilancia como ha sido interpretada por la ciudad de Seattle. Fue analizada de esta manera: "La vigilancia es definida como tecnologías que observan o analizan los movimientos, comportamientos, o acciones de individuales identificables de una manera que razonablemente levanta inquietudes sobre libertades civiles, la libertad de expresión o asociación, igualdad racial o justicia social."

- Los movimientos de la gente son observados a través de esta tecnología y puede que para algunas personas esto sea incómodo.
- Las cámaras de policía no califican como tecnologías de vigilancia en este tema.
- La presentación mostrada en la pantalla a través de los videos será transmitida en inglés.
- Se pidió que todos se traten con respeto y que opinen y que su nombre sea mencionado e incluso la vecindad donde viven.

El Grupo

Participante vino porque quiere obtener más información y dar su opinión. Es de Seattle.

Participante viene de Shoreline/Seattle para ver cuánto la tecnología entra afecta

Participante vino porque quiere saber qué información es colectada por el gobierno y para qué usan esa información. Puede que la información obtenida a través de la tecnología sea usada para perseguir a personas de color/minorías/personas marginadas.

Participante vino de First Hill, porque quiere ver el punto de vista de la ciudad y ver que opiniones surgirán.

Participante viene de Seatac porque tiene interés en el tema y porque la seguridad es importante y quiere saber a dónde llega la información.

Participante vine en Ravenna/Northgate, quiere ver que tan confiable es la tecnología y para qué es utilizada. Perjudicial o beneficial?

Participante vine en Seatac y vino porque es un tema muy interesante ya que se tiene que saber/mantener informado de lo que hacen los gobernantes.

Participante vino de Burien por la importancia del tema y la privacidad.

Presentador: La tecnología no es nueva. Ya está siendo usada. Y quieren saber el formato para que las futuras tecnologías tengan.

El video de Seattle Department of Transportation de Acyclica fue mostrado

Esta tecnología es un sensor que detecta el wifi. Es un sensor que detecta la tecnología wifi.

Seattle Metering Tool fue mostrada

Nadie del grupo sabe del tema más el presentador no hablará a fondo de esto para no influenciar opiniones.

Video de Fire Department's Computer Aided Dispatch fue mostrado

El 9-1-1 logging recorder video fue mostrado

Aclaración: Información impresa fue entregada explicando cada una de las tecnologías.

Video de Coplogic fue mostrado

El grupo no conocía que se puede reportar a la policía a través de su página/en línea.

El video de Seattle Police Computer Aided Dispatch fue mostrado

Esta tecnología es similar a la de los bomberos.

Se preguntó cuál video era de interés para analizar

Se acordó el análisis de Acyclica, Binoculares/Sensorlink, y Coplogic

Las Preguntas que sea harán serán las siguientes:

¿Qué piensan de este sistema de tecnología en específico y el motivo de usarla?
¿Cuál creen que sea el aporte de esta tecnología a la cuidad?
¿Qué preocupación les causa el uso que se le dará a este sistema?
¿Qué recomendarían a el grupo de políticos de la cuidad responsables de tomar las decisiones de implementar estas tecnologías?
¿Qué otra manera habría de resolver el problema que esta tecnología esta designada a resolver?

La Acyclica

Pregunta: ¿Qué piensan de este sistema de tecnología en específico y el motivo de usarla? (Como se usa y cuál es el uso)

- Bien, la tecnología ayuda con la velocidad o el movimiento de los coches.
- La información se guarda y analizan por donde viajas o cuantas veces cruzas este rastreo.

- Si es solo para ver el tráfico está bien.

- Está bien en algunas partes. Puede que sea algo bueno. Pero puede que esta tecnología pueda compartir información personal que puede ser utilizada de otra forma en especial si hay Hacking (forma negativa, uso de datos).

- La tecnología en sí no es tan grande (de tamaño) para ser algo visualmente desagradable. La información captada a través de estos medios puede que ayude a conducir el tráfico de mejor manera pero también puede que tome información personal.

Pregunta: Qué es lo que aporta esta tecnología a la ciudad?

- Seria algo bueno el aporte por la agilidad del tráfico solo si la tecnología está sincronizada con los semáforos, de otra manera no es útil si no aporta para el mejoramiento del tráfico.

- Participante dice que hay alternativas para esquivar el tráfico.

- Participante opina que la tecnología es interesante ya que usa google maps y está de acuerdo con el mejoramiento del tráfico.

- Si el objetivo es de mejorar el tráfico está de acuerdo. Pero también quiere saber en qué lugar(es) estarán los aparatos, si algunas personas serán beneficiadas más que otras.

Pregunta: Qué preocupaciones tienen con posible uso/uso potencial de esta tecnología?

- Le preocupa el uso de wifi en Acyclica porque pueden obtener toda la información de los teléfonos.

- Si el potencial puede ser aplicada a la inversión.

Enfocando al grupo: La tecnología ya está instalada, que les preocupa de su uso?

- El tráfico sigue igual.

- Quien usa o almacena la información.

- La preocupación es la colección de data.

Más de la mitad de grupo opina que esa (el almacén y colección de información) es la preocupación.

- Participante no está de acuerdo. No es la colección de data lo alarmante sino los recursos (dinero utilizado) ya que o la tecnología no están funcionando porque el tráfico sigue igual. No hay cambio con la nueva tecnología, esos gastos no son válidos ya que no hay resultados. Esos gastos pudieran ser utilizados para la comunidad.

- También tienen que ver si la tecnología emite radiación o alguna otra cosa dañina; perjudicial a la salud.

- El gobierno tiene todos los datos.

- Opinión de otro participante: No necesitan esta tecnología para tener los datos porque ya existen métodos para eso, incluso aplicaciones o alguna otra cosa.

La otra preocupación del grupo es que no haya un cambio al problema que se quiere resolver. En el caso de Acrylica sería el mejorar el tráfico.

- Tecnologías como esta necesitan recolectar más opiniones de expertos.

- Sería bueno que la información sea compartida con la comunidad. (Transparencia en fines y objetivos de la tecnología y datos guardados, tácticas implementadas.)

Pregunta: Le dirían algo a los políticos algo del lugar donde se encuentran estos aparatos?

- Hay lugares donde no se necesitan. En algunas partes de Magnolia, Queen Anne, Northgate, no se ocupan.

Seguimiento de pregunta: En las comunidades donde viven los latinos que tanto se ocupa Acyclica?

- Participante no cree que allí se ocupan.

Hablaron sobre la necesitad de puntos estratégicos y calles con más necesidad de ayuda por causa del tráfico.

Presentrador: Crees que Acylica es como el router de google?

- La tecnología no es un router, sino colección de data para planeaciones urbanas.

- Participante: “quiero creer” “convencerme” que los sensores están allí para ayudar con el tráfico.

- No se sabe cuándo las instalaron, los resultados deberían de ser públicos. Si la tecnología es para aliviar el flujo de tráfico entonces por qué no extienden el programa? O por qué no hay mejoramiento del tráfico?

Otra pregunta: Alguna otra tecnología que pueda ser utilizada en vez de Acyclica?

Alternativas:

- Alguna pantalla que indique cuáles vías son alternativas puede reemplazar esto.
- Cambios al límite de velocidad puede que alivie el flujo del tráfico.
- Dejar de construir tanto.
- Rediseño de calles ayudaría flujo de tráfico.
- El rediseñar las vías servirá para las futuras generaciones.

Tecnologia #2

Sensorlink/Binoculares

Pregunta: Que opina el grupo de la tecnología?

- Los binoculares son preocupantes si la persona no tiene ética. Es preocupante que una persona vea a través de binoculares a que una tecnología mida el uso de la electricidad.

- Un sensor que detecta la electricidad sería mejor.

- Al grupo le incomoda el uso de binoculares.

Pregunta: Qué opinas sobre la tecnología medidora de electricidad (sensorlink) y que sea usada en tu casa?

- No le incomoda o afecta a dos participantes.

- La preocupación sería que le quita el trabajo a una persona.

- Los binoculares son invasivos.

- Para que usar binoculares si es que se puede llegar a el hogar y ver el medidor en persona, pidiendo permiso? Si la tecnología es usa para ver que las personas se roban la electricidad, creen que no saben quiénes roban?

- El grupo cree que si saben.

Pregunta: Cual creen que sea el aporte que esta tecnología?

- El video dice que 3 millones de dólares son ahorrados.

Pregunta: De qué manera beneficia esto a la cuidad/ciudadanos/comunidad?

- El robo de la luz es preocupante.
- Si ya llevan el record y datos y le hacen saber a la comunidad puede que ahorren dinero.
- Uso de binoculares puede dar trabajo a una persona y dinero puede ser ahorrado con esta tecnología.
- La tecnología trae gasto de electricidad para poder ver gastos de luz? Si pretende evitar el robo entonces los gastos de la factura eléctrica deberían de seguir estables.

Pregunta: La confianza en estos medidores serán confiables? Serán efectivos?

- Ayuda a la precisión, a bajar precios.
- Que quiten los binoculares sería una sugerencia, o usar binoculares que graban con video.
- Si ya tienen récord sobre la energía (consumo, gastos, etc.), el robo de energía no es suficiente para establecer este tipo de tecnología ya que puede ser identificado el robo o alguna otra anomalía dependiendo en el nivel alto o bajo o repentino analizado/visto/detectado por métodos convencionales ya establecidos.
- Otra recomendación: Usar background check, uso de uniforme por trabajadores, cámara en binoculares.
- Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad
- .La preocupación es que no tan solo será para leer la electricidad sino para obtener otros tipos de información si cámaras fueran usadas.

Tecnologia #3 Coplogic

- Esta tecnología no solo el ahorro de tiempo, sino el ahorro de tiempo policial ya que ellos trabajarían en otras cosas
- El uso de computadora está bien para las denuncias.

- Si personas usan esta tecnología y es analizada en tiempo real por otras personas no hay problema.

Enfoque: Lo que estamos queriendo dialogar es el uso del internet y las denuncias.

- Es otro método para denunciar
- Está de acuerdo con el uso de computadoras para denunciar solo que no todos son capaz de usar este método/tecnología.

Pregunta: En que ayuda a la comunidad?

- Por qué usar estos métodos?
- Grupo están de acuerdo con su uso.
- Puede salvar una vida.
- Los riesgos y acciones determinan la urgencia de la intermisión policiaca.
- Alguna gente se siente más capaz de acudir a través de este sistema la tecnología en uso tiene validez.
- Bueno para la violencia doméstica.
- Las fallas electrónicas son preocupantes especialmente en reportes policiacos.
- Las preocupaciones es que el reporte no salió, no llegó por cualquier razón.
- No todos podrán o saben usar las computadoras.
- Fallas de los algoritmos o cuando o que promueve urgencia de cada demanda es alarmante.
- Criterio de demandas y que clase de preocupación de parámetros son confiables tienen que ser cuestionados/analizados, y que/quien es digno de prioridad o importancia o de ayuda.

Pregunta: De qué manera este uso beneficiaria a la comunidad?

- Personas pueden ser discriminadas

- Las personas le temen a los policías. Y este medio puede ayudar a que el miedo disminuya.

- La computadora decidirá la importancia/urgencia del reporte/emergencia dando a llevar acciones de emergencia.

- Gravedad de emergencia determina uso de tecnología.

Pregunta: Alguna inquietud sobre el uso de esta tecnología?

- La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

Pregunta: En qué situación usarán esta tecnología?

- Una pelea en la calle, un malestar corporal, cuestiones de vida, abuso doméstico
- Cada uno tiene la definición de vigilancia, pero que tal la definición de emergencia?
- La definición de emergencia es diferente con cada persona.
- Si nos basamos en la definición de emergencia sólo en cuanto estemos en peligro inmediato o en tiempos mínimos/ de transcurrencia alarmante/peligrosa el uso de será implementado o limitado solo a instantes inmediatos de peligro

Pregunta: Para qué sirve el reporte de la computadora?

- Para reportar algo que ya sucedió o que son recurrentes.
- Basado en el concepto de emergencia, las personas pueden tomar el método adecuado para reportar su caso y a través del medio necesario.
- Los reportes no son anónimos.
- Los datos son recolectados aun, a pesar de la opción escogida.

Pregunta: Qué les recomendarían a los políticos?

- Que sea multi-idioma, implementar audio, implementar sistemas que ayuden a múltiples personas con diversas capacidades/necesidades

Pregunta: Algún otro comentario en general sobre la tecnología de vigilancia?

- Si es usada de manera adecuada y como han dicho está bien.

- El uso de la tecnología es bueno para dar respuesta para todas las cosas y personas.

Consejo:

- Den información más información sobre lo que están haciendo. (transparencia/divulgación de información)

- Que haya más transparencia.

Ser transparentes sobre la colección de datos, para que haya discusiones y decisiones Informadas, en todas las tecnologías implementadas/por implementar.

Byrd Barr Place

2/28/2019 Surveillance Technology Focus Group

Thursday, February 28, 2019
1:42 PM

Disclaimer: some of these notes are written in first-person. These should not be considered direct quotes

Videos:

- Acyclica: sensors recognize when a wifi enabled device is in range of it. Attached to street lights
- 911 recorder: records the conversation with the person calling 911, and conversation with the dispatched officers
- CopLogic: Online police report, treated as a regular policy report
- Computer Aided Dispatch
- Seattle City Light: Binoculars for meter readers; sensor to see if someone is stealing electricity

Tom: Read definition of surveillance

Craig: invasion of privacy?

- Electric one: I never even know they had the sensor one.

Community Member: used to be in the tech industry for thirty years. Writing a book about surveillance and technology
Wanda: I like the online police report. If someone is experiencing a crisis or trauma, you can go ahead and report it.

- Surveillance, I understand the concern, but overall I think it's a good thing. There is good and bad in any location, you'll find people who are taking advantage of it, but hopefully there are systems in place.
- Used to work nights, and catching the bus at night is scary. Having the cameras and police out when catching the bus helps, I appreciate that. No one likes to be watched, but if it's gonna keep people safe, that's a good thing.

Mercy: security is a great safety issue
Craig: there are some parts of the neighborhood/city that need to be watched, and some that need to be left alone
Wanda: as long as it's even
Craig: Sometimes it's not even
Both: There are hot spots though

Which of the surveillance technologies do you think could be abused to pinpoint specific communities?

IG: The Computer Aided Dispatch

Talking about the International District:

- Lots of businesses and residential crammed together in a larger space
- Talking about a great community member who died; if they had surveillance technology them, maybe they would have found his killer

"Some neighborhoods need to be watched"

- Gangs; drug use

Tom: getting back to CAD, how do we feel about the information that is stored

- Craig: there are concerns, but who is allowed to see it, how is it stored? That's a concern
    - Is it used for BOLOs? Is it everyone who is in the area, all of the police officers? Or is there some discretion as to which police officers would be given the information?
- Wanda: plenty of people are arrested who "fit a description"
    - Discussion about the racial discrimination: how people who think that "all [insert race here] look alike".
    - Individuals may think like that, but police officers have the capability to ruin someone's life.
- Marjorie: just recently got a smart phone, and it's new to me that someone could know where I'm going and I wouldn't be aware of it
    - Without my consent.
- Mercy: grew up with the idea that big brother is watching you
    - Tracking how many times I go to the library seems like a waste of money
    - People who are not law abiding citizens, they are the ones to be worried
- Craig: What about selling weed, coke, etc. Should they be worried?
    - Mercy: well at least in Seattle, it's ok to sell
- Mercy: big brother is watching. We already know that, it's just more obvious now
- There is a lot of technology that we are not made aware of

Tom: So acyclica, is it worth it? Some people worried it's tracking, is it something that we can live without?

- Should we put up signs that this road is tracked?
    - Viron: Maybe
    - Mercy: let people out there know that you're on camera.
    - Viron: does it work if your device is not turned on?

Tom: what do you want to tell the city council about tech that is collecting personal information?

- Wanda: they should get our individual consent

- Martha: putting it on the ballot doesn't mean that you are getting individual consent, because if you vote no but it still passes, you didn't give your consent
- Deana: there are some places around Capitol Hill that I don't feel safe at at night
    - Talking about fire department responding to a fire in her building: when one building alarm system goes off, it goes directly to the fire department - affects multiple buildings.
        - Response time is very good.
    - I choose to turn off the GPS tracking, because I don't need people to know where I'm at
        - If others are watching where I'm at, that's an invasion of privacy. I should be able to walk out my front door and go wherever I want without anyone knowing.
- Location privacy: you can tell a lot about a person based on where they go, and tracking that can build a pretty extensive profile of who you are
- IG: now that I know they are tracking, I will turn it off.

Mr. Surveillance: Surveillance is always secret, and it's an aggressive act. It's meant to exert power over others.

Do you think any individual could raise enough concern that it would change anything?

- Resounding no
- Maybe with a larger group
    - Maybe with the whole city

SCL binoculars:

- Craig: they should warn their customers and let them know they are coming into their yard/looking through binoculars.
- Wanda: as long as they aren't looking in people's windows.
    - When we're walking down the street, it's a little different. Certain neighborhoods do need more surveillance than others

Regarding being watched in public:

- Eydie: in public, it depends on how long. If it's a short period of time, that's one thing, but if you're tracked the whole time you're out, it's unreasonable.
    - I don't know what the solutions would be.
    - Even when the meter read just walks into your yard, it's unnerving.
    - What’s the purpose of tracking it this way?
- Mercy: (referring to the acyclica) Why are they doing it all the time? Have they not gotten the information yet?
    - They should already know what the traffic flow would be.
    - We lost a lane to the bicyclist
- Craig: facial recognition used on the street is bad.
- Vyron: sometimes you can't walk down the street and shake someone's hand without getting in trouble

- Mr. Surveillance: The technology has gotten ahead of the law, and it means they have to pay less people

Tom: Are we willing to accept more technology to have less police?

- Craig: how about just making it even? Police have an image to people of color; they are afraid of why they are going to be there. We can police ourselves
- Wanda: I disagree. There are some who think there should be less, but there are also a lot of people who worry about walking down the street
    - As a woman and DV survivor, I appreciate the police and appreciate living in a country where I can call a number for help.
    - I have a big problem with the shooting of unarmed black men, but as an individual I still appreciate the police.
    - But I have a problem being tracked, and I have a problem being watched in my home.
- General comment: The number of police being on the corner is a touchy situation
    - Knowing the police that are on your corner makes a difference. They can police the community better if there is more of a relationship between the two.
- Craig: it has to be both, even. You can't trade off the technology for the police.
- Mr. Surveillance: The trend is they want to go to more technology and less police.

Tom: If right now we have lots of technology, and we want a balance, then how do we do that?

- Craig: keep it the way it is but clean up the police department. Make sure the people who are working there are good at their jobs, not biased or discriminating

CopLogic: making police reports online

- Craig: I think it's stupid.
    - Would use that technology for stupid crimes
- Mercy: you could report your neighbor for silly things
    - Anonymous reporting of crimes that could target people for things they might not call 911 for
- Wanda: there were some lines of traffic where I saw cars lined up with their windows smashed in; nothing taken, but glass all over the place.
    - Police response when called: maybe you should get a cheaper type of car
    - Would he have said that to us if we were a different skin color, or lived in a different neighborhood?
- IG: I think it's a bad thing: someone could make up a story and the officer didn’t have to check it.
- Marjorie: I think the online reporting could be abused

Appendix E: All Comments Received from Members of the Public

ID: 10617592348
Submitted Through: Survey Monkey
Date: 3/25/2019 12:51:06 PM
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Sensorlink Check Meter Device
What concerns, if any, do you have about the use of this technology?
Medium Concern: The draft SIR says that the data is retrieved from the device "via secure radio protocol", but the SIR never explains that in more detail. Radio frequencies are not inherently secure, so the SIR should specify how this communication channel is supposedly secured so as to prevent other (knowledgeable) passerby from retrieving the data. Other Concerns: Originally, one of my other concerns was that the Check Meter Device (aka SensorLink Transformer Meter System (TMS)) would collect more types of data and at a finer granularity of occurrence than what the normal functioning household meter would collect. However, the SCL staff at the SIR tech fair said it collects the same kinds of data as a normal meter, just that it's located upstream, thus addressing my concerns on that. With that in mind, most of my concerns are alleviated (aside from the radio protocol details) by the fact that the CDT crew is small ("five journey-level engineers"), the "CDT owns six SensorLink TMS units", that the "CDT only investigates specific, metered locations previously identified and properly documented as sites of suspected current diversion", and that mis-use/abuse of this technology would likely not be compliant with IBEW Local 77 & Energy Northwest's "Code of Excellence Program" (http://www.ibew77.com/Letter%20of%20Agreement%20IBEW%20Code%20of%20Excellence%20Energy%20NW.pdf). Additionally, even with those items in mind, SCL might be using the TMS devices and enforcement mechanisms at location/for households disproportionately based on race or other minority characteristics. To that end, I was happy to see in the SIR that "City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible." Hopefully, there are sufficient other programs/discounts for low-income individuals such that people never feel the need to resort to manipulating their electrical system (but I'm not familiar enough with SCL's offerings for low-income individuals, nor have I been low-income while living in Seattle, so I can't make that claim with 100% certainty).
What value, if any, do you see in the use of this technology?
There is a direct monetary cost to current diversion, thus identifying it and recouping the costs helps the city save money.
What do you want City leadership to consider about the use of this technology?
City leadership should ask to review SCL's "equity analysis of past enforcement locations". Additionally, (if not included in said analysis) City leadership should specifically inquire as to what percentage of people/households that were enforcement locations would also be considered low-income. If that percentage is high, then that likely means SCL may cause people to be jailed for effectively being poor (and resourceful); and SCL may have inadequate support offerings for people who are low-income.
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

ID: 10617585382

Submitted Through: Survey Monkey
Date: 3/25/2019 12:48:12 PM
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars / Spotting Scope
What concerns, if any, do you have about the use of this technology?
My concerns are largely alleviated by the fact that the "binoculars are standard, commercial-grade, unpowered binoculars...[without] any special enhancements requiring power (e.g., night-vision or video-recording capabilities)", the CDT crew is small ("five journey-level engineers"), the binoculars are used "for approximately one minute at a time in those cases where an initial investigation has been authorized by the Current Diversion Coordinator", they're only used " to read a meter from a distance when the CDT is otherwise unable to access physically the meter for the purpose of inspection upon suspected current diversion", and that mis-use/abuse of this technology would likely not be compliant with IBEW Local 77 & Energy Northwest's "Code of Excellence Program" (http://www.ibew77.com/Letter%20of%20Agreement%20IBEW%20Code%20of%20Excellence%20Energy%20NW.pdf). Additionally, even with those items in mind, SCL might be using the binoculars and enforcement mechanisms at location/for households disproportionately based on race or other minority characteristics. To that end, I was happy to see in the SIR that "City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible." All things considered then, I'm hopeful that SCL is on the right track. Hopefully, there are sufficient other programs/discounts for low-income individuals such that people never feel the need to resort to manipulating their electrical system (but I'm not familiar enough with SCL's offerings for low-income individuals, nor have I been low-income while living in Seattle, so I can't make that claim with 100% certainty).
What value, if any, do you see in the use of this technology?
There is a direct monetary cost to current diversion, thus identifying it and recouping the costs helps the city save money.
What do you want City leadership to consider about the use of this technology?
City leadership should ask to review SCL's "equity analysis of past enforcement locations". Additionally, (if not included in said analysis) City leadership should specifically inquire as to what percentage of people/households that were enforcement locations would also be considered low-income. If that percentage is high, then that likely means SCL may cause people to be jailed for effectively being poor (and resourceful); and SCL may have inadequate support offerings for people who are low-income.
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

ID: 10617574681
Submitted Through: Survey Monkey
Date: 3/25/2019 12:45:12 PM
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Ampstick
What concerns, if any, do you have about the use of this technology?
My concerns are largely alleviated by the fact that there's only 4 Ampstick devices, "they are deployed by hand for approximately ten minutes at a time, only when suspected diversion cases occur", and can only measure one 'line' at a time. Additionally, even with those items in mind, SCL might be using the Ampsticks and enforcement mechanisms at location/for households disproportionately based on race or other minority characteristics. To that end, I was happy to see in the SIR that "City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible." All things considered then, I'm hopeful that SCL is on the right track. Hopefully, there are sufficient other programs/discounts for low-income individuals such that people never feel the need to resort to manipulating their electrical system (but I'm not familiar enough with SCL's offerings for low-income individuals, nor have I been low-income while living in Seattle, so I can't make that claim with 100% certainty).
What value, if any, do you see in the use of this technology?
There is a direct monetary cost to current diversion, thus identifying it and recouping the costs helps the city save money.
What do you want City leadership to consider about the use of this technology?
City leadership should ask to review SCL's "equity analysis of past enforcement locations". Additionally, (if not included in said analysis) City leadership should specifically inquire as to what percentage of people/households that were enforcement locations would also be considered low-income. If that percentage is high, then that likely means SCL may cause people to be jailed for effectively being poor (and resourceful); and SCL may have inadequate support offerings for people who are low-income.
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

ID: 10617441686
Submitted Through: Survey Monkey
Date: 3/25/2019 11:51:11 AM
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars / Spotting Scope
What concerns, if any, do you have about the use of this technology?
none
What value, if any, do you see in the use of this technology?
It's a good way to spot problems and get readings.
What do you want City leadership to consider about the use of this technology?
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

ID: 10600927069
Submitted Through: Survey Monkey
Date: 3/18/2019
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars
What concerns, if any, do you have about the use of this technology?
What a joke. The city has spent millions of dollars converting to digital meters that automatically report usage. Nobody needs binoculars to read them!
What value, if any, do you see in the use of this technology?
Zero
What do you want City leadership to consider about the use of this technology?
Forget it.
Do you have any other comments?
No
Are there any questions you have, or areas you would like clarification?

ID: 10
Submitted Through: Focus Group
Date: 2/28/2019
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars
What concerns, if any, do you have about the use of this technology?
the use of the binoculars can be an invasion of privacy. Period of three days is too vast a window to give note. The lack of knowledge in different standards of privacy by different tenants
What value, if any, do you see in the use of this technology?
What do you want City leadership to consider about the use of this technology?
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

ID: 9
Submitted Through: Focus Group
Date: 2/28/2019
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars
What concerns, if any, do you have about the use of this technology?
ensure that all tenants are aware of the use of binoculars
What value, if any, do you see in the use of this technology?
none. It honestly appears outdated especially with automatic meters being available
What do you want City leadership to consider about the use of this technology?
I would recommend phasing it out completely. If not, ensure that all tenants know that this decision is being made for them.
Do you have any other comments?
I would not assume that all consumers are literate. Have other ways to communicate with individuals such as phone call, news outlets
Are there any questions you have, or areas you would like clarification?

ID: 3
Submitted Through: Focus Group
Date: 2/27/2019
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars, SCL: CheckMeter, SCL: AmpFork, SFD: CAD, SPD: CAD, SPD: 911 Logging Recorder
What concerns, if any, do you have about the use of this technology?
That would be good with advanced technology
What value, if any, do you see in the use of this technology?
Yes, around the city.
What do you want City leadership to consider about the use of this technology?
Need good train to people who use new technologies
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

ID: 10550713652
Submitted Through: Survey Monkey
Date: 2/23/2019 12:12:23 PM
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars
What concerns, if any, do you have about the use of this technology?
This is playing outrageous. Well we are telling the public is that it is okay for a city worker to come and use binoculars to look into your private property.
What value, if any, do you see in the use of this technology?
This really is barbaric there are certain technologies that their intermediate benefit might be greater than the risk that provide a much more simple solution then this solution. This solution a binocular use can possibly be interpreted for many things ho
What do you want City leadership to consider about the use of this technology?
It's just not right.
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

Appendix F: Department Responses to Public Inquiries

City Light received the following questions for Group 2 surveillance technologies during the public comment period of Feb. 5, 2019 to March 26, 2019. City Light's answers to the questions, which solely related to City Light's use of binoculars for current diversion detection, are presented below.

Do Seattle City Light Current Diversion employees wear something visible that shows customers they are from Seattle City Light?

Seattle City Light employees who are working in the field can be identified by their Seattle City Light ID badge and a hard hat.

If a City Light customer wants to file a complaint about a City Light employee, how do they do that?

A customer can file a complaint about a City Light employee by contacting Customer Care at (206) 684-3000, via email, mail, or in person at the Customer Service Center in the Seattle Municipal Tower located at 700 Fifth Ave., 4th floor lobby, Seattle, WA 98104.

Has there been a situation where a customer sees a City Light employee looking at someone's house with binoculars and the customer may not have been notified?

No advance notification is provided to the public, as doing so may compromise the detection of current diversion on a single, previously suspected service-drop location. Current Diversion staff view locations that are in public view, so it is possible other customers have observed this work. However, staff use binoculars for approximately one-minute at a time and only for City Light business purposes.

Has there been a situation where the meter was located on the opposite side of where the City Light employee was looking?

The Current Diversion team only investigates specific meters and other implicated electrical equipment at locations previously identified and documented as sites of suspected current diversion. Binoculars are used only to make determinations about whether current diversion is likely taking place, and, in certain instances, to view implicated and potentially dangerous electrical equipment.

Do City Light employees get background checks?

City Light conducts job-related background checks prior to hire in order to ensure a safe and secure work environment in which employees, the public, resources, and assets are protected, while protecting the integrity and confidentiality of information gathered during the evaluation. In most cases, a background check will be conducted for the finalist following a contingent offer of employment. Offer letters issued prior to completion of the background check will notify the finalist that the offer is contingent upon successful completion of any and all required background checks. In addition, City Light personnel whose work duties require having critical

access to City Light physical and logical assets must have a background check prior to being granted such access, which is renewed at least once every four years.

If a City Light customer files a complaint against an employee, are complaints being followed up? What is the average time for disciplinary action for a City Light employee? How long is the process for a full investigation?

Yes. City Light customer complaints about employee conduct are generally escalated to the People & Culture team at City Light for further action in order to ensure that City Light employees are serving customers reliably and with integrity. Appropriate next steps to address employee conduct are determined on a case-by-case basis. The complaining customer may not be informed of the specific action taken by City Light, due to the confidential nature of personnel matters. However, City Light is committed to employee accountability and providing excellent customer service.

When a full fact-finding investigation is necessary, it is City Light's objective to complete it as promptly as possible while ensuring that the investigation is fair, complete, and impartial. In the event of harassment, discrimination, or retaliation allegations, it is City Light's objective to complete investigations within 90 days unless compelling circumstances require more time. The duration of investigations is often dependent upon the availability and cooperation of witnesses, the volume of relevant documents, as well as the complexity of the subject-matter at issue. Resulting disciplinary and follow-up actions after an investigation are completed as promptly as possible while respecting the due process rights of City Light employees.

What is the purpose of tracking current diversion by using binoculars?

Binoculars may be used to address meter access issues, such as locked gates, unsafe premises, or threatening dogs. The binoculars enable Current Diversion staff to evaluate if a meter has been tampered with to substantiate suspicions of current diversion.

Appendix G: Letters from Organizations or Commissions

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

March 12th, 2019

Seattle City Council
600 4th Ave
Seattle, WA 98104

Re: Surveillance Ordinance Group 2 Public Comment

We would like to first thank City Council for passing one of the strongest surveillance technology policies in the country, and thank Seattle IT for facilitating this public review process.

These public comments were prepared by volunteers from the Community Technology Advisory Board (CTAB) Privacy & Cybersecurity Committee, as part of the surveillance technology review defined in Ordinance 125376. These volunteers range from published authors, to members of the Seattle Privacy Coalition, to industry experts with decades of experience in the information security and privacy sectors.

We reviewed and discussed the Group 2 Surveillance Impact Reports (SIRs) with a specific emphasis on privacy policy, access control, and data retention. Some recurring themes emerged, however, that we believe will benefit the City as a whole, independent of any specific technology:

- **Interdepartmental sharing of privacy best practices**: When we share what we've learned with each other, the overall health of the privacy ecosystem goes up.
- **Regular external security audits**: Coordinated by ITD (Seattle IT), routine third-party security audits are invaluable for both hosted-service vendors and on-premises systems.
- **Mergers and acquisitions**: These large, sometimes billion-dollar ownership changes introduce uncertainty. Any time a vendor, especially one with a hosted service, changes ownership, a thorough review of any privacy policy or contractual changes should be reviewed.
- **Remaining a Welcoming City**: As part of the Welcoming Cities Resolution, no department should comply with a request for information from Immigration and Customs Enforcement (ICE) without a criminal warrant. In addition, the privacy of all citizens should be protected equally and without consideration of their immigration status.

Sincerely,

Privacy & Cybersecurity Committee volunteers
Torgie Madison, Co-Chair
Smriti Chandashekar, Co-Chair
Camille Malonzo
Sean McLellan
Kevin Orme
Chris Prosser
Rabecca Rocha
Adam Shostack
T.J. Telan

Community Technology Advisory Board
Steven Maheshwary, CTAB Chair
Charlotte Lunday, CTAB Co-Vice Chair
Torgie Madison, CTAB Co-Vice Chair
Smriti Chandashekar, CTAB Member
Mark DeLoura, CTAB Member
John Krull, CTAB Member
Karia Wong, CTAB Member

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SFD: Computer-Aided Dispatch (CAD)

Comments

The use of a centralized Computer-Aided Dispatch (CAD) system is essential to protecting the health and safety for all Seattle citizens. The National Fire Protection Association (NFPA) standards outline specific alarm answering, turnout, and arrival times[1] that could only be accomplished in a city of this size with a CAD system.

In addition, with over 96,000 SFD responses per year (2017)[2], only a computerized system could meet the state's response reporting guidelines established in RCW 35A.92.030[3].

CentralSquare provides the dispatch service used by SFD. CentralSquare is a new entity resulting from the merger of Superion, TriTech, Zuercher, and Aptean[4] in September 2018.

Recommendations

- Tritech, the underlying technology supplying SFD with CAD services, has been in use since 2003 [SIR 4.3], making it 16 years old. As with any technology, advancements in security, speed, usefulness, and reliability come swiftly. Due to the age of the technology, we recommend conducting a survey into the plausibility of replacing Tritech as SFD's CAD solution.

- Tritech was merged very recently into CentralSquare in one of the largest-ever government technology mergers to date. Due diligence should be exercised to ensure that this vendor is keeping up to date with industry best practices for security and data protection, and that their privacy policies are still satisfactory after the CentralSquare merger. We recommend ensuring that the original contracts and privacy policies have remained unchanged as a result of this merger.

---

[1] "NFPA Standard 1710." https://services.prod.iaff.org/ContentFile/Get/30541
[2] "2017 annual report - Seattle.gov." https://www.seattle.gov/Documents/Departments/Fire/FINAL%20Annual%20Report_2017.pdf
[3] "RCW 35A.92.030: Policy statement—Service ... - Access WA.gov." https://app.leg.wa.gov/rcw/default.aspx?cite=35A.92.030
[4] "Superion, TriTech, Zuercher, and Aptean's Public Sector Business to " 5 Sep. 2018, https://www.tritech.com/news/superion-tritech-zuercher-and-apteans-public-sector-business-to-form-centra

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SDOT: Acyclica

Comments

Traffic congestion is an increasingly major issue for our city. Seattle is the fastest-growing major city in the US this decade, at 18.7% growth, or 114,00 new residents[5]. Seattle ranks sixth in the nation for traffic congestion[6]. The need for intelligent traffic shaping and development has never been greater. Acyclica, a service provided by Western Systems and now owned by FLIR[7], is an implementation of surveillance technology specifically designed to address this problem.

We were happy to see the 2015 independent audit of Acyclica's systems [SIR 8.2]. This is an excellent industry best practice, and one that we'll be recommending to other departments throughout this document.

In addition, we are pleased to see the hashing function's salt value rotated every 24-hours [SIR 4.10]. This ensures that even the 10-year retention policy [SIR 5.2] cannot be abused to correlate multiple commute sessions and individually identify a person.

Recommendations

- FLIR Systems' acquisition of Acyclica is a recent development (September 2018). We recommend verifying that the Western Systems terms [SIR 3.1] still apply. If they have been superseded by new terms from FLIR Systems, those should be subject to an audit by SDOT and Seattle IT. Specifically, section 2.5.1 of Western Systems' terms must still apply:

  > 2.5.1. It is the understanding of the City that the data gathered are encrypted to fully eliminate the possibility of identifying individuals or vehicles. In no event shall City or Western Systems and its subcontractors make any use of the data gathered by the devices for any purpose that would identify the individuals or vehicles included in the data.

- FLIR Systems is known primarily as an infrared technology vendor. Special care should be taken if FLIR/Acyclica attempt to couple IR scanning with WiFi/MAC sniffing. Implementation of an IR system would necessitate a new public surveillance review.

---

[5] "114,000 more people: Seattle now decade's fastest-growing big city in ...." 24 May. 2018, https://www.seattletimes.com/seattle-news/data/114000-more-people-seattle-now-this-decades-fastest-growing-big-city-in-all-of-united-states/
[6] "INRIX Global Traffic Scorecard." http://inrix.com/scorecard/
[7] "FLIR Systems Acquires Acyclica | FLIR Systems, Inc.." 11 Sep. 2018, http://investors.flir.com/news-releases/news-release-details/flir-systems-acquires-acyclica

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SCL: Binoculars, Check Meter, SensorLink

Comments

As these three technologies are serving the same team and mission objectives, we will review them here in a combined section.

The mission of the Current Diversion Team (CDT) is to investigate and gather evidence of illegal activity related to the redirection and consumption of electricity without paying for its use. As such, none of these technologies surveil the public at large. They instead target specific locations and equipment, albeit without the associated customer's knowledge.

It appears as though all data collected through the Check Meter Device and SensorLink Amp Fork are done without relying on a third-party service, so the usual scrutiny of a vendor's privacy policies does not apply.

Recommendations

- **Binoculars**: We have no recommendations for the use of binoculars.
- **Check Meter Device & SensorLink Amp Fork**: As noted in the comments above, we have no further recommendations for the use of the Check Meter Device and SensorLink Amp Fork technologies.
- **Racial Equity**: As with any city-wide monitoring practice, it can be easy to more closely scrutinize one neighborhood over another. Current diversion may be equally illegal (and equally prevalent) across the city, but the enforcement of this law may be unevenly applied. This could introduce racial bias by disproportionately burdening specific neighborhoods with a higher level of surveillance.

  As described, DPP 500 P III-416 section 5.2[8] asserts that all customers shall receive uniform consideration [SIR RET 1.7]. To ensure this policy is respected, we encourage City Light to track and routinely review the neighborhoods where CDT performs investigations, with a specific emphasis on racial equity. This information should be made publicly available.

  When asked at the February 27th Surveillance Technology public meeting, SDOT indicated that no tracking is currently being done on where current diversion is enforced.

[8] "SCL DPP 500 P III-416 Current Diversion - Seattle.gov." 11 Jan. 2012, http://www.seattle.gov/light/policies/docs/III-416%20Current%20Diversion.pdf

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: 911 Logging Recorder

Comments

This is a technology that the general public would likely already assume is in place. Some of the more sensational 911 call logs have been, for example, played routinely on the news around the country. Since it would not alarm the public to know that 911 call recording is taking place, our recommendations will focus primarily on data use, retention, and access control.

Call logging services are provided by NICE Ltd., an Israeli company founded in 1986. This vendor has had a troubling history with data breaches. For example, a severe vulnerability discovered in 2014 allowed unauthorized users full access to a NICE customer's databases and audio recordings[9]. Again, in 2017, a NICE-owned server was set up with public permissions, exposing phone numbers, names, and PINs of 6 million Verizon customers[10].

Recommendations

- SIR Appendix K includes a CJIS audit performed in 2017. SIR section 4.10 also mentions that ITD (Seattle IT) periodically performs routine monitoring of the SPD systems.

  However, given the problematic history with the quality of the technology vendor, if any of the NICE servers, networks, or applications were installed by the vendor (or installation was overseen/advised by the vendor), we recommend an external audit of the implementation of the call logging technology.

- SIR sections 3.3 and 4.2 outline the SPD-mandated access control and data retention policies, however it is not apparent if there is a policy that strictly locks down the use of this technology to a well-defined list of allowed cases. We recommend formally documenting the allowed 911 Logging use cases, and creating a new SIR for any new desired applications of this technology.

  With a 90-day retention policy [SIR 4.2], and with SPD receiving 900,000 calls per year[11], there are about 220,000 audio recordings existing at any given time. This is enough for a data mining, machine learning, or voice recognition project.

---

[9] "Backdoor in Call Monitoring, Surveillance Gear — Krebs on Security." 28 May. 2014, https://krebsonsecurity.com/2014/05/backdoor-in-call-monitoring-surveillance-gear/
[10] "Nice Systems exposes 14 million Verizon customers on open AWS ...." 12 Jul. 2017, https://www.techspot.com/news/70106-nice-systems-exposes-14-million-verizon-customers-open.html
[11] "9-1-1 Center - Police | seattle.gov." https://www.seattle.gov/police/about-us/about-policing/9-1-1-center

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: Computer-Aided Dispatch (CAD)

Comments

As mentioned in the section "SFD: Computer-Aided Dispatch (CAD)" and the section "SPD: 911 Logging Recorder", these dispatch technologies are mandatory for functional emergency services of a city this size. No other system would be able to meet the federal- and state-mandated response times and reporting requirements.

SIR section 4.10 mentions that ITD (Seattle IT) performs routine inspections of the Versaterm implementation.

Versaterm, founded in 1977, provides the technology used by SPD's CAD system. SPD purchased this technology in 2004. In September of 2016, there was a legal dispute between Versaterm and the City of Seattle over a Public Records Act (PRA) disclosure of certain training and operating manuals[12]. The court ruled in favor of Versaterm.

Recommendations

- It is not immediately clear what use cases are described in SIR 2.5 describing data access by "other civilian staff whose business needs require access to this data". All partnerships and data flows between SPD and businesses should be explicitly disclosed.

- This system has been in place for 15 years. As with any technology, advancements in security, speed, usefulness, and reliability come swiftly. Due to the age of the technology, and the potential damaged relationship between Seattle and Versaterm due to the aforementioned legal dispute, we recommend conducting a survey into the plausibility of replacing Versaterm as SPD's CAD solution.

- As mentioned in the introduction to this document, Seattle has adopted the Welcoming Cities Resolution[13]. In honoring this resolution, we recommend that SPD never disclose identifying information, from CAD or any system, to Immigrations and Customs Enforcement (ICE) without a criminal warrant.

[12] "Versaterm Inc. v. City of Seattle, CASE NO. C16-1217JLR | Casetext." 13 Sep. 2016, https://casetext.com/case/versaterm-inc-v-city-of-seattle-2
[13] "Welcoming Cities Resolution - Council | seattle.gov." http://www.seattle.gov/council/issues/past-issues/welcoming-cities-resolution

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: CopLogic

Comments

Track 1 - Public reporting of no-suspect, no-evidence, non-emergency crimes

CTAB understands that in cases where no evidence or suspect is available, a crime should be reported (for statistical or insurance purposes) but does not require the physical appearance of an SPD officer.

Track 2 - Retail Loss Prevention

This track is more problematic, as it could be used by retailers as a method to unreasonably detain, intimidate, or invade the privacy of a member of the public accused of, but not proven guilty of, shoplifting.

Recommendations

- **Track 2**: If not already done, retailers should be trained and informed that having a CopLogic login does not allow them to act as if they are law enforcement officers. Members of the public suspected of shoplifting need to have an accurate description of their rights in order to make informed decisions before providing identifying information. Retailers are also held to a lower standard than SPD regarding racial bias. It is virtually guaranteed that people of color are disproportionately apprehended and entered into the retail track of CopLogic.

  We recommend discontinuing Track 2 entirely.

- **Track 1 & 2**: If not already done, SPD, in coordination with Seattle IT, should perform or hire a company to perform an audit of the vendor's systems. If this audit has not been performed in the 8 years since purchasing this system, it should absolutely be done before the 10-year mark in 2020.
- **Track 1 & 2**: It is not immediately clear in the SIR or LexisNexis's Privacy Policy what CopLogic does with these records long-term, after SPD has imported them into their on-premises system. A written statement from LexisNexis on how this data is used, mined, or sold to affiliates/partners should be acquired by SPD.
- **Track 1 & 2**: We recommend migrating CopLogic to an on-premises solution. We found the LexisNexis privacy policy to be obfuscated and vague[14]. Such sensitive information should not be protected by trust alone.

[14] "Privacy Policy | LexisNexis." 7 May. 2018, https://www.lexisnexis.com/en-us/terms/privacy-policy.page

City of Seattle

AMERICAN CIVIL LIBERTIES UNION
Washington

901 Fifth Ave, Suite #630
Seattle, WA 98164
(206) 624-2184
aclu-wa.org

Tana Lin
Board President

Michele Storms
Executive Director

Shankar Narayan
Technology & Liberty Project Director

March 20, 2019

RE: ACLU-WA Comments Regarding Group 2 Surveillance Technologies

Dear Seattle IT:

On behalf of the ACLU of Washington, I write to offer our comments on the surveillance technologies included in Group 2 of the Seattle Surveillance Ordinance process. We are submitting these comments by mail and electronically because they do not conform to the specific format of the online comment form provided on the CTO's website, and because the technologies form groups in which some comments apply to multiple technologies.

These comments should be considered preliminary, given that the Surveillance Impact Reports (SIR) for each technology leave a number of significant questions unanswered. Specific unanswered questions for each technology are noted in the comments relating to that technology, and it is our hope that those questions will be answered in the updated SIR provided to the Community Surveillance Working Group and to the City Council prior to their review of that technology. In addition to the SIR, our comments are also based on independent research relating to the technology at hand.

The 8 technologies in Group 2 are covered in the following order.

I. Acyclica (SDOT)

II. CopLogic (SPD)

III. Computer-Aided Dispatch & 911 Logging Recorder Group

1. Computer-Aided Dispatch (SPD)
2. Computer-Aided Dispatch (SFD)
3. 911 Logging Recorder (SPD)

IV. Current Diversion Technology Group

1. Check Meter Device (Seattle City Light)
2. SensorLink Amp Fork (Seattle City Light)
3. Binoculars/Spotting Scope (Seattle City Light)

I. Acyclica - SDOT

Background

Acyclica technology is a powerful location-tracking technology that raises a number of civil liberties concerns because of its ability to uniquely identify individuals and their daily movements. Acyclica (via its hardware vendor, Western Systems), manufactures Intelligent Transportation System (ITS) sensors called RoadTrend that are used by the Seattle Department of Transportation for the stated purpose of traffic management. These RoadTrend sensors collect encrypted media access control (MAC) addresses, which are transmitted by any Wi-Fi enabled device including phones, cameras, laptops, and vehicles. Collection of MAC addresses, even when hashed (a method of de-identifying data irreversibly),[1] can present locational privacy challenges.

Experts analyzing a dataset of 1.5 million individuals found that just knowing four points of approximate spaces and times that individuals were near cell antennas or made a call were enough to uniquely identify 95% of individuals.[2] In the case of Acyclica's operation in Seattle, the dataset is comprised of MAC addresses recorded on at least 301 intersections,[3] which allows Acyclica to generate even more precise location information about individuals. Not only do the RoadTrend sensors pick up the MAC addresses of vehicle drivers and riders, but these sensors can also pick up the MAC addresses of all nearby individuals, including pedestrians, bicyclists, and people in close structures (e.g., apartments, offices, and hospitals). Acyclica technology's location tracking capabilities means that SDOT's use of Acyclica can not only uniquely identify individuals with ease, but can also create a detailed map of their movements. This raises privacy concerns for Seattle residents, who may be tracked without their consent by this technology while going about their daily lives.

These location-tracking concerns are exacerbated by the lack of clarity around whether SDOT has a contract with Acyclica (see below). Without a contract, data ownership and scope of data sharing and repurposing by Acyclica is unclear. For example, without contractual restrictions, Acyclica

[1] Hashing is a one-way function that scrambles plain text to produce a unique message digest. Unlike encryption—which is a two-way function, allowing for decryption—what is hashed cannot be un-hashed. However, hashed location data can still be used to uniquely identify individuals. While it is infeasible to compute an input given only its hash output, pre-computing a table of hashes is possible. These types of tables consisting of pre-computed hashes and their inputs are called rainbow tables. With a rainbow table, if an entity has a hash, then they only need to look up that hash in their table to then know what the original MAC address was.
[2] Montjoye, Y., Hidalgo, C., Verleysen, M., and Blondel, V. 2013. Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports.* 3:1375.
[3] The SIR states that SDOT has 301 Acyclica units installed throughout the City. However, an attached location excel sheet in Section 2.1 lists 389 Acyclica units, but only specifies 300 locations.

would be able to share the raw data (i.e., the non-aggregated, hashed data before it is summarized and sent to SDOT) with any third parties, and these third parties would be able to use the data in any way they see fit, including combining the data with additional data such as license plate reader or facial recognition data. Acyclica could also share the data with law enforcement agencies that may repurpose the data, as has happened with other City data. For example, in 2018, U.S. Immigration and Customs Enforcement (ICE) approached Seattle City Light with an administrative subpoena demanding information on a particular customer location, including phone numbers and information on related accounts.[4] ICE also now has agency-wide access to a nationwide network of license plate readers controlled by Vigilant Solutions,[5] indicating the agency may seek additional location data for immigration enforcement purposes in the future. Data collected via Acyclica should never be used for law enforcement purposes.

The uncertainty around the presence or absence of a contract contributes to two key issues: (1) lack of a clearly defined purpose of use of Acyclica technology; and (2) lack of clear restrictions on the use of Acyclica technology that track that purpose. With no contract, SDOT cannot enforce policies restricting the use of Acyclica technology to the intended purpose.

There are also a number of contradictory statements in the SIR concerning the operation of Acyclica technology,[6] as well as discrepancies between the SIR, the information shared at the technology fair (the first public meeting to discuss the Group 2 technologies),[7] and ACLU-WA's conversation with the President of Acyclica, Daniel Benhammou. All these leave us with concerns over whether SDOT fully understands (and the SIR reflects) the capabilities of the technology. In addition, there remain a number of critical unanswered questions that the final SIR must address (set forth below).

Of additional concern is the recent acquisition of Acyclica by FLIR Systems, an infrared and thermal imaging company funded by the U.S. Department of Defense.[8] As of March 2019, FLIR has discontinued Acyclica RoadTrend sensors.[9] Neither the implications of the FLIR acquisition nor the discontinuation of the RoadTrend sensors are mentioned in the SIR—but if the sensors used will change, the SIR should make clear how that will impact the technology.

a. Specific Concerns

- *Inadequate Policies Defining Purpose of Use.* Policies cited in the SIR are vague,

[4] https://crosscut.com/2018/02/immigration-officials-subpoena-city-light-customer-info
[5] https://www.theverge.com/2018/3/1/17067188/ice-license-plate-data-california-vigilant-solutions-alpr-sanctuary
[6] Explained in further detail in 1. Acyclica – SDOT *Major Concerns* below.
[7] http://www.seattle.gov/tech/initiatives/privacy/events-calendar#/ri=3
[8] https://www.crunchbase.com/acquisition/flir-systems-acquires-acyclica--e6043a1a#section-overview
[9] https://www.flir.com/support/products/roadtrend#Specifications

short, and impose no meaningful restrictions on the purposes for which Acyclica devices may be used.[10] Section 1.1 of the abstract set forth in the SIR states that Acyclica is used by over 50 agencies to "to help to monitor and improve traffic congestion." Section 2.1 is similarly vague, providing what appear to be examples of some types of information the technology produces (e.g., calculated average speeds) in order to facilitate outcomes (correcting traffic signal timing, providing information to travelers about expected delays, and allowing SDOT to meet traffic records and reporting requirements)—but it's not clear this list is exhaustive. Section 2.1 fails to describe the purpose of use, all the types of information Acyclica provides, and all the types of work that Acyclica technology facilitates. All these must be clarified.

- *Lack of Clarity on Whether Acyclica and SDOT have a Written Contract.* The SIR does not state that any contract exists, and in the 2018 conversation ACLU-WA had with Benhammou, he stated that there was no contract between the two parties. However, at the 2019 technology fair, the SDOT representative affirmatively stated that SDOT has a contract with Acyclica. As previously mentioned, the lack of a contract limits SDOT's ability to restrict the scope of data sharing and repurposing. The only contractual document provided appears to be a terms sheet in Section 3.0 detailing SDOT's terms of service with Western Systems (the hardware vendor that manufactures the Acyclica RoadTrend sensors), which states that Western Systems only deals with the maintenance and replacement of the hardware used to gather the data, and not the data itself.

- *Lack of Clarity on Data Ownership.* At the technology fair, the SDOT representative stated that SDOT owns all the data collected (including the raw data), but the SIR only states that the aggregated traffic data is owned by SDOT. In the 2018 conversation, Benhammou stated that Acyclica owns all the raw data. There is an apparent lack of clarity between SDOT and Acyclica concerning ownership of data that must be addressed.

- *Data Retention Periods are Unclear.* Section 5.2 of the SIR states that there is a 10-year internal deletion requirement for the aggregated traffic data owned by SDOT, but pg. 37 of the SIR states that "the data is deleted within 24 hours to prevent tracking devices over time." In the 2018 interview, Benhammou stated that Acyclica retains all non-aggregated data indefinitely. It is unclear whether the different retention periods stated in the SIR are referring to different types of data. The lack of clarity on data retention periods also relates to the lack of clarity on data ownership given that data retention periods may depend on data ownership.

[10] As noted in 1. Acyclica – SDOT *Background* above.

- *Inaccurate Descriptions of Anonymization/Data Security Practices.* The SIR appears to use the terms "encryption" and "hashing" interchangeably in some parts of the SIR, making it difficult to clearly understand Acyclica's practices in this area. For example, Section 7.2 states: "Contractually, Acyclica guarantees that the data gathered is encrypted to fully eliminate the possibility of identifying individuals or vehicles." But by design, encryption allows for decryption with a key, meaning anyone with that key and access to the data can identify individuals. (Also, if there is no contract between SDOT and Acyclica, the use of 'contractually' is misleading). This language is also used in the terms sheet detailing SDOT's contract with Western Systems (in Section 2.5.1 in the embedded contract). The SIR compounds this confusion with additional contradictory statements. For example, the SIR states in multiple sections that the data collected by the RoadTrend sensors are encrypted and hashed on the actual sensor. However, according to a letter from Benhammou provided by SDOT representatives at the technology fair,[11] the data is never hashed on the sensor—the data is only hashed after being transmitted to Acyclica's cloud server. These contradictory descriptions cause concern.

- *No Restrictions on Non-City Data Use.* Section 6.3 of the SIR states that there are no restrictions on non-City data use. However, there are no policies cited making clear the criteria for such use, any inter-agency agreements governing sharing of Acyclica data with non-City parties, or why the data must be shared in the first place.

- *Not All Locations of Acyclica Devices are Specified.* Section 2.1 of the SIR states that there are 301 Acyclica locations in Seattle. However, in the embedded excel sheet detailing the serial numbers and specific intersections in which Acyclica devices are installed, there are 389 serial numbers, but only 300 addresses/locations specified. The total number and the locations of Acyclica devices collecting data in Seattle is unclear. This gives rise to the concern that there are unspecified locations in which Acyclica devices are collecting MAC addresses.

- *No Mention of RoadTrend Sensor Discontinuation.* As noted in the background,[12] Acyclica has been acquired by FLIR, an infrared and thermal imaging company. As of March 2019, FLIR's product webpage states that the Acyclica RoadTrend sensors (those currently used by SDOT) have been discontinued.[13] From the information we have, it is unclear if SDOT will be able to continue using the RoadTrend sensors described in the 2019 SIR. Given that FLIR sensors, such as the TrafiOne, have capabilities that go much farther than those of the

[11] Included in Appendix 1.
[12] As noted in 1. Acyclica – SDOT *Background* above.
[13] https://www.flir.com/support/products/roadtrend#Specifications

RoadTrend sensors (e.g., camera technology and thermal imaging)[14] as well as potentially different technical implementations, their use would give rise to even more serious privacy and misuse concerns. Neither the implications of the FLIR acquisition nor the discontinuation of the RoadTrend sensors are mentioned in the SIR.

- *No Mention of Protecting MAC Addresses of Non-Drivers/Riders (e.g., people in nearby buildings).* The Acyclica sensors will pick up the MAC addresses of all nearby individuals, regardless of whether they are or are not driving or riding in a vehicle. The SIR does not mention any steps taken to reduce the privacy infringements on non-drivers/riders.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- For what specific purpose or purposes will Acyclica be used, and what policies state this?
- Does SDOT have a contract with Acyclica, and if so, why is the contract not included in the SIR?
- Who owns the raw, non-aggregated data collected by Acyclica devices?
- What is the retention period for the different types of collected data (aggregated and non-aggregated)—for both SDOT and Acyclica?
- Provide accurate descriptions of Acyclica's data security practices, including encryption and hashing, consistent with the letter from Daniel Benhammou, including any additional practices that prevent reidentification.
- What third parties will access Acyclica's data, for what purpose, and under what conditions?
- Why are 89 locations not specified in the embedded Acyclica locations sheet in Section 2.1 of the SIR?
- Will SDOT continue to use Acyclica RoadTrend Sensors, and for how long? If SDOT plans to switch to other sensors, which ones, and how do their capabilities differ from the RoadTrend Sensors?
- Did SDOT consider any other alternatives when deciding to acquire Acyclica? Did SDOT consider other, more privacy protective traffic management tools in use (for example, inductive-loop detectors currently used by the Washington State Department of Transportation and the US

[14] https://www.flir.com/support/products/trafione#Resources

Department of Transportation)?[15]

- How does SDOT plan to reduce the privacy infringements on non-drivers/riders?

c. Recommendations for Regulation:

At this stage, pending answers to the questions set forth above, we can make only preliminary recommendations for regulation of Acyclica. We recommend that the Council adopt, via ordinance, clear and enforceable rules that ensure, at a minimum, the following:

- There must be a binding contract between SDOT and Acyclica.
- The contract between SDOT and Acyclica must include the following minimum provisions:
  - A data retention period of 12 hours or less for any data Acyclica collects, within which time Acyclica must aggregate the data, submit it to SDOT, and delete both non-aggregated and aggregated data.
  - SDOT receives only aggregated data.
  - SDOT owns all data, not Acyclica.
  - Acyclica cannot share the data collected with any other entity besides SDOT for any purpose.
- The ordinance must define a specific purpose of use for Acyclica technology, and all use of the tool and its data must be restricted to that purpose. For example: Acyclica may only be used for traffic management purposes, defined as activities concerning calculating average travel times, regulating traffic signals, controlling traffic disruptions, determining the placement of barricades or signals for the duration of road incidents impeding normal traffic flow, providing information to travelers about traffic flow and expected delays, and allowing SDOT to meet traffic records and reporting requirements.
- SDOT must produce an annual report detailing its use of Acyclica, including details how SDOT used the data collected, the amount of data collected, and for how long it was retained and in what form.

II. CopLogic – SPD

[15] https://www.fhwa.dot.gov/publications/research/operations/its/06108/03.cfm

Background

CopLogic (LexisNexis's Desk Officer Reporting System-DORS)[16] is a technology owned by LexisNexis and used by the Seattle Police Department to allow members of the public and retailers to submit online police reports regarding non-emergency crimes. Members of the public and retailers can submit these reports through an online portal they can access via their phone, tablet, or computer. Community members can report non-emergency crimes that have occurred within the Seattle city limits, and retail businesses that participate in SPD's Retail Theft Program may report low-level thefts that occur in their businesses when they have identified a suspect. This technology is used by SPD for the stated purpose of freeing up resources in the 9-1-1 Center, reducing the need for a police officer to be dispatched for the sole purpose of taking a police report.

This technology gives rise to potential civil liberties concerns because it allows for the collection of information about community members, unrelated to a specific incident, and without any systematic method to verify accuracy or correct inaccurate information. In addition, there is lack of clarity surrounding data retention and data sharing by LexisNexis, and around how CopLogic data will be integrated into SPD's Records Management System.

a. Concerns

- *Lack of Clarity on CopLogic/LexisNexis Data Collection and Retention.* There is no information in the SIR or in the contract between SPD and LexisNexis detailing the data retention period by LexisNexis (Section 5.2 of the SIR). This lack of clarity stems in part from an unclear description of what's provided by LexisNexis—it's described as an online portal, but the SIR and the contract provided appears to contemplate in Section 4.8 that LexisNexis will indeed access and store collected data. If true, the nature of that access should be clarified, and data restrictions including clear access limitations and retention periods should accordingly be put in place. Once reports are transferred over to SPD's Records Management System (RMS), the reports should be deleted by CopLogic/LexisNexis.

- *Lack of Clarity on LexisNexis Data Sharing with Other Agencies or Third Parties.* If LexisNexis does access and store data, it should do so only for purposes of fulfilling the contract, and should not share that data with third parties. But the contract between SPD and LexisNexis does not make clear whether LexisNexis is prohibited entirely from sharing data with other entities (it does contain a restriction on "transmit[ting]" the data, but without reference to third parties.

[16] https://risk.lexisnexis.com/products/desk-officer-reporting-system

- *No Way to Correct Inaccurate Information Collected About Community Members.* Community members or retailers may enter personally-identifying information about third parties without providing notice to those individuals, and there is no immediate, systematic method to verify the accuracy of information that individuals provide about third parties. There are also no stated measures in the SIR to destroy improperly collected data.

- *Lack of clarity on how the CopLogic data will be integrated with and analyzed within SPD's RMS.* At the technology fair, SPD stated that completed complaints will go into Mark43[17] when it is implemented. ACLU-WA has previously raised concerns about the Mark43 system, and it should be made clear how CopLogic data will enter that system, including to what third parties it will be made available.[18]

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What data does LexisNexis collect and store via CopLogic? What are LexisNexis's data retention policies for CopLogic data?

- Are there specific policies restricting LexisNexis from sharing CopLogic data with third parties? If so, what are they?

- Is there any way to verify or correct inaccurate information collected about community members?

- How will CopLogic data be integrated with Mark43?

c. Recommendations for Regulation:

Pending answers to the questions set forth above, we can make only preliminary recommendations for regulation of CopLogic. SPD should adopt clear and enforceable policies that ensure, at a minimum, the following:

- After CopLogic data is transferred to SPD's RMS, LexisNexis must delete all CopLogic data.

- LexisNexis is prohibited from using CopLogic data for any purpose other than those set forth in the contract, and from sharing CopLogic data with third parties.

[17] https://www.aclu-wa.org/docs/aclu-letter-king-county-council-regarding-mark-43
[18] A Records Management System (RMS) is the management of records for an organization throughout the records-life cycle. New RMSs (e.g., Mark43) may have capabilities that allow for law enforcement agencies to track and analyze the behavior of specific groups of people, leading to concerns of bias in big data policing, particularly for communities of color.

- Methods are available to the public to correct inaccurate information entered in the CopLogic portal.
- Measures are implemented to delete improperly collected data.

III. Computer-Aided Dispatch & 911 Logging Recorder Group

Overall, concerns around the Computer-Aided Dispatch (CAD) and 911 Logging Recorder technologies focus on use of the technologies and/or collected data them for purposes other than those intended, over-retention of data, and sharing of that data with third parties (such as federal law enforcement agencies). Therefore, for all of these technologies as appropriate, we recommend that the responsible agency should adopt clear and enforceable rules that ensure, at a minimum, the following:

- The purpose of use must be clearly defined, and its operation and data collected must be explicitly restricted to that purpose only.
- Data retention must be limited to the time needed to effectuate the purpose defined.
- Data sharing with third parties, if any, must be limited to those held to the same restrictions.
- Clear policies must govern operation, and all operators should be trained in those policies.

Specific comments follow:

1. Computer-Aided Dispatch – SPD

Background

CAD is a software package (made by Versaterm) utilized by the Seattle Police Department's 9-1-1 Center that consists of a set of servers and software deployed on dedicated terminals in the 9-1-1 center, in SPD computers, and as an application on patrol vehicles' mobile data computers and on some officers' smart phones. The stated purpose of CAD is to assist 9-1-1 Center call takers and dispatchers with receiving requests for police services, collecting information from callers, and providing dispatchers with real-time patrol unit availability. Concerns include lack of clarity surrounding data retention and data sharing with third parties.

a. Concerns:

- *Lack of clarity on data retention within CAD v. RMS.* While the SIR makes clear that at some point, CAD data is transferred to SPD's RMS, it is unclear what data, if any, the CAD system itself retains and for how long. If the CAD system does retain some data (for example, call logs)

independent of the RMS, and that data is accessible to the vendor, appropriate data protections should be put in place. But because the SIR usually references "data collected by CAD," it is unclear where that data resides.

- *Lack of a policy defining purpose of the technology and limiting its use to that purpose*: Unlike SFD's similar system, SPD appears to have no specific policy defining the purpose of use for CAD and limiting its use to that purpose.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- Does the CAD system itself store data? If so, what data and for how long? Who can access that data?

c. Recommendations for Regulation:

Depending on the answer to the question above, appropriate data protections may be needed as described above. In addition, SPD should adopt a policy similar to SFD's, clearly defining purpose and limiting use of the tool to that purpose.

2. Computer-Aided Dispatch – SFD

Background

Computer Aided Dispatch (CAD) is a suite of software packages used by SFD and made by Tritech that provide unit recommendations for 911 emergency calls based on the reported problem and location of a caller. The stated purpose of CAD is to allow SFD to manage emergency and non-emergency call taking and dispatching operations. The technology allows SFD to quickly enable personnel to execute rapid aid deployment.

Generally and positively, SFD clearly defines the purpose of use, restricts CAD operation and data collection to that purpose only, limits sharing with third parties, and specifies policies on operation and training. However, SFD must clarify what data is retained within CAD, data retention policies, and provide information about its data sharing partners.

d. Concerns

- *Lack of clarity on data retention within CAD*. It is unclear what data, if any, the CAD system itself retains and for how long. If the CAD system does retain some data (for example, call logs) and that data is accessible to the vendor, appropriate data protections should be put in place.
- *Lack of clarity on data retention policies*. At the technology fair, we learned that CAD data is retained indefinitely. It is not clear what justifies indefinite retention of this data.

- *Lack of clarity on data sharing partners.* In Section 6.3 of the SIR, SFD states that in rare case where CAD data is shared with partners other than those specifically named in the SIR, a third-party nondisclosure agreement is signed. However, there are no examples or details of who those partners are and the purposes for which CAD data would be shared.

e. Outstanding Questions That Must be Addressed in the Final SIR:

- Does the CAD system itself store data? If so, what data and for how long? Who can access that data?
- Who are SFD's data sharing partners? For what purpose is data shared with them?

f. Recommendations for Regulation:

Depending on the answer to the question regarding if the CAD system itself stores data, appropriate data protections may be needed as described above. SFD should adopt a clear policy requiring deletion of CAD data no longer needed. In addition, depending on how data is shared, SFD should adopt a policy that clearly limits what for what purposes CAD data would be shared, and with what entities.

3. 911 Logging Recorder – SPD

Background

The NICE 911 logging recorder is a technology used by SPD to audio-record all telephone calls to SPD's 9-1-1 communications center and all radio traffic between dispatchers and patrol officers. The stated purpose of the 9-1-1 Logging Recorder is to allow SPD to provide evidence to officers and detectives who investigate crimes and the prosecutors who prosecute offenders. These recordings also provide transparency and accountability for SPD, as they record in real time the interactions between 9-1-1 call takers and callers, and the radio traffic between 9-1-1 dispatchers and police officers. The NICE system also supports the 9-1-1 center's mission of quickly determining the nature of the call and getting the caller the assistance they need as quickly as possible with high quality, consistent and professional services.

Concerns include lack of clarity surrounding data retention schedules and data sharing with third parties.

a. Concerns

- *Lack of clarity on data retention.* Section 4.2 of the SIR states: "Recordings

requested for law enforcement and public disclosure are downloaded and maintained for the retention period related to the incident type." Similar to other technologies noted above, it is unclear whether the 9-1-1 system itself stores these recordings, or if they are stored on SPD's RMS. If the former, it should be made clear how the technology vendor accesses these recordings and for what purpose, if at all.

- *More clarity needed on data sharing with third parties.* There are no details or examples of the "discrete pieces of data" that are shared outside entities and individuals as referenced in Section 6.0 of the SIR.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What is SPD's data retention schedule for data stored in the NICE system, if any?
- What "discrete pieces of data" does SPD share with third parties?

c. Recommendations for Regulation:

SPD should adopt a clear policy requiring deletion of data no longer needed. In addition, depending on how data is shared, SPD should adopt a policy that clearly limits what for what purposes data would be shared, and with what entities.

IV. Current Diversion Technology Group – Seattle City Light

The technologies in this group—the Check Meter device (SensorLink TMS), the SensorLink Amp Fork, and the Binoculars/Spotting Scope raise civil liberties concerns primarily due to lack of explicit, written policies imposing meaningful restrictions on use of the technologies. While the purpose of the current diversion technologies appears clear—to assess whether suspected diversions of current have occurred and/or are continuing to occur—there are no explicit policies in the SIR detailing restrictions on what can and cannot be recorded by these technologies.

Below are short descriptions of the technologies, followed by concerns and recommendations.

Background

1. Check Meter Device (SensorLink TMS)

The SensorLink TMS device measures the amount of City Light-provided electrical energy flowing through the service-drop wire over time, digitally capturing the instantaneous information on the device for later retrieval by the Current Diversion Team via the use of a secure wireless protocol.

The stated purpose of use is to allow Seattle City Light to maintain the integrity of its electricity distribution system, to determine whether suspected current diversions have taken place, and to provide the valuation of the diverted energy to proper authorities for cost recovery.

2. SensorLink Amp Fork

The SensorLink Amp Fork is an electrical device mounted on an extensible pole allowing a circular clamp to be placed around the service-drop wire that provides electrical service to a customer location via its City Light-provided meter. The device then displays instantaneous readings of the amount of electrical energy (measured in amperage, or "amps") that the Current Diversion Team may compare against the readings displayed on the meter, allowing them to determine if current is presently being diverted.

The stated purpose of use of the Amp Fork is to allow Seattle City Light to assess whether suspected diversions of current have occurred and/or are continuing to occur. The Amp Fork allows the Utility to determine the valuation of the energy illegally diverted, which supports City Light's mission of recovering this value for ratepayers via a process called "back-billing."

3. Binoculars/Spotting Scope

The binoculars are standard, commercial-grade, unpowered binoculars. They do not contain any special enhancements requiring power (e.g., night-vision or video-recording capabilities). They are used to read a meter from a distance when the Current Diversion Team is otherwise unable to access physically the meter for the purpose of inspection upon suspected current diversion.

The stated purpose of the binoculars is to allow Seattle City Light to inspect meters and other implicated electrical infrastructure at a distance. If a determination of diversion is sustained, data may be used to respond to lawful requests from the proper law enforcement authorities for evidence for recovering the value of the diverted energy.

a. Concerns Regarding all Three Current Diversion Technologies

- *Absence of explicit, written policies imposing meaningful restrictions on use.* At the technology fair, a Seattle City Light representative stated that these technologies are used only for the purpose of checking current diversions, but could not confirm that Seattle City Light had clear, written policies for what data could and could not be recorded (e.g., an employee using the binoculars to view non-meter related information). The absence of written, specific policies increases the risk of unwarranted surveillance of individuals. There is also no mention in the SIRs of

specific data protection policies in place to safeguard the data (e.g., encryption, hashing, etc.).

- *Seattle City Light's records retention schedule is mentioned in the SIRs, but details about it are omitted.* It is unclear how long Seattle City Light retains data collected, and for what reason.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What enforceable policies, if any, apply to use of these three technologies?
- What is Seattle City Light's data retention schedule?

c. Recommendations for Regulation:

Seattle City Light must create clear, enforceable policies that, at a minimum:

- Define purpose of use for each technology and restrict its use to that purpose.
- Clearly state what clear data protection policies exist to safeguard stored data, if any, and ensure the deletion of data collected by the technology immediately after the relevant current diversion investigation has closed.

Thank you for your consideration, and please don't hesitate to contact me with questions.

Best,

Shankar Narayan
Technology and Liberty Project Director

Jennifer Lee
Technology and Liberty Project Advocate

15

Appendix 1: Benhammou Letter

16

City of Seattle

Acyclica

February 6th, 2015

RE: Acyclica data privacy standards

To whom it may concern:

The purpose of this letter is to provide information regarding the data privacy standards maintained by Acyclica. Acyclica is a traffic information company specializing in traffic congestion information management and analysis. Among the various types of data sources which make of Acyclica's traffic data portfolio including GPS probe data, video detection and inductive loops, Acyclica also utilizes our own patent-pending technology for the collection of Bluetooth and Wifi MAC addresses. MAC or Media Access Control addresses are unique 48-bit numbers which are associated with devices with Bluetooth and/or Wifi capable devices.

While MAC addresses themselves are inherently anonymous, Acyclica goes to great lengths to further obfuscate the original source of data through a combination of hashing and encryption to all but guarantee that information derived from the initial data bears no trace of any individual.

Acyclica's technology for collecting MAC addresses for congestion measurement operates by detecting nearby MAC addresses. The MAC addresses are then encrypted using GPG encryption before being transmitted to the cloud for processing. Encrypting the data prior to transmission means that no MAC addresses are ever written where they can be retrieved from the hardware. Once the data is received by our servers, the data is further anonymized using a SHA-256 algorithm which makes the raw MAC address nearly impossible to decipher from the hashed output. Furthermore, any customer seeking to download data for further investigation or integration through our API can only ever view the hashed MAC address.

Acyclica occasionally provides data to partners to help enhance the quality of congestion information. The information which is provided to such partners is received through API calls which only return aggregated information about traffic data over a given period such as the average travel-time over a 5-minute period. Aggregating the data provides a final layer of anonymization by reporting on the collective trend of all vehicles rather than the specific behavior of a single vehicle.

As always questions, comments and concerns are welcome. Please do let me know if we can provide further clarity and transparency on our internal operations with regards to data processing and privacy standards. We take the privacy of the public very seriously and always treat our customers and the data with the utmost respect.

Regards,

Daniel Benhammou
President
Acyclica Inc.

Appendix H: Comment Analysis Methodology

Overview

The approach to comment analysis includes combination of qualitative and quantitative methods. A basic qualitative text analysis of the comments received, and a subsequent comparative analysis of results, were validated against quantitative results. Each comment was analyzed in the following ways, to observe trends and confirm conclusions:

1. Analyzed collectively, as a whole, with all other comments received
2. Analyzed by technology
3. Analyzed by technology and question

A summary of findings are included in Appendix B: Public Comment Demographics and Analysis. All comments received are included in Appendix E: All Individual Comments Received.

Background on Methodological Framework

A modified Framework Methodology was used for qualitative analysis of the comments received, which "…*approaches [that] identify commonalities and differences in qualitative data, before focusing on relationships between different parts of the data, thereby seeking to draw descriptive and/or explanatory conclusions clustered around themes" (Gale, N.K., et.al, 2013).* Framework Methodology is a coding process which includes both inductive and deductive approaches to qualitative analysis.

The goal is to classify the subject data so that it can be meaningfully compared with other elements of the data and help inform decision-making. Framework Methodology is "not designed to be representative of a wider population, but purposive to capture diversity around a phenomenon" (*Gale, N.K., et.al, 2013).*

Methodology

Step One: Prepare Data

1. Compile data received.
    a. Daily collection and maintenance of 2 primary datasets.
        i. Master dataset: a record of all raw comments received, questions generated at public meetings, and demographic information collected from all methods of submission.
        ii. Comment analysis dataset: the dataset used for comment analysis that contains coded data and the qualitative codebook. The codebook contains the qualitative codes used for analysis and their definitions.
2. Clean the compiled data.
    a. Ensure data is as consistent and complete as possible. Remove special characters for machine readability and analysis.

b. Comments submitted through SurveyMonkey for "General Surveillance" remained in the "General Surveillance" category for the analysis, regardless of content of the comment. Comments on surveillance generally, generated at public meetings, were categorized as such.
c. Filter data by technology for inclusion in individual SIRs.

Step Two: Conduct Qualitative Analysis Using Framework Methodology

1. Become familiar with the structure and content of the data. This occurred daily compilation and cleaning of the data in step one.
2. Individually and collaboratively code the comments received, and identify emergent themes.
   I. Begin with deductive coding by developing pre-defined codes derived from the prescribed survey and small group facilitator questions and responses.
   II. Use clean data, as outlined in Data Cleaning section above, to inductively code comments.
      A. Each coder individually reviews the comments and independently codes them.
      B. Coders compare and discuss codes, subcodes, and broad themes that emerge.
      C. Qualitative codes are added as a new field (or series of fields) into the Comments dataset to derive greater insight into themes, and provide increased opportunity for visualizing findings.
   III. Develop the analytical framework.
      A. Coders discuss codes, sub-codes, and broad themes that emerge, until codes are agreed upon by all parties.
      B. Codes are grouped into larger categories or themes.
      C. The codes are be documented and defined in the codebook.
   IV. Apply the framework to code the remainder of the comments received.
   V. Interpret the data by identifying differences and map relationships between codes and themes, using R and Tableau.

Step Three: Conduct Quantitative Analysis

1. Identify frequency of qualitative codes for each technology overall, by questions, or by themes:
   I. Analyze results for single word codes.
   II. Analyze results for word pair codes (for context).
2. Identify the most commonly used words and word pairs (most common and least common) for all comments received.

I. Compare results with qualitative code frequencies and use to validate codes.
II. Create network graph to identify relationships and frequencies between words used in comments submitted. Use this graph to validate analysis and themes.

3. Extract CSVs of single word codes, word pair codes, and word pairs in text of the comments, as well as the corresponding frequencies for generating visualizations in Tableau.

Step Four: Summarization

1. Visualize themes and codes in Tableau. Use call out quotes to provide context and tone.
2. Included summary information and analysis in the appendices of each SIR.

Appendix I: Supporting Policy Documentation

Appendix J: CTO Notification of Surveillance Technology

Thank you for your department's efforts to comply with the new Surveillance Ordinance, including a review of your existing technologies to determine which may be subject to the Ordinance. I recognize this was a significant investment of time by your staff; their efforts are helping to build Council and public trust in how the City collects and uses data.

As required by the Ordinance (SMC 14.18.020.D), this is formal notice that the technologies listed below will require review and approval by City Council to remain in use. This list was determined through a process outlined in the Ordinance and was submitted at the end of last year for review to the Mayor's Office and City Council.

The first technology on the list below must be submitted for review by March 31, 2018, with one additional technology submitted for review at the end of each month after that. The City's Privacy Team has been tasked with assisting you and your staff with the completion of this process and has already begun working with your designated department team members to provide direction about the Surveillance Impact Report completion process.

Please let me know if you have any questions.

Thank you,
Michael Mattmiller

Technology	Description	Proposed Review Order
Binoculars/Spotting Scope	The spotting scope is used to read meters from a distance when direct access to the meter is obstructed. Scopes are used by SCL's Current Diversion team to conduct investigations. Use of this technology may occur without informing a domicile's resident(s).	1
SensorLink Amp Fork	The SensorLink Amp Fork is used by SCL's Current Diversion team to measure the load on line-side entrance conductors, allowing SCL to determine the total amount of power being consumed at a service location. This tool provides an instantaneous reading to the group conducting the investigation. Use of this technology may occur without informing a domicile's resident(s).	2
Check Meter Device	This device measures the total amount of power being consumed at a service location where current diversion is confirmed or suspected. The device is set at the transformer and is used when a prolonged reading is desired by the Current Diversion team. Use of this technology may occur without informing a domicile's resident(s).	3

City of Seattle

2019 Surveillance Impact Report

Current Diversion Team: Check Meter Device

Seattle City Light

Table of Contents

Submitting Department Memo 3
Surveillance Impact Report ("SIR") overview 7
Privacy Impact Assessment 8
Financial Information 20
Expertise and References 21
Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet 23
Privacy and Civil Liberties Assessment 37
CTO Response 43
Appendix A: Glossary 50
Appendix B: Meeting Notice(s) 52
Appendix C: Meeting Sign-in Sheet(s) 60
Appendix D: Department of Neighborhood Focus Group Notes 85
Appendix E: All Comments Received from Members of the Public 117
Appendix F: Department Responses to Public Inquiries 125
Appendix G: Letters from Organizations or Commissions 127
Appendix H: Comment Analysis Methodology 151
Appendix I: Supporting Policy Documentation 154
Appendix J: CTO Notification of Surveillance Technology 155

City of Seattle

Submitting Department Memo

Seattle City Light

MEMO

APRIL 16, 2019

TO
Seattle City Council

FROM
Julie Moore, Public Information Officer

SUBJECT
Summary of Surveillance Impact Reports for Three Current Diversion Detection Technologies

---

Seattle City Light's three current diversion detection technologies are undergoing review pursuant to Seattle Municipal Code, Chapter 14.18, *Acquisition and Use of Surveillance Technologies*.

The utility's Current Diversion Team (CDT) is responsible for investigating when electricity is being used but unaccounted for by City Light's billing system, and hence, not paid for. The three technologies City Light's CDT employs are:

1. Standard, commercial-grade, unpowered binoculars.
2. The SensorLink Ampstik.
3. The SensorLink Transformer Meter System.

Formal policies and procedures governing current diversion activity are described in City Light's Department Policy and Procedure (DPP) P III-416, *Current Diversion*. The CDT manager is responsible for ensuring City Light staff comply with the DPP and all existing rules.

TECHNOLOGIES

The utility's CDT members are the only staff who use the three technologies to investigate current diversion, and always upon preexisting and/or reported suspicion and with the approval of the current diversion coordinator. Suspicion of current diversion can take a variety of forms, such as a neighbor's report of questionable circumstances, a meter reader's observation of a tampered meter, or a billing specialist's observation of unusual or zero consumption.

CDT members who investigate potential current diversions drive standard City Light-marked vehicles and can be identified by their City Light ID badge and a hard hat.

1) BINOCULARS

When distance is a barrier to close physical inspection, CDT members may use binoculars to examine meters in assessing if current diversion is taking place. Binoculars may also be used to determine if potentially dangerous alterations to City Light's electrical infrastructure exist. The binoculars do not collect data, and do not contain any special enhancements requiring power (e.g., night vision, video-recording capabilities). Data derived from observations via CDT binoculars are accessible only by CDT members.

When used, CDT members use the binoculars for approximately one minute at a time. CDT members view locations that are in public view and the binoculars do not digitally record anything. Furthermore, the CDT only investigates specific meters and other implicated electrical equipment where current diversion is suspected. Therefore, the risk of staff inadvertently capturing data related to other customers is extremely low.

Data obtained by means of binoculars—which consist of notes made by staff based on their binocular-facilitated observations—are stored in a secure folder on City Light's digital network drive. The data, as well as overall incident reports, are accessible only by CDT members and the current diversion coordinator. Data will be retained per City Light records retention schedules. The current diversion coordinator has responsibility for ensuring compliance with data retention requirements.

The limited number of binoculars and of CDT members makes the routine tracking of this equipment relatively straight forward. Binoculars are issued to CDT members and are stored in their official vehicles. These vehicles are operated, locked, and stored in accordance with utility security procedures.

2) SENSORLINK AMPSTIK

The SensorLink Ampstik ("Ampstik") is a hand-held tool used to detect instantaneous current flow through a service drop. Specifically, it is an electrical device mounted on an extensible pole (up to 40' to 50') that allows a circular clamp to be placed around a service-drop wire. The wire is the same wire that provides electrical service to a customer location via a City Light-provided meter. The device then displays instantaneous readings of the amount of electrical energy flow as measured in amperage or "amps." The CDT member may then compare those reads against the readings displayed on the electric meter, allowing staff to determine if current is presently being diverted. Because the device delivers a point-in-time reading, it is deployed by hand for approximately 10 minutes at a time. The Ampstik ultimately allows the utility to determine the valuation of the energy illegally diverted, which supports City Light's mission of recovering this value for the ratepayers via a process called "back-billing."

Risk of inadvertent or improper collection is low for two reasons. First, the CDT only investigates specific, metered locations previously identified as sites of suspected current diversion. Second, Ampstik devices are used only on those service-drop lines that are delivering electrical service to the suspected location.

The limited number of this equipment and of CDT members makes the routine tracking of the Ampstik devices relatively straight forward. Ampstiks are issued to CDT members and are stored in their official vehicles. These vehicles are operated, locked, and stored in accordance with

utility security procedures. City Light records Ampstik serial numbers and their assignments to CDT members, along with their deployment status.

CDT members who are journey-level electrical workers trained to use Ampstiks may collect and access this data. This data may be accessed only by CDT staff and the current diversion coordinator, and are stored in a secure folder on City Light's digital network drive. Data will be retained per City Light records retention schedules. The current diversion coordinator has responsibility for ensuring compliance with data retention requirements.

3) SENSORLINK TRANSFORMER METER SYSTEM (TMS)

The SensorLink Transformer Meter System ("TMS") is a device that measures the amount of electrical energy flowing through a service-drop wire over time. It digitally captures the instantaneous information for later retrieval by the CDT member(s) via a secure wireless protocol. TMS devices are housed in a black, weatherproof box of approximately four square inches, and have an external City Light inventory control number so that line workers know what function the device serves. These devices are typically installed on an electric pole adjacent to a transformer for a period of one week to one month depending on the specific case needs and crew availability. These units ultimately allow the utility to determine the valuation of the energy illegally diverted, which supports City Light's mission of recovering this value for the ratepayers via a process called "back-billing."

The CDT owns six TMS units, which are deployed on the basis of case number and need. Deployment level on a given case can vary from none (zero) to all (six). Once a case is properly opened, CDT members may check the devices out without prior additional authorization, although in nearly all circumstances, the current diversion coordinator is aware of deployment due to position responsibilities. City Light records TMS serial numbers and their assignments to CDT members, along with their deployment status.

Risk of inadvertent or improper collection is low for two reasons. First, the CDT member only investigates specific, metered locations previously identified and properly documented as a site of suspected current diversion. Second, TMS devices are used only on those service-drop lines that are delivering electrical service to a suspected location.

The SensorLink TMS device is not "visible to the public" in any conventional sense, although to a trained eye, it may be visible near a transformer on an electrical pole. CDT members, who are journey-level electrical workers trained in the placement, use, and removal of the device, may collect the data. The quantitative data – accumulated consumption (in kilowatt hours), average volts (current strength), average amps (current flow), and interval consumption (in kilowatt hours per a pre-defined time unit) – are accessed by CDT members remotely using a secure radio protocol and a specific, password-protected software program.

Data obtained by means of the TMS are stored in a secure folder on City Light's digital network drive, accessible only by CDT members and City Light management. Data stored in the TMS are deleted after its retrieval by the CDT staff and/or upon its removal from the electrical pole. In other words, no data remains in the TMS once its use for a specific current diversion case has been completed. Data will be retained per City Light record retention schedules. The current

diversion coordinator has responsibility for ensuring compliance with data retention requirements.

DATA SHARING & AUDITING

Data collected from the use of the three technologies may be shared with other government staff in two instances. When a determination is made that current diversion has taken place, a valuation of the stolen energy is shared with City Light's billing division so that the utility can "back-bill" and recover the diverted energy costs from the appropriate customer. Also, data is shared with police investigators and/or prosecutors for the purposes of law enforcement or legal action in complex or aggravated cases (e.g., when large sums of energy have been diverted/stolen, or where there is a safety risk to the public). This policy is formally laid out in City Light's DPP 500 P III-416. In both instances, data sharing is required for City Light to recover stolen energy costs. In the latter case (i.e., information sharing with police investigators) data sharing may also be required in order to protect public safety, since unauthorized alterations to the electrical system can pose a serious, and at times, lethal danger to the public.

To safeguard CDT data, the current diversion coordinator will request Seattle IT to provide audit data, so that City Light may complete an audit to ensure that access rights are assigned only to authorized staff.

IMPORTANCE OF TECHNOLOGIES – SUPPORTING CITY LIGHT'S MISSION

One of City Light's core missions as an electric utility is to recoup the costs of the energy provided to customers. This is required by Seattle Municipal Code 21.49.100, *Application and Contract Provisions*. Additionally, as a general rule the Washington State Constitution's Article VIII, Section 7 prohibits the gifting of public funds. Since all three technologies enable City Light to recover unaccounted for electricity costs, they contribute to the department's mission of being legally compliant. Translated into monetary value, the utility recovered over $1.6 million in 2017 using these technologies. This would otherwise be a substantial financial loss for the City.

City of Seattle

Surveillance Impact Report ("SIR") overview

About the Surveillance Ordinance

The Seattle City Council passed Ordinance 125376, also referred to as the "Surveillance Ordinance," on September 1, 2017. SMC 14.18.020.b.1 charges the City's executive with developing a process to identify surveillance technologies subject to the ordinance. Seattle it, on behalf of the executive, developed and implemented a process through which a privacy and surveillance review is completed prior to the acquisition of new technologies. This requirement, and the criteria used in the review process, are documented in Seattle it policy pr-02, the "surveillance policy".

How this Document is Completed

This document is completed by the requesting department staff, support and coordinated by the Seattle information technology department ("Seattle it"). As Seattle it and department staff complete the document, they should keep the following in mind.

1. Responses to questions should be in the text or check boxes only; all other information (questions, descriptions, etc.) Should **not** be edited by the department staff completing this document.
2. All content in this report will be available externally to the public. With this in mind, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.

Surveillance Ordinance Review Process

The following is a high-level outline of the complete SIR review process.

Upcoming for Review	Initial Draft	Open Comment Period	Final Draft	Working Group	Council Review
The technology is upcoming for review, but the department has not begun drafting the surveillance impact report (SIR).	Work on the initial draft of the SIR is currently underway.	The initial draft of the SIR and supporting materials have been released for public review and comment. During this time, one or more public meetings will take place to solicit feedback.	During this stage the SIR, including collection of all public comments related to the specific technology, is being compiled and finalized.	The surveillance advisory working group will review each SIR's final draft and complete a civil liberties and privacy assessment, which will then be included with the SIR and submitted to Council.	City Council will decide on the use of the surveillance technology, by full Council vote.

Privacy Impact Assessment

Purpose

A Privacy Impact Assessment ("PIA") is a method for collecting and documenting detailed information collected in order to conduct an in-depth privacy review of a program or project. A PIA asks questions about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. It also requests information about policies, training and documentation that govern use of the technology. The PIA responses are used to determine privacy risks associated with a project and mitigations that may reduce some or all of those risks. In the interests of transparency about data collection and management, the City of Seattle has committed to publishing all PIAs on an outward facing website for public access.

When is a Privacy Impact Assessment Required?

A PIA may be required in two circumstances.

1. When a project, technology, or other review has been flagged as having a high privacy risk.
2. When a technology is required to complete the surveillance impact report process. This is one deliverable that comprises the report.

1.0 Abstract

1.1 Please provide a brief description (one paragraph) of the purpose and proposed use of the project/technology.

Seattle City Light's ("City Light") Current Diversion Team ("CDT") consists of a group of approximately five journey-level engineers who are dispatched to collect data to attempt to determine whether a suspected diversion of current (i.e., alterations to the City Light-owned electrical system by a third-party in order to consume electric power without it being registered by the City Light meter installed for that purpose) has taken place. In support of this mission, the CDT crew uses a Check Meter (subsequently referred to as SensorLink TMS throughout this SIR) device. Data from the device are retrieved via secure radio protocol. If a determination of diversion is sustained, data may be used to respond to lawful requests from the proper law enforcement authorities for evidence for recovering the value of the diverted energy.

In conjunction with this technology, two others – standard, commercial-grade, unpowered binoculars, and the SensorLink Ampstik device – are used by the CDT. As a result, City Light's three retroactive Surveillance Impact Reports ("SIRs") may be, at times, duplicative, so that each report contains the necessary information.

1.2 Explain the reason the project/technology is being created or updated and why the PIA is required.

This technology is used in furtherance of a mission supported by ordinance (SMC 21.49.100, requiring recovery of payment for electric services provided) and an existing City Light department policy procedure (DPP 500 P III-416, hereafter "DPP"). City Light provided the information in the Privacy Impact Assessment to fulfill the requirements of the Surveillance Ordinance and so that the public may understand the nature of the CDT and the tools that are essential to its carrying out its mission for the benefit of ratepayers. The SensorLink TMS device provides data to the CDT member by recording data over time for the CDT to retrieve at a later date via a secure wireless protocol.

2.0 Project / Technology Overview

Provide an overview of the project or technology. The overview gives the context and background necessary to understand the purpose, mission and justification for the project / technology proposed

2.1 Describe the benefits of the project/technology.

As described in Section 1, the CDT utilizes the SensorLink TMS device in order to assess whether suspected diversions of current have occurred and/or are continuing to occur. The SensorLink TMS device allows the Utility to determine the valuation of the energy illegally diverted, which supports City Light's mission of recovering this value for the ratepayers via a process called "back-billing."

2.2 Provide any data or research demonstrating anticipated benefits.

In 2017, the CDT's operations, via the use of the SensorLink TMS device (in combination with the other two technologies under review), City Light recovered $1.6 million. This would otherwise remain a substantial financial loss to the Utility. City Light implemented the SensorLink TMS technology as an efficient and accurate means of assessing amounts of current being diverted after CDT staff studied their use by Portland General Electric, the electric energy provider for the Portland, Oregon area.

2.3 Describe the technology involved.

The SensorLink TMS device measures the amount of City Light-provided electrical energy flowing through the service-drop wire over time, digitally capturing the instantaneous information on the device for later retrieval by the CDT via the use of a secure wireless protocol. The SensorLink TMS device is housed in a black, weatherproofed box of approximately four square inches, with a City Light inventory control number on the outside for identification by City Light line crews. These are typically deployed on the electric pole, adjacent to the transformer, from one week to one month, depending on the specific case need and crew availability.

2.4 Describe how the project or use of technology relates to the department's mission.

The SensorLink TMS device allows City Light to maintain the integrity of its electricity distribution system, to determine whether suspected current diversions have taken place, and to provide the valuation of the diverted energy to proper authorities for cost recovery. These are supported by ordinance (SMC 21.49.100) and Department Policy and Procedure (DPP).

2.5 Who will be involved with the deployment and use of the project / technology?

The CDT members are the only City Light staff who deploy the SensorLink TMS device, and always upon pre-existing and/or reported suspicion of current diversion (e.g., neighbor report, unusual or no energy consumption detected upon a routine meter reading by City Light, visual observation of tampered-with meter or other City Light-owned or -maintained electrical equipment

3.0 Use Governance

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities contracting with the City are bound by restrictions specified in the surveillance ordinance and privacy principles and must provide written procedures for how the entity will comply with any restrictions identified.

3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

The CDT owns six SensorLink TMS units, which are deployed on the basis of case number and need. Deployment level on a given case can vary from none (zero) to all (six). Once a case is properly opened, CDT crew members may check them out without prior additional authorization, though the Current Diversion Coordinator is under nearly all circumstances aware of deployment due to position responsibilities. Serial numbers are recorded and the CDT member to whom they are assigned, as well as their deployment status, are logged.

3.2 List the legal standards or conditions, if any, that must be met before the project / technology is used.

Routine deployment in support of making an internal determination as to current diversion is not subject to additional prior legal authorization.

3.3 Describe the policies and training required of all personnel operating the project / technology, and who has access to ensure compliance with use and management policies.

In addition to routine privacy and security training undergone by all City Light employees per Seattle IT policy, the Current Diversion Coordinator has responsibility for ensuring compliance with all existing rules and procedures.

4.0 Data Collection and Use

4.1 Provide details about what information is being collected from sources other than an individual, including other IT systems, systems of record, commercial data aggregators, publicly available data and/or other City departments.

No additional information is collected by the CDT in making its determinations, nor is any third-party or other aggregation taking place.

4.2 What measures are in place to minimize inadvertent or improper collection of data?

Risk of inadvertent or improper collection is low for two reasons. First, the CDT only investigates specific, metered locations previously identified and properly documented as sites of suspected current diversion. And second, SensorLink TMS devices are used only on those service-drop lines that are delivering electrical service to the suspected location.

4.3 How and when will the project / technology be deployed or used? By whom? Who will determine when the project / technology is deployed and used?

SensorLink TMS devices are used throughout the year based on suspected cases of current diversion, by the CDT staff and with the approval of the Current Diversion Coordinator. As mentioned above, these can be triggered in several ways, for example: neighbor report to the customer service bureau or other City Light representatives; recognition by billing specialists of highly out-of-the-ordinary meter readings; or observations by meter and other crews of tampering with metering or other electrical service provision equipment.

4.4 How often will the technology be in operation?

SensorLink TMS devices, once deployed pursuant to determinations mentioned in 4.3 and the approval of the Current Diversion Coordinator, are in operation for a period varying from approximately one week and one month at a time on a given case.

4.5 What is the permanence of the installation? Is it installed permanently, or temporarily?

SensorLink TMS devices are installed temporarily for periods normally varying from one week to one month. The amount of time depends on the specific measurement need of the case, as well as crew availability.

4.6 Is a physical object collecting data or images visible to the public? What are the markings to indicate that it is in use? What signage is used to determine department ownership and contact information?

The SensorLink TMS device is not "visible to the public" in any conventional sense, though to a trained eye, it may be visible near a transformer on an electrical pole (for images of the technology, see the attached Specification Sheet in the "Expertise and References" section 3.0). The device contains an City Light inventory tag so that line workers may know what function it serves when they are working in the electrical space of the pole. No notification is made to the public of its use, as this may risk defeating its purpose of detecting a diversion of current on a single, previously-suspected service-drop.

4.7 How will data that is collected be accessed and by whom?

CDT members, who are journey-level electrical workers trained in the placement, use, and removal of the SensorLink TMS device, may collect this data. The quantitative data – accumulated consumption (in kilowatt-hours), average volts (current strength), average amps (current flow), and interval consumption (in kilowatt-hours per a pre-defined time-unit) – are accessed by CDT crew members remotely using a secure radio protocol and a specific, password-protected software program, known as Steelhead.

4.8 If operated or used by another entity on behalf of the City, provide details about access, and applicable protocols.

City Light is the only entity operating or using the technology.

4.9 What are acceptable reasons for access to the equipment and/or data collected?

The SensorLink TMS device is used only to make determinations about whether a current diversion is likely to be taking place. As the device gathering and storing data for later retrieval over time, the SensorLink TMS may be accessed for said data retrieval, or for its installation or removal in connection with the given investigation.

4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

Data obtained by means of the SensorLink TMS device are stored in a private folder on City Light's digital file locations, accessible only by CDT members and management. Data stored in the SensorLink TMS device itself are deleted after its observations are retrieved by the CDT and/or upon its removal from the electrical pole (i.e., no data remain on the SensorLink TMS once its use for a given determination of current diversion has been completed and before it is therefore made available to other CDT staff for subsequent deployment).

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

Data obtained by means of the SensorLink TMS device are stored in a private folder on City Light's digital file locations, accessible only by CDT members and management. Data stored in the SensorLink TMS device itself during deployment are deleted after its observations are retrieved by the CDT and/or upon its removal from the electrical pole (i.e., no data remain on the SensorLink TMS once its use for a given determination of current diversion has been completed and, therefore, before it is made available for subsequent deployment).

5.2 How will the owner allow for departmental and other entities, to audit for compliance with legal deletion requirements?

City Light will make CDT file locations and staff available for properly authorized entities wishing to ensure compliance. Data will be retained per City Light record retention schedules.

5.3 What measures will be used to destroy improperly collected data?

To the extent permitted by the Washington State Public Disclosure Law, any improperly collected data will be deleted from City Light's digital file locations, and hard-copy documents will be destroyed.

5.4 which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

The Current Diversion Coordinator has responsibility for this function.

6.0 Data Sharing and Accuracy

6.1 Which entity or entities inside and external to the City will be data sharing partners?

Data, or information derived from the data, may be shared with other parties in two instances, both of which are public entities. These are (1) when a determination is made that current diversion has taken place, in which case a valuation of the stolen energy is sent to the customer billing division of City Light for "back-billing" to the customer for cost recovery, and (2) when police investigators and/or prosecutors require evidence for further proceedings in complex or aggravated cases, as when large sums of energy have been diverted/stolen, or where there is a safety risk to the public.

6.2 Why is data sharing necessary?

In both cases, this is required for City Light to recoup stolen energy costs. In the second case (information sharing with police investigators) it may also be required to protect public safety, since unauthorized alterations to the electrical system can pose a serious and at times lethal danger to the public.

6.3 Are there any restrictions on non-City data use?

Yes ☒ No ☐

6.3.1 If you answered yes, provide a copy of the department's procedures and policies for ensuring compliance with these restrictions.

Data are collected and maintained for City Light use and may only be shared with outside entities for the purposes of law enforcement or legal action by the relevant jurisdictional authority. This policy is formally laid out in Seattle City Light Department Policy & Procedure DPP 500 P III-416.

6.4 How does the project/technology review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?

City Light anticipates no additional data-sharing, as the CDT's mission is fixed. Additional changes would require review the Current Diversion Coordinator. Law enforcement, as mentioned in 6.3, may request these data and findings but only pursuant to a subpoena or a request pursuant to the Public Disclosure Law (based upon probable cause, see RCW 42.56.335).

6.5 Explain how the project/technology checks the accuracy of the information collected. If accuracy is not checked, please explain why.

As the data come from the SensorLink TMS device are designed to measure accurately in a scientific manner the amount of energy passing through them, these data are not checked further, beyond regular maintenance of the equipment to ensure proper functioning.

6.6 Describe any procedures that allow individuals to access their information and correct inaccurate or erroneous information.

Upon a proper finding of current diversion, customers are back-billed to recoup these losses. DPP 500 P III-416 provides that "all customers shall receive uniform consideration and courtesy in all matters involving actual or suspected current diversion." Customers are notified of findings and offered opportunities to respond and/or object.

7.0 Legal Obligations, Risks and Compliance

7.1 What specific legal authorities and/or agreements permit and define the collection of information by the project/technology?

One of City Light's core missions as an electric utility is to recoup the costs of the energy it provides to its customers as part of its operations, as required in SMC 21.49.100.

7.2 Describe what privacy training is provided to users either generally or specifically relevant to the project/technology.

CDT members are trained in how to store information in private folders on City Light's digital storage locations, in addition to the general privacy and security training required by Seattle IT.

7.3 Given the specific data elements collected, describe the privacy risks identified and for each risk, explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

The SensorLink TMS device only measures specific, individual service-drops directly linking the customer suspected of current diversion to City Light's electric services. As such, there is no additional privacy risk present.

7.4 Is there any aspect of the project/technology that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?

City Light has considered but does not anticipate such objections, since the data collected are used for one purpose only.

8.0 Monitoring and Enforcement

8.1 Describe how the project/technology maintains a record of any disclosures outside of the department.

When a report is sent to law enforcement, it does not include power consumption information. Law enforcement then relies upon the Public Disclosure Law to request power records, if they decide to do so, and City Light would provide that information pursuant to that request. This may be effectuated either by a subpoena or by a request from law enforcement based upon probable cause and pursuant to the Washington Public Disclosure Law (see RCW 42.56.335).

8.2 What auditing measures are in place to safeguard the information, and policies that pertain to them, as well as who has access to the audit data? Explain whether the project/technology conducts self-audits, third party audits or reviews.

To safeguard the information, the Current Diversion Coordinator will request Seattle IT to provide audit data, so that City Light may complete an audit to ensure that access rights are assigned only those who should have access to the shared drive containing customer/current-diversion data.

Financial Information

Purpose

This section provides a description of the fiscal impact of the surveillance technology, as required by the surveillance ordinance.

1.0 Fiscal Impact

Provide a description of the fiscal impact of the project/technology by answering the questions below.

1.1 Current or potential sources of funding: initial acquisition costs.

Current ☒ potential ☐

Date of initial acquisition	Date of go live	Direct initial acquisition cost	Professional services for acquisition	Other acquisition costs	Initial acquisition funding source
2014 & 2016	Same	$4,800	None	None	City Light

Notes:

City Light obtained the SensorLink TMS technology in 2014. A reorder was placed in 2016. City Light now owns six such devices.

1.2 Current or potential sources of funding: on-going operating costs, including maintenance, licensing, personnel, legal/compliance use auditing, data retention and security costs.

Current ☒ potential ☐

Annual maintenance and licensing	Legal/compliance, audit, data retention and other security costs	Department overhead	IT overhead	Annual funding source
None	See below	None	None	City Light

Notes:

Compliance and audit costs are internal, as detailed above, and are therefore part of Current Diversion Team's normal workflow and procedures. There are no costs directly related to the "use" or "maintenance" of the six SensorLink TMS devices.

1.3 Cost savings potential through use of the technology

In 2017, through the use of the Current Diversion Team's technologies – including the SensorLink TMS device – City Light was able to recover $1.6 million in stolen energy costs.

1.4 Current or potential sources of funding including subsidies or free products offered by vendors or governmental entities

None identified.

Expertise and References

Purpose

The following information is provided to ensure that Council has a group of experts to reference while reviewing the completed surveillance impact report ("SIR"). Any individuals or agencies referenced must be made aware ahead of publication that their information has been included. All materials must be available for Council to access or review, without requiring additional purchase or contract.

1.0 Other Government References

Please list any other government bodies that have implemented this technology and can speak to the implementation of this technology.

Agency, municipality, etc.	Primary contact	Description of current use
N/A	N/A	N/A

2.0 Academics, Consultants, and Other Experts

Please list any experts in the technology under consideration, or in the technical completion of the service or function the technology is responsible for.

Agency, municipality, etc.	Primary contact	Description of current use
N/A	N/A	N/A

3.0 White Papers or Other Documents

Please list any authoritive publication, report or guide that is relevant to the use of this technology or this type of technology.

Title	Publication	Link
SensorLink TMS Overhead Transformer Meter Technical Specification Sheet	TMS%20Datasheet %20V01.pdf	Weblink to PDF document

Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet

Purpose

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit ("RET") in order to:

- Provide a framework for the mindful completion of the SIR in a way that is sensitive to the historic exclusion of vulnerable and historically underrepresented communities. Particularly, to inform the public engagement efforts departments will complete as part of the surveillance impact report.
- Highlight and mitigate any impacts on racial equity from the adoption and the use of the technology.
- Highlight and mitigate any disparate impacts on individuals or vulnerable communities.
- Fulfill the public engagement requirements of the surveillance impact report.

Adaptation of the RET for Surveillance Impact Reports

The RET was adapted for the specific use by the Seattle Information Technology Departments' ("Seattle IT") Privacy Team, the Office of Civil Rights ("OCR"), and Change Team members from Seattle IT, Seattle City Light, Seattle Fire Department, Seattle Police Department, and Seattle Department of Transportation.

Racial Equity Toolkit Overview

The vision of the Seattle Race and Social Justice Initiative ("RSJI") is to eliminate racial inequity in the community. To do this requires ending individual racism, institutional racism and structural racism. The RET lays out a process and a set of questions to guide the development, implementation and evaluation of policies, initiatives, programs, and budget issues to address the impacts on racial equity.

1.0 Set Outcomes

1.1. Seattle City Council has defined the following inclusion criteria in the surveillance ordinance, and they serve as important touchstones for the risks departments are being asked to resolve and/or mitigate. Which of the following inclusion criteria apply to this technology?

☐ The technology disparately impacts disadvantaged groups.

☐ There is a high likelihood that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service.

☒ The technology collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection.

☐ The technology raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice.

1.2 What are the potential impacts on civil liberties through the implementation of this technology? How is the department mitigating these risks?

Because SensorLink TMS, in conjunction with the two other diversion technologies being reviewed, are designed to measure electric current at one connection point assigned to one customer, no impacts on civil liberties are anticipated from the technologies themselves. At the same time, City Light is aware that the methods and procedures surrounding the use or installation of an otherwise non-offensive technology is just as important. For that reason, we ensure that our staff are clearly identified as Seattle City Light employees when in the field; there is no surreptitious operation in the field.

1.3 What are the risks for racial or ethnicity-based bias through each use or deployment of this technology? How is the department mitigating these risks?

Include a description of any issues that may arise such as algorithmic bias or the possibility for ethnic bias to emerge in people and/or system decision-making.

City Light is committed to equitable enforcement of all its legal mandates, in the same way that it is committed to equity in its provision of clean, affordable, and reliable power for its customers. City Light aims to ensure that the enforcement mechanisms are similarly equitable, in that they should be not only unbiased but also equitably enforced. For that reason, City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible.

1.4 Where in the City is the technology used or deployed?

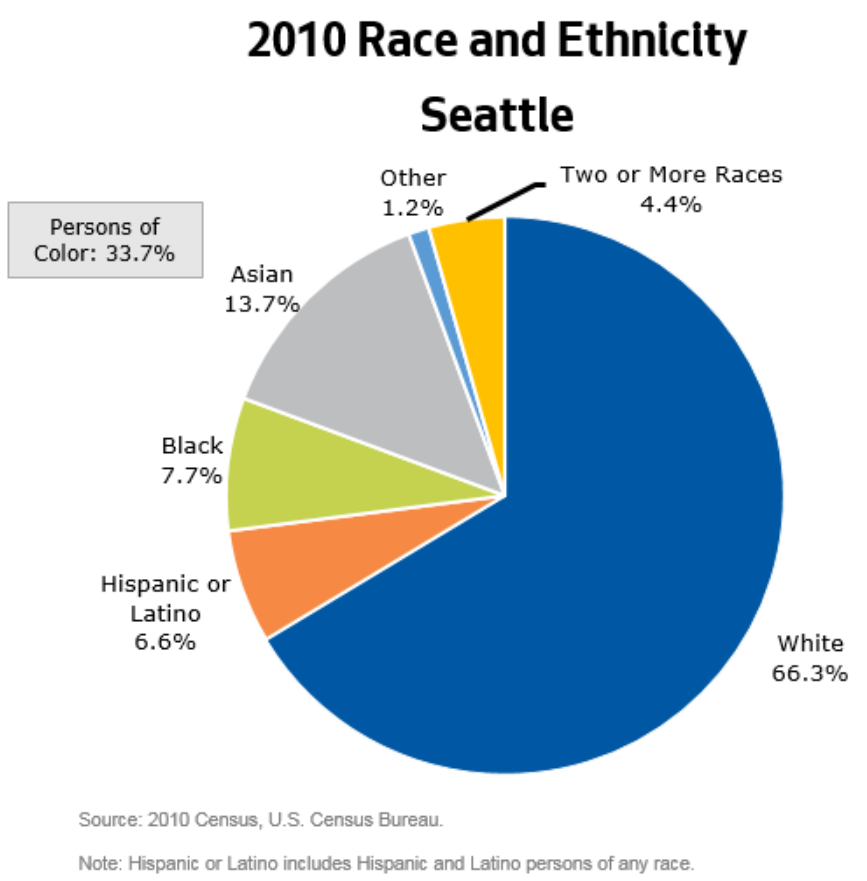
☒ all Seattle neighborhoods

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County.

If possible, please include any maps or visualizations of historical deployments / use.

Seattle City Light's service territory extends beyond the boundary of the City of Seattle. Other areas include: Burien, Lake Forest Park, Normandy Park, Renton, SeaTac, Shoreline, Tukwila, and areas of unincorporated King County.

1.4.1 What are the racial demographics of those living in this area or impacted by these issues?



1.4.2 How does the Department to ensure diverse neighborhoods, communities, or individuals are not specifically targeted through the use or deployment of this technology?

DPP 500 P III-416 provides that "all customers shall receive uniform consideration and courtesy in all matters involving actual or suspected current diversion." City Light aims to ensure that the enforcement mechanisms are equitable, in that they should be not only unbiased but also equitably enforced. For that reason, City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible.

1.5 How do decisions around data sharing have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

Data is collected for Seattle City Light use and may only be shared with outside entities for the purposes of law enforcement or legal action by the relevant jurisdictional authority. This policy is formally laid out in Seattle City Light Department Policy & Procedure DPP 500 P III-416. As stated previously, City Light aims to ensure that the enforcement mechanisms are equitable, in that they should be not only unbiased but also equitably enforced. For that reason, City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible.

1.6 How do decisions around data storage and retention have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

Data is maintained for Seattle City Light use and may only be shared with outside entities for the purposes of law enforcement or legal action by the relevant jurisdictional authority. This policy is formally laid out in Seattle City Light Department Policy & Procedure DPP 500 P III-416. As stated previously, City Light aims to ensure that the enforcement mechanisms are equitable, in that they should be not only unbiased but also equitably enforced. For that reason, City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible.

1.7 What are potential unintended consequences (both negative and positive potential impact)? What proactive steps can you can / have you taken to ensure these consequences do not occur.

One of City Light's core missions as an electric utility is to recoup the costs of the energy it provides to its customers as part of its operations (as required in SMC 21.49.100 and the general rule against gifts of public funds found in the Washington State Constitution at Article VIII, Section 7). Per DPP 500 P III-416,"all customers shall receive uniform consideration and courtesy in all matters involving actual or suspected current diversion." As stated previously, City Light aims to ensure that the enforcement mechanisms are equitable, in that they should be not only unbiased but also equitably enforced. For that reason, City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible.

2.0 Public Outreach

2.1 Organizations who received a personal invitation to participate.

Please include a list of all organizations specifically invited to provide feedback on this technology.

1. ACLU of Washington	2. Ethiopian Community Center	3. Planned Parenthood Votes Northwest and Hawaii
4. ACRS (Asian Counselling and Referral Service)	5. Faith Action Network	6. PROVAIL
7. API Chaya	8. Filipino Advisory Council (SPD)	9. Real Change
10. API Coalition of King County	11. Friends of Little Saigon	12. SCIPDA
13. API Coalition of Pierce County	14. Full Life Care	15. Seattle Japanese American Citizens League (JACL)
16. CAIR	17. Garinagu HounGua	18. Seattle Neighborhood Group
19. CARE	20. Helping Link	21. Senior Center of West Seattle
22. Central International District Business Improvement District	23. Horn of Africa	24. Seniors in Action
25. Church Council of Greater Seattle	26. International ImCDA	27. Somali Family Safety Task Force
28. City of Seattle Community Police Commission (CPC)	29. John T. Williams Organizing Committee	30. South East Effective Development
31. City of Seattle Community Technology Advisory Board	32. Kin On Community Health Care	33. South Park Information and Resource Center SPIARC
34. City of Seattle Human Rights Commission	35. Korean Advisory Council (SPD)	36. STEMPaths Innovation Network
37. Coalition for Refugees from Burma	38. Latina/o Bar Association of Washington	39. University of Washington Women's Center
40. Community Passageways	41. Latino Civic Alliance	42. United Indians of All Tribes Foundation
43. Council of American Islamic Relations - Washington	44. LELO (Legacy of Equality, Leadership, and Organizing)	45. Urban League
46. East African Advisory Council (SPD)	47. Literacy Source	48. Wallingford Boys & Girls Club
49. East African Community Services	50. Millionair Club Charity	51. Washington Association of Criminal Defense Lawyers
52. Education for All	53. Native American Advisory Council (SPD)	54. Washington Hall
55. El Centro de la Raza	56. Northwest Immigrant Rights Project	57. West African Community Council
58. Entre Hermanos	59. OneAmerica	60. YouthCare
61. US Transportation expertise	62. Local 27	63. Local 2898
64. (SPD) Demographic Advisory Council	65. South Seattle Crime Prevention Coalition (SSCPC)	66. CWAC
67. NAAC		

2.2 Additional Outreach Efforts

Department	Outreach Area	Description
ITD	Social Media Outreach Plan: Twitter	Directed Tweets and Posts related to Open Public Comment Period for Group 2 Technologies, as well as the BKL event.
SPD, SFD, OPCD, OCR, SPL, SDOT, SPR, SDCI, SCL, OLS, Seattle City Council	Social Media Outreach Plan: Twitter	Tweets and Retweets regarding Group 2 comment period and/or BKL event.
ITD	Press Release	Press release sent to several Seattle media outlets.
ITD	Ethnic Media Press Release	Press Release sent to specific ethnic media publications.
ITD	Social Media Outreach Plan: Facebook Event Post	Seattle IT paid for boosted Facebook posts for their BKL event.
ITD	CTAB	Presented and utilized the Community Technology Advisory Board (CTAB) network and listserv for engaging with interested members of the public
ITD	Blog	Wrote and published a Tech Talk blog post for Group 2 technologies, noting the open public comment period, BKL event, and links to the online survey/comment form.
ITD	Technology Videos	Seattle IT worked with the Seattle Channel to produce several short informational/high level introductory videos on group 2 technologies, which were posted on seattle.gov/privacy. And used at a number of Department of Neighborhoods-led focus groups.

2.3 Scheduled public meeting(s).

Meeting notes, sign-in sheets, all comments received, and questions from the public will be included in Appendix B, C, D, E, F, G, H and I. Comment analysis will be summarized in section 3.0 Public Comment Analysis.

Location	Bertha Knight Landes Room, 1st Floor City Hall 600 4th Avenue, Seattle, WA 98104
Time	February 27, 2018; 6 p.m. – 8 p.m.
Capacity	100+
Link to URL Invite	BKL Event Invitation

2.4 Scheduled focus Group Meeting(s)

Meeting 1

Community Engaged	Council on American-Islamic Relations - Washington (CAIR-WA)
Date	Thursday, February 21, 2019

Meeting 2

Community Engaged	Entre Hermanos
Date	Thursday, February 28, 2019

Meeting 3

Community Engaged	Byrd Barr Place
Date	Thursday, February 28, 2019

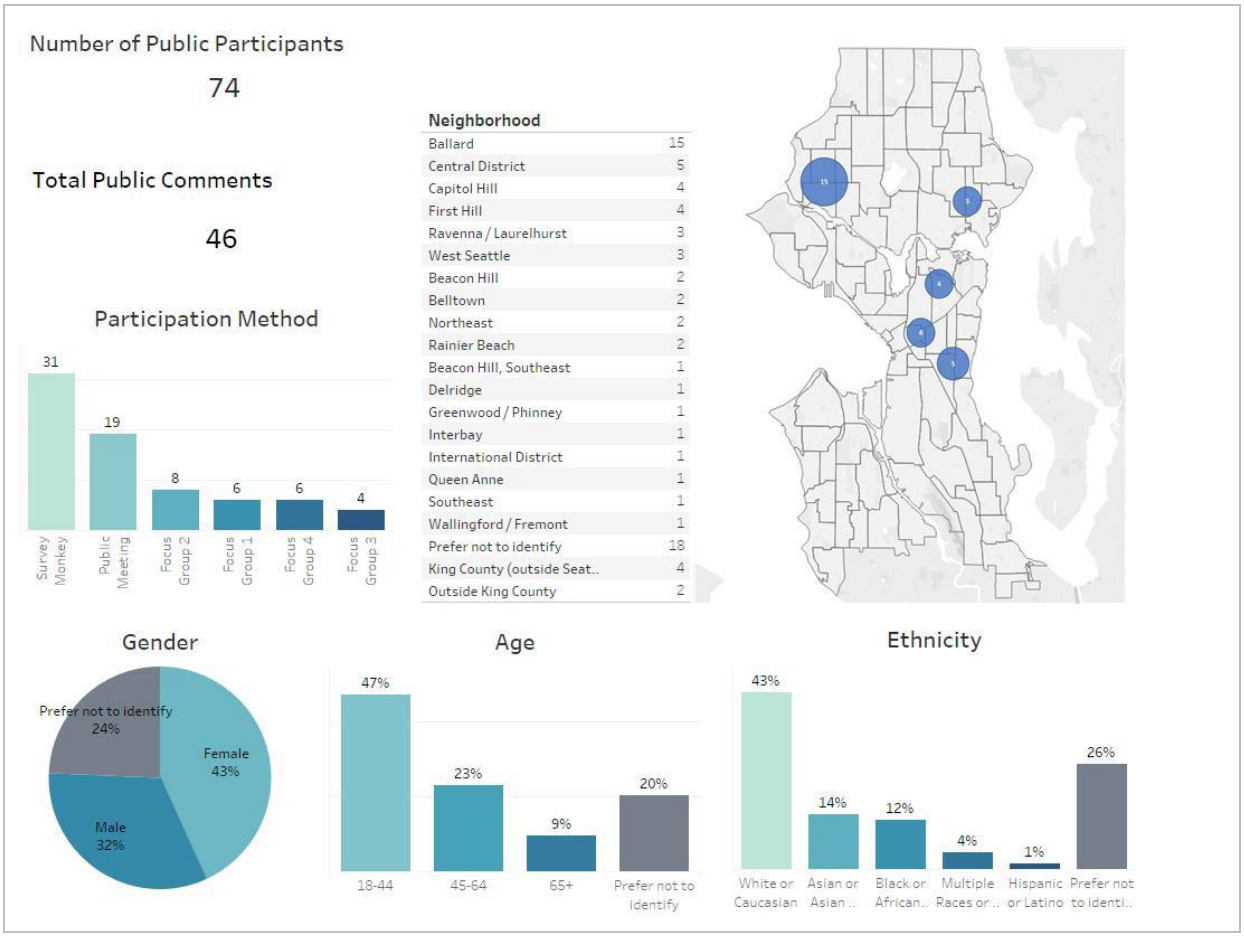
Meeting 4

Community Engaged	Friends of Little Saigon
Date	Wednesday, February 27, 2019

3.0 Public Comment Analysis

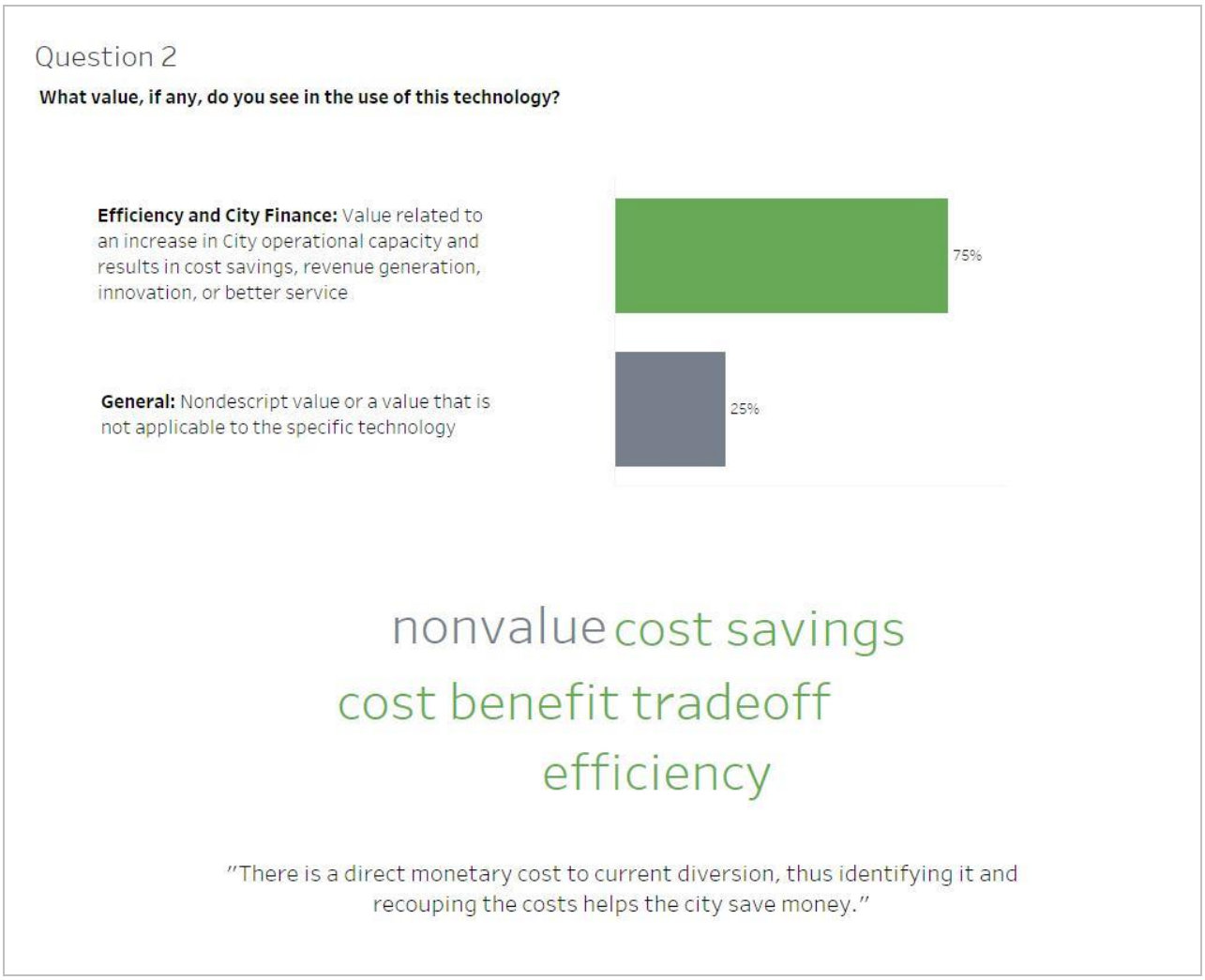
Please note, due to the nature of the comments received and the related purpose of the Seattle City Light technologies, this comment analysis reflects comments received for the SCL Binoculars/Spotting Scope, SensorLink Amp Fork, and Check Meter Device.

3.1 Summary of Response Volume



3.2 Question One: What concerns, if any, do you have about the use of this technology?

3.3 Question Two: What value, if any, do you see in the use of this technology?



3.4 Question Three: What do you want City leadership to consider about the use of this technology?

Question 3

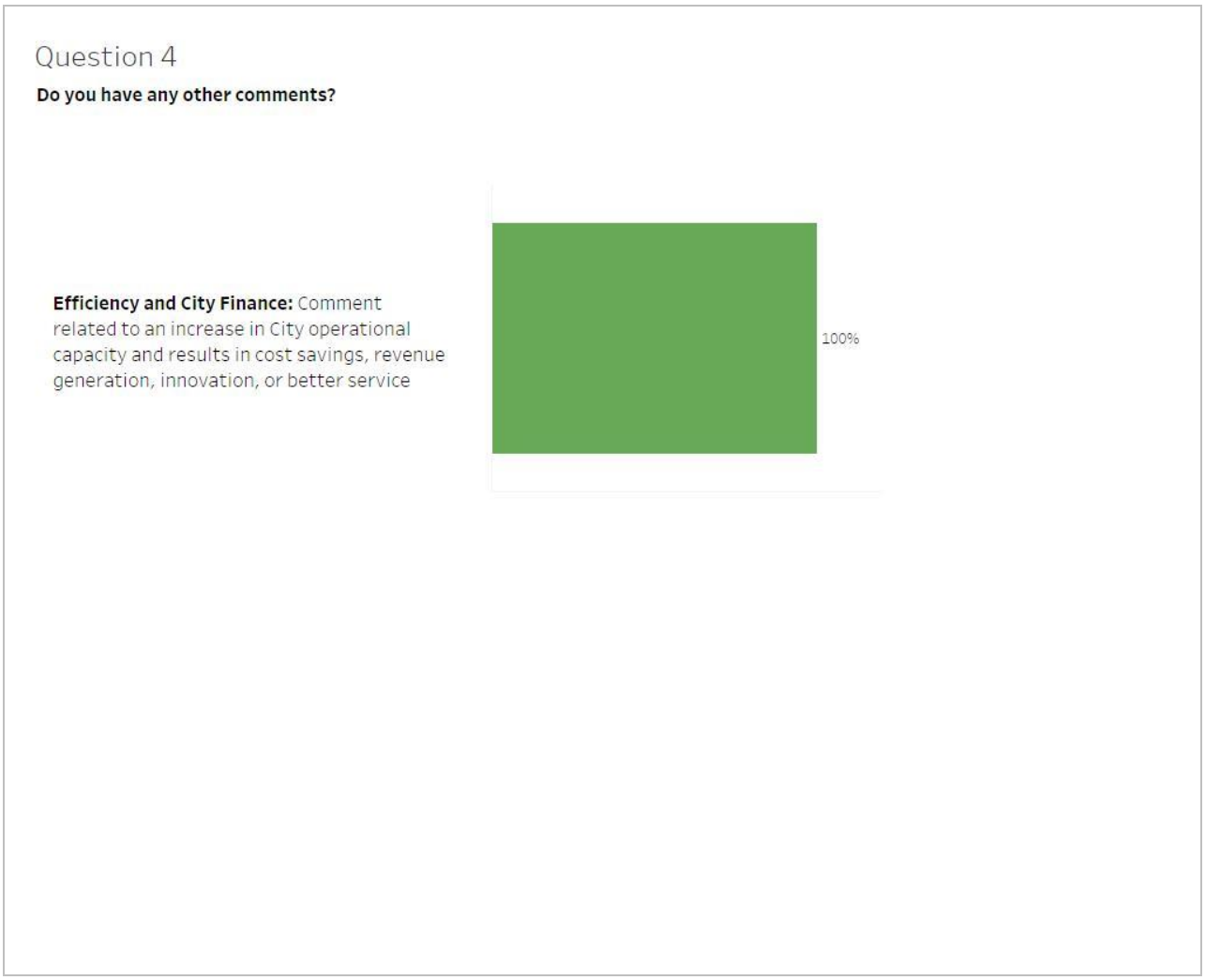
What do you want City leadership to consider about the use of this technology?

Increase policy, enforcement, and oversight: Recommendations related to department and City policy, oversight, accountability, transparency, audit, and policy enforcement.

oversight
reporting statisticscease use

"City leadership should specifically inquire as to what percentage of people/households that were enforcement locations would also be considered low-income. If that percentage is high, then that likely means SCL may cause people to be jailed for effectively being poor (and resourceful); and SCL may have inadequate support offerings for people who are low-income."

3.5 Question Four: Do you have any other comments?



4.0 Equity Annual Reporting

4.1 What metrics for this technology be reported to the CTO for the annual equity assessments?

Seattle City Light is currently working to finalize these metrics.

Privacy and Civil Liberties Assessment

Purpose

This section shall be completed after public engagement has concluded and the department has completed the racial equity toolkit section above. The privacy and civil liberties assessment is completed by the community surveillance working group ("working group"), per the surveillance ordinance which states that the working group shall:

"Provide to the executive and the City Council a privacy and civil liberties impact assessment for each SIR that must be included with any departmental request for surveillance technology acquisition or in-use approval. The impact assessment shall include a description of the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities. The CTO shall share with the working group a copy of the SIR that shall also be posted during the period of public engagement. At the conclusion of the public engagement period, the CTO shall share the final proposed SIR with the working group at least six weeks prior to submittal of the SIR to Council for approval. The working group shall provide its impact assessment in writing to the executive and the City Council for inclusion in the SIR within six weeks of receiving the final proposed SIR. If the working group does not provide the impact assessment before such time, the working group must ask for a two-week extension of time to City Council in writing. If the working group fails to submit an impact statement within eight weeks of receiving the SIR, the department and City Council may proceed with ordinance approval without the impact statement."

Working Group Privacy and Civil Liberties Assessment

The Working Group's Privacy and Civil Liberties Impact Assessment for this technology is below, and is also included in the Ordinance submission package, available as an attachment.

From: Seattle Community Surveillance Working Group (CSWG) To: Seattle City Council

Date: June 4, 2019

Re: Privacy and Civil Liberties Impact Assessment for Check Meter Device, SensorLink Amp Fork, and Binoculars/Spotting Scope (Current Diversion Technologies, SDOT)

Executive Summary

On April 25, 2019, the CSWG received the Surveillance Impact Reports (SIRs) on three Current Diversion Technologies (Check Meter Device, SensorLink Amp Fork, and Binoculars/Spotting Scope) used by Seattle City Light (SCL) included in Group 2 of the Seattle Surveillance Ordinance technology review process. This document is CSWG's Privacy and Civil Liberties Impact Assessment for these technologies as set forth in SMC 14.18.080(B)(1), which we provide for inclusion in the final SIRs submitted to the City Council.

This document first provides recommendations in this executive summary, then provides background information, key concerns, and outstanding questions on the current diversion technologies.

Our assessment of the three current diversion technologies (Check Meter Device, SensorLink Amp Fork, and Binoculars/Spotting Scope) focuses on two key issues:

(1) The use of these systems and the data collected by them for purposes other than those intended;
(2) Over-collection and over-retention of data.

While the stated purposes of the three current diversion technologies may be relatively innocuous, it is important to note that these technologies may be used to gather identifying information about individuals. Particularly in the absence of written, explicit policies governing what these technologies can and cannot be used for, the data collected by these technologies may compromise the privacy of individuals and may be misused to target individuals and communities. It is important that these technologies have explicit protections limiting the use of these tools to their intended purpose.

Recommendations

We recommend that the Council and SCL adopt clear and enforceable rules that ensure, at a minimum, the following:

(1) Define purpose of use for each technology and restrict its use to that purpose.
(2) Ensure there are clear data protection policies to safeguard stored data.
(3) Ensure the deletion of data collected by the technology immediately after the relevant current diversion investigation has closed.

Background on the Three Current Diversion Technologies

The Check Meter Device, the SensorLink Amp Fork, and the Binoculars/Spotting Scope are technologies used by SCL's Current Diversion Team to investigate when electricity is being used without being paid for.

The Check Meter Device is a device that measures the amount of electrical energy flowing through a service-drop wire over time. It digitally captures the information for later retrieval by the Current Diversion Team member(s) via a wireless protocol. These devices are typically installed on an electric pole adjacent to a transformer for a period of one week to one month. The stated purpose of this technology is to determine the valuation of the energy illegally diverted.

The SensorLink Amp Fork is a hand-held electrical device used to detect current flow. It is mounted on an extensible pole (up to 40' to 50') that allows a circular clamp to be placed around a wire. The device then displays instantaneous readings of the amount of electrical energy flow. The Current Diversion Team member may then compare those reads against the readings displayed on the electric meter, allowing staff to determine if current is being diverted.

The Binoculars/Spotting Scope is a device used to determine if current diversion is taking place when distance is a barrier to physical inspection. Binoculars may also be used to determine if potentially dangerous alterations to City Light's electrical infrastructure exist. The relevant SIR states that the binoculars do not collect data, and do not contain any special enhancements requiring power (e.g., night vision or video-recording capabilities).[1]

Key Concerns Regarding all Three Current Diversion Technologies

Seattle City Light's policy:

(1) **Does not include explicit, written restrictions on use.** An April 3, 2019 email from Seattle City Light to the ACLU stated that "Seattle City Light does not have any formal, explicit, written policies on what the technologies can be used for."[2] The email states that Section 3.0 (Use Governance) of the SIRs describes SCL's standards, but this section does not contain meaningful restrictions on use. The absence of written, specific policies increases the risk of misuse.

(2) **Does not include specific data protection provisions.** For example, the draft SIR for the Check Meter Device (SensorLink Transformer Meter System) says that the data is retrieved from the device "via secure radio protocol," but the SIR does not explain further. Radio frequencies are not inherently secure, so the policy should define how this data is secured, including when it is on the Check Meter Device and once it is stored off the device.

(3) **Includes an unjustifiably long data retention period.** According to Seattle City Light, the retention period for current diversion data collected is at least 6 years.[3] Such a lengthy retention period for electricity diversion investigation records is unnecessary. Data should be deleted as soon as an investigation is closed.

In addition, all three SIRs state: "City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible." This equity analysis should be provided for public review.

[1] 2019 Surveillance Impact Report SCL Check Meter Device, pages 3-6.

[2] See pages 3-4 for Seattle City Light Response to ACLU-WA on April 3, 2019.

[3] Ibid.

City of Seattle

Seattle City Light

700 5th Ave. | P.O. Box 34023 | Seattle WA 98124-4023
TEL (206) 684-3000 TTY/TDD (206) 684-3225 FAX (206) 625-3709
seattle.gov/light
twitter.com/SEACityLight facebook.com/SeattleCityLight

April 3, 2019

Shankar Narayan, Technology and Liberty Project Director
Jennifer Lee, Technology and Liberty Project Advocate
American Civil Liberties Union – Washington
901 Fifth Ave, Suite 630
Seattle, WA 98164

Dear Shankar and Jennifer,

We have received your letter dated March 20, 2019 with comments on the three Seattle City Light technologies included in Group 2 of the Seattle Surveillance Ordinance process. We appreciate your feedback, which will be considered as the Surveillance Impact Reports (SIRs) are finalized.

In the meantime, I can offer the below information related to your two questions:

What enforceable policies, if any, apply to use of these three technologies?

Current Diversion Detection Technology Policies: Seattle City Light does not have any formal, explicit, written policies on what the technologies can be used for. However, City Light's draft 2019 Surveillance Impact Reports (SIRs) outline the non-written standards for use of the technologies. Please refer to Section 3.0, "Use Governance," of the attached SIRs for the three current diversion technologies, as they describe City Light's standards.

Also, please know that City Light has formally adopted a Department Policy & Procedure (DPP P III-416, "Current Diversion") governing the prevention, detection, reporting, investigation, and correction of illegal, unauthorized, or inadvertent diversions of electric current, and the recovery of associated lost revenues and costs. Please see the attached DPP.

What is Seattle City Light's data retention schedule?

City Light follows the record retention period presented in the following chart.

An equal employment opportunity, affirmative action employer. Accommodations for people with disabilities provided upon request.

City of Seattle

Retention Schedule	Series Title and Description	DAN #	Retention and Disposition Action (Primary Record Copy)	Designation
Utility Services Power Distribution	ELECTRICITY DIVERSION INVESTIGATION RECORDS Inquiry regarding problems or discrepancies with meters, either from meter reader or other parties. Investigation records may include: site visit dates, notes regarding location, pictures of meter or surrounding area, consumption history, special meter read, and service order for technical support.	UT55-05G-07 Rev. 0	Investigation closed plus 6 years	Non-Archival Non-Essential OPR

Please let me know if you have additional questions.

Sincerely,

Julie Moore
Public Information Officer
Seattle City Light

City of Seattle

CTO Response

Memo

Date: 11/17/2020

To: Seattle City Council, Transportation and Utilities Committee

From: Saad Bashir

Subject: CTO Response to the Surveillance Working Group SCL Current Diversion Technologies SIR Review

---

To the Council Transportation and Utilities Committee,

I look forward to continuing to work together with Council and City departments to ensure transparency about the use of surveillance technologies and finding a mutually agreeable means to use technology to improve City services while protecting the privacy and civil rights of the residents we serve. Specific concerns in the Working Group comments about SCL's Current Diversion Technologies are addressed in the attached document.

As provided in the Surveillance Ordinance, SMC 14.18.080, this memo outlines the Chief Technology Officer's (CTO's) response to the Surveillance Working Group assessment on the Surveillance Impact Report for Seattle City Light's Current Diversion Technologies, including the Check Meter Device, SensorLink Amp Fork, and Binoculars/Spotting Scope.

Background

The Information Technology Department (ITD) is dedicated to the Privacy Principles and Surveillance Ordinance objectives to provide oversight and transparency about the use and acquisition of specialized technologies with potential privacy and civil liberties impacts. All City departments have a shared mission to protect lives and property while balancing technology use and data collection with negative impacts to individuals. This requires ensuring the appropriate use of privacy invasive technologies through technology limitations, policy, training and departmental oversight.

The CTO's role in the SIR process has been to ensure that all City departments are compliant with the Surveillance Ordinance requirements. As part of the review work for surveillance technologies, ITD's Privacy Office has facilitated the creation of the Surveillance Impact Report documentation, including collecting comments and suggestions from the Working Group and members of the public about these technologies. IT and City departments have also worked collaboratively with the Working Group to answer additional questions that came up during their review process.

Technology Purpose

Seattle City Light's Current Diversion Team (CDT) consists of a group of approximately five journey-level engineers who are dispatched to collect data to attempt to determine whether a suspected diversion of current (i.e., alterations to the City Light-owned electrical system by a third-party in order to consume electric power without it being registered by the City Light meter installed for that purpose) has taken

place. Diversion alterations can result in injury to people and can damage SCL equipment and Infrastructure. Further, SCL is required by law (SMC 21.49.100) to collect payment for utility use and so investigates and remediates any loss of payment created by such situations.

In support of this mission, the CDT crew uses a Check Meter Device, SensorLink Amp Fork, and Binoculars/Spotting Scope. If a determination of diversion is sustained, data may be used to respond to lawful requests from the proper law enforcement authorities for evidence for recovering the value of the diverted energy.

Working Group Concerns

In their review, the Working Group has raised concerns about these Current Diversion Technologies being used in a privacy impacting way, including use of these systems for other than their stated purpose, and over-collection and over-retention of the data collected.

1) The use of these systems and the data collected by them for purposes other than those intended.
2) Over-collection and over-retention of data.

The policy and training enacted by SCL and limitations from the technologies themselves provide adequate mitigation for the potential privacy and civil liberties concerns raised by the Working Group about the use of this important operational technology.

Response to Specific Concerns: SCL Current Diversion Technologies

Concern: Use of these systems and the data collected by them for purposes other than those intended.

CTO Assessment: SCL's Department Policy & Procedure, DPP P III-416 outlines the process for determining why and how the department investigates suspected current diversion. This policy includes how evidence (such as data collected from current diversion technologies) must be handled and who is authorized to receive a report. Some of the technologies are not capable of sharing data outside of additional manual observations, and any data as a part of the investigation is securely stored and only accessible by members of the Current Diversion Team. This body of policy and operational documentation provides detail about how the technology is used and how any data collected is managed, and it is our assessment that the documentation provides adequate protections.

SIR Response:
Check Meter Device
Section 3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

"The CDT owns six SensorLink TMS units, which are deployed on the basis of case number and need. Deployment level on a given case can vary from none (zero) to all (six). Once a case is properly opened, CDT crew members may check them out without prior additional authorization, though the Current Diversion Coordinator is under nearly all circumstances aware of deployment due to position

responsibilities. Serial numbers are recorded and the CDT member to whom they are assigned, as well as their deployment status, are logged."

Section 4.2 What measures are in place to minimize inadvertent or improper collection of data?

"Risk of inadvertent or improper collection is low for two reasons. First, the CDT only investigates specific, metered locations previously identified and properly documented as sites of suspected current diversion. And second, SensorLink TMS devices are used only on those service-drop lines that are delivering electrical service to the suspected location."

Amp Fork

Section 3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

"The limited number of this equipment and of CDT members makes the routine tracking of the Ampstik devices relatively straight-forward. Ampstiks are issued to CDT members, and stored in their official vehicles. These vehicles are operated, locked, and stored in accordance with Utility security procedures. Ampstiks' serial numbers are recorded and the CDT member to whom they are assigned, as well as their deployment status, are logged."

Section 4.2 What measures are in place to minimize inadvertent or improper collection of data?

"Risk of inadvertent or improper collection is low for two reasons. First, the CDT only investigates specific, metered locations previously identified as sites of suspected current diversion. And second, Ampstik devices are used only on those service-drop lines that are delivering electrical service to the suspected location."

Binoculars

Section 3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

"The limited number of this equipment and of CDT members makes the routine tracking of the binoculars relatively straight-forward. Binoculars are issued to CDT members, and stored in their official vehicles. These vehicles are operated, locked, and stored in accordance with Utility security procedures."

Section 4.2 What measures are in place to minimize inadvertent or improper collection of data?

"Risk of inadvertent or improper collection is low. The CDT only investigates specific meters and other implicated electrical equipment at locations previously identified and properly documented as sites of suspected current diversion."

Concern: Data Protection Policies

CTO Assessment: The data storage location and access controls are adequate for protecting information collected by these technologies during current diversion investigations. All users that have access to this data have an authorized and specified use for the data. For those devices that are capable of collecting data, none is retained on the device, and any data stored would be kept in line with the department retention policy.

SIR Response:

Check Meter Device

Section 4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

"Data obtained by means of the SensorLink TMS device are stored in a private folder on City Light's digital file locations, accessible only by CDT members and management. Data stored in the SensorLink TMS device itself are deleted after its observations are retrieved by the CDT and/or upon its removal from the electrical pole (i.e., no data remain on the SensorLink TMS once its use for a given determination of current diversion has been completed and before it is therefore made available to other CDT staff for subsequent deployment)."

Amp Fork

Section 4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

"Data obtained by means of the Ampstik are stored in a private folder on City Light's digital file locations. The data, as well as incident reports, are accessible only by CDT members and its Current Diversion Coordinator."

Binoculars

Section 4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

"Data obtained by means of binoculars (which consist of notes made by staff based on their binocular-facilitated observations) are stored in a private folder on City Light's digital file locations. The data, as well as overall incident reports, are accessible only by CDT members and its Current Diversion Coordinator."

Concern: Overcollection and over retention of data

CTO Assessment: SCL follows legally required retention periods that ensure that only data that is necessary to complete an investigation is preserved after the investigation in case of any dispute. The data is protected and only accessible by those who are related to the investigation

SIR Response:
Check Meter Device
Section 4.7 How will data that is collected be accessed and by whom?

"CDT members, who are journey-level electrical workers trained in the placement, use, and removal of the SensorLink TMS device, may collect this data. The quantitative data – accumulated consumption (in kilowatt-hours), average volts (current strength), average amps (current flow), and interval consumption (in kilowatt-hours per a pre-defined time-unit) – are accessed by CDT crew members remotely using a secure radio protocol and a specific, password-protected software program, known as Steelhead."

Section 4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

"Data obtained by means of the SensorLink TMS device are stored in a private folder on City Light's digital file locations, accessible only by CDT members and management. Data stored in the SensorLink TMS device itself are deleted after its observations are retrieved by the CDT and/or upon its removal from the electrical pole (i.e., no data remain on the SensorLink TMS once its use for a given determination of current diversion has been completed and before it is therefore made available to other CDT staff for subsequent deployment)."

Amp Fork
Section 4.7 How will data that is collected be accessed and by whom?

"CDT members, who are journey-level electrical workers trained in the use of the Ampstik, may collect and access this data. Additionally, the Current Diversion Coordinator may access the data."

Section 4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

"Data obtained by means of the Ampstik are stored in a private folder on City Light's digital file locations. The data, as well as incident reports, are accessible only by CDT members and its Current Diversion Coordinator."

Binoculars
Section 4.7 How will data that is collected be accessed and by whom?

"CDT members, who are journey-level electrical workers trained in the proper use this equipment, may collect these data. These consist of meter reads and, in certain instances, other implicated electrical equipment that poses a present danger to the public or the electrical system integrity."

Section 4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

"Data obtained by means of binoculars (which consist of notes made by staff based on their binocular-facilitated observations) are stored in a private folder on City Light's digital file locations. The data, as well as overall incident reports, are accessible only by CDT members and its Current Diversion Coordinator."

SCL's Required Retention period

Retention Schedule	**Series Title and Description**	**DAN #**	**Retention and Disposition Action (Primary Record Copy)**	**Designation**
Utility Services Power Distribution	ELECTRICITY DIVERSION INVESTIGATION RECORDS Inquiry regarding problems or discrepancies with meters, either from meter reader or other parties. Investigation records may include: site visit dates, notes regarding location, pictures of meter or surrounding area, consumption history, special meter read, and service order for technical support.	UT55-05G-07 Rev. 0	Investigation closed plus 6 years	Non-Archival Non-Essential OPR

Appendix A: Glossary

Accountable: (taken from the racial equity toolkit.) Responsive to the needs and concerns of those most impacted by the issues you are working on, particularly to communities of color and those historically underrepresented in the civic process.

Community outcomes: (taken from the racial equity toolkit.) The specific result you are seeking to achieve that advances racial equity.

Contracting equity: (taken from the racial equity toolkit.) Efforts to achieve equitable racial outcomes in the way the City spends resources, including goods and services, consultants and contracting.

DON: "department of neighborhoods."

Immigrant and refugee access to services: (taken from the racial equity toolkit.) Government services and resources are easily available and understandable to all Seattle residents, including non-native English speakers. Full and active participation of immigrant and refugee communities exists in Seattle's civic, economic and cultural life.

Inclusive outreach and public engagement: (taken from the racial equity toolkit.) Processes inclusive of people of diverse races, cultures, gender identities, sexual orientations and socio-economic status. Access to information, resources and civic processes so community members can effectively engage in the design and delivery of public services.

Individual racism: (taken from the racial equity toolkit.) Pre-judgment, bias, stereotypes about an individual or group based on race. The impacts of racism on individuals including white people internalizing privilege, and people of color internalizing oppression.

Institutional racism: (taken from the racial equity toolkit.) Organizational programs, policies or procedures that work to the benefit of white people and to the detriment of people of color, usually unintentionally or inadvertently.

OCR: "Office of Civil Rights."

Opportunity areas: (taken from the racial equity toolkit.) One of seven issue areas the City of Seattle is working on in partnership with the community to eliminate racial disparities and create racial equity. They include: education, health, community development, criminal justice, jobs, housing, and the environment.

Racial equity: (taken from the racial equity toolkit.) When social, economic and political opportunities are not predicted based upon a person's race.

Racial inequity: (taken from the racial equity toolkit.) When a person's race can predict their social, economic, and political opportunities and outcomes.

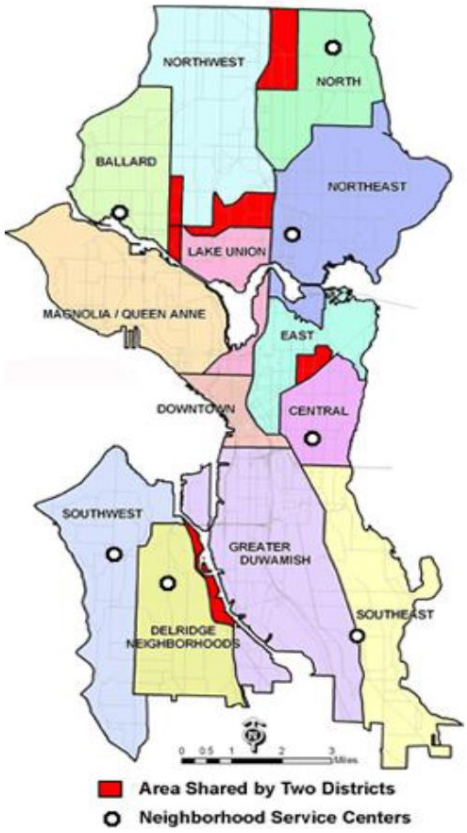
RET: "racial equity toolkit"

Seattle neighborhoods: (taken from the racial equity toolkit neighborhood.) Boundaries defined for the purpose of understanding geographic areas in Seattle.

Stakeholders: (taken from the racial equity toolkit.) Those impacted by proposed policy, program, or budget issue who have potential concerns or issue expertise. Examples might include: specific racial/ethnic groups, other institutions like Seattle housing authority, schools, community-based organizations, change teams, City employees, unions, etc.

Structural racism: (taken from the racial equity toolkit.) The interplay of policies, practices and programs of multiple institutions which leads to adverse outcomes and conditions for communities of color compared to white communities that occurs within the context of racialized historical and cultural conditions.

Surveillance ordinance: Seattle City Council passed ordinance 125376, also referred to as the "surveillance ordinance."



SIR: "surveillance impact report", a document which captures the fulfillment of the Council-defined surveillance technology review process, as required by ordinance 125376.

Workforce equity: (taken from the racial equity toolkit.) Ensure the City's workforce diversity reflects the diversity of Seattle.

City of Seattle

Appendix B: Meeting Notice(s)

City Surveillance Technology Fair

February 27, 2018

6:00 p.m. – 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Join us for a public meeting to comment on a few of the City's surveillance technologies:

Seattle City Light
- Binoculars
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation
- Acyclica

Seattle Fire Department
- Computer Aided Dispatch

Seattle Police Department
- 911 Call Logging Recorder
- Computer Aided Dispatch
- CopLogic

Can't join us in person?

Visit www.seattle.gov/privacy to leave an online comment or send your comment to **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** The Open Comment period is from **February 5 - March 5, 2019.**

Please let us know at Surveillance@seattle.gov if you need any accommodations. For more information, visit Seattle.gov/privacy.

Surveys, sign-in sheets and photos taken at this event are considered a public record and may be subject to public disclosure. For more information see the Public Records Act RCW Chapter 42.56 or visit Seattle.gov/privacy. All comments submitted will be included in the Surveillance Impact Report.

City of Seattle

Giám Sát Thành Phố
Hội Chợ Công Nghệ

ngày 27 tháng 2 năm 2019
6 :00 giờ chiều – 8:00 giờ chiều
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Hãy tham gia cuộc họp công cộng cùng chúng tôi để nhận xét về một số công nghệ giám sát của Thành phố:

Seattle City Light
- Ống nhòm quan sát
- Sensorlink Ampstik
- Đồng hồ đo máy biến áp của Sensorlink

Seattle Department of Transportation (Sở Giao Thông Vận Tải Seattle)
- Acyclica

Seattle Fire Department (Sở Phòng Cháy Chữa Cháy Seattle)
- Hệ Thống Thông Tin Điều Vận Có Máy Tính Trợ Giúp

Seattle Police Department (Sở Cảnh Sát Seattle)
- Hệ Thống Ghi Âm Cuộc Gọi 911
- Hệ Thống Thông Tin Điều Vận Có Máy Tính Trợ Giúp
- CopLogic

Quý vị không thể tới tham dự trực tiếp cùng chúng tôi?

Hãy truy cập www.seattle.gov/privacy và để lại nhận xét trực tuyến hoặc gửi ý kiến của quý vị tới **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** Giai đoạn Góp Ý Mở từ **Ngày 5 tháng 2 - Ngày 5 tháng 3 năm 2019.**

Vui lòng thông báo cho chúng tôi tại Surveillance@seattle.gov nếu quý vị cần bất kỳ điều chỉnh nào. Để có thêm thông tin, hãy truy cập Seattle.gov/privacy.

Các khảo sát, danh sách đăng ký và ảnh chụp tại sự kiện này được coi là thông tin công cộng và có thể được tiết lộ công khai. Để biết thêm thông tin, hãy tham khảo Public Records Act (Đạo Luật Hồ Sơ Công Cộng) RCW Chương 42.56 hoặc truy cập Seattle.gov/privacy. Tất cả các ý kiến đóng góp mà quý vị gửi đến sẽ được đưa vào Báo Cáo Tác Động Giám Sát.

City of Seattle

Eksibisyon ng Teknolohiya Sa Pagmamatyag sa Lungsod

Pebrero 27, 2019

6:00 p.m. - 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Samahan kami para sa isang pampublikong pagpupulong upang magbigay ng komento sa ilan sa mga teknolohiya sa pagmamanman ng Lungsod:

Seattle City Light
- Mga Binocular
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation (Departamento ng Transportasyon ng Seattle)
- Acyclica

Seattle Fire Department (Departamento para sa Sunog ng Seattle)
- Pagdispatsa sa Tulong ng Computer

Seattle Police Department (Departamento ng Pulisya ng Seattle)
- Rekorder ng Pagtawag sa 911
- Pagdispatsa sa Tulong ng Computer
- CopLogic

Hindi kami masasamahan nang personal?

Bumisita sa www.seattle.gov/privacy upang mag-iwan ng online na komento o ipadala ang iyong komento sa **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** Ang panahon ng Bukas na Pagkomento ay sa **Pebrero 5 - Marso 5, 2019.**

Mangyaring ipaalam sa amin sa Surveillance@seattle.gov kung kailangan mo ng anumang tulong. Para sa higit pang impormasyon, bumisita sa Seattle.gov/privacy.

Itinuturing na pampublikong rekord ang mga survey, papel sa pag-sign-in at mga larawan na makukuha sa pangyayaring ito at maaaring mapasailalim sa paghahayag sa publiko. Para sa higit pang impormasyon, tingnan ang Public Records Act (Batas sa Mga Pampublikong Rekord) RCW Kabanata 42.56 o bumisita sa Seattle.gov/privacy. Isasama ang lahat ng isinumiteng komento sa Surveillance Impact Report (Ulat sa Epekto ng Pagmamanman).

City of Seattle

Feria de tecnología de vigilancia ciudadana

27 febrero de 2019

De 6:00 p. m. a 8:00 p. m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Acompáñenos en la reunión pública para dar su opinión sobre algunas de las tecnologías de vigilancia de la ciudad:

Seattle City Light
- Binoculars
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation (Departamento de Transporte de Seattle)
- Acyclica

Seattle Fire Department (Departamento de Bomberos de Seattle)
- Computer Aided Dispatch

Seattle Police Department (Departamento de Policía de Seattle)
- 911 Call Logging Recorder
- Computer Aided Dispatch
- CopLogic

¿No puede asistir en persona?

Visite www.seattle.gov/privacy para dejar un comentario en línea o enviar sus comentarios a **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** El período de comentarios abiertos es desde el **5 de febrero al 5 de marzo de 2019.**

Avísenos en Surveillance@seattle.gov si necesita adaptaciones especiales. Para obtener más información, visite seattle.gov/privacy.

Las encuestas, las planillas de asistencia y las fotos que se tomen en este evento se consideran de dominio público y pueden estar sujetas a la difusión pública. Para obtener más información, consulte la Public Records Act (Ley de Registros Públicos), RCW capítulo 42.56, o visite Seattle.gov/privacy. Todos los comentarios enviados se incluirán en el Informe del efecto de la vigilancia.

City of Seattle

Kormeerida Bandhigga Tiknoolajiyada ee Magaalada

Feebaraayo 27, 2019
6:00 p.m. - 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Nagulasoo biir bandhigga dadweynaha si fikir looga dhiibto dhawr kamid ah aaladaha tiknoolajiyada ee City surveillance:

Seattle City Light
- Binoculars
- Sensorlink Ampstik
- Sensorlink Cabiraha mitirka Gudbiyaha

Seattle Department of Transportation
(Waaxda Gaadiidka ee Seattle)
- Acyclica

Seattle Fire Department
(Waaxda Dab damiska ee Seattle)
- Adeeg Qaybinta Kumbuyuutarka loo adeegsado

Seattle Police Department
(Waaxda Booliiska ee Seattle)
- Qalabka Duuba Wicitaanada 911
- Computer Aided Dispatch
- CopLogic

Nooguma imaan kartid miyaa si toos ah?

Booqo barta www.seattle.gov/privacy si aad fikirkaaga oonleen ahaan uga dhiibato **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.**
Mudada Fikrad Dhiibashadu furantahay waxay kabilaabanaysaa **Feebaraayo 5 - Maarso 5, 2019.**

Fadlan noogusoo gudbi ciwaankaan Surveillance@seattle.gov hadaad ubaahantahay hooy laguusii qabto. Wixii macluumaad dheeri ah, booqo Seattle.gov/privacy.

Xog aruurinada, waraaqaha lasaxixaayo iyo sawirada lagu qaado munaasabadaan waxaa loo aqoonsanayaa diiwaan bulsho waxaana suuragal ah in bulshada lagu dhex faafiyo. Wixii macluumaad dheeri ah kafiiri Public Records Act (Sharciga Diiwaanada Bulshada) RCW Cutubkiisa 42.56 ama booqo Seattle.gov/privacy. Dhammaan fikradaha ladhiibto waxaa lagusoo darayaa Warbixinta ugu danbaysa ee Saamaynta Qalabka Muraaqabada.

City of Seattle

城市监控技术博览会

2019 年 2 月 27 日
下午 6:00 至下午 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 9810

加入我们的公众会议，留下您对纽约市监控技术的意见：

Seattle City Light
- 望远镜
- Sensorlink Ampstik
- Sensorlink 变压器表

Seattle Department of Transportation（西雅图交通局）
- Acyclica

Seattle Fire Department（西雅图消防局）
- 计算机辅助调度

Seattle Police Department（西雅图警察局）
- 911 通话记录录音器
- 计算机辅助调度
- CopLogic

无法亲自前来？

访问 www.seattle.gov/privacy 发表在线评论或将您的意见发送至 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124。开放评论期：2019 年 2 月 5 日至 3 月 5 日。

如果您需要任何住宿服务，请通过 Surveillance@seattle.gov 联系我们。要获得更多信息，请访问 Seattle.gov/privacy。

此次活动中的调查、签到表和照片被视为公共记录，可能会被公开披露。有关更多信息，请参阅 Public Records Act（信息公开法）RCW 第 42.56 章或访问 Seattle.gov/privacy。提交的所有意见都将包含在监控影响报告内。

City of Seattle

도시 감시 기술 박람회

2019 년 2 월 27 일
오후 6:00 – 오후 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

공개모임에 참여하시고, 도시 감시 기술과 관련한 의견을 공유해 주십시오.

Seattle City Light
- 쌍안경
- Sensorlink Ampstik
- Sensorlink 변압기 미터

Seattle Department of Transportation(시애틀 교통국)
- Acyclica

Seattle Fire Department(시애틀 소방국)
- 컴퓨터 지원 출동 지시

Seattle Police Department(시애틀 경찰국)
- 911 전화 기록 녹음기
- 컴퓨터 지원 출동 지시
- CopLogic

현장 참여가 어려우신가요?

www.seattle.gov/privacy 를 방문하셔서 온라인 의견을 남기시거나 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124 로 의견을 송부해 주시기 바랍니다. 공개 의견 수렴 기간은 2019 년 2 월 5 일 – 3 월 5 일입니다.

편의사항이 필요하신 경우 Surveillance@seattle.gov 로 문의해 주시기 바랍니다.
자세한 정보는 Seattle.gov/privacy 를 참조해 주십시오.

본 행사에서 수집된 설문 조사, 참가 신청서 및 사진은 공개 기록으로 간주되며 일반에 공개될 수 있습니다. 자세한 사항은 Public Records Act(공공기록물법) RCW 챕터 42.56 을 참조하시거나, Seattle.gov/privacy 를 방문하시기 바랍니다. 제출된 모든 의견은 감시 영향 보고서에 수록됩니다.

City of Seattle

城市監視技術展覽會

2019 年 2 月 27 日
下午 6:00 至下午 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

加入我們的公眾會議，留下您對紐約市監視技術的意見：

Seattle City Light
- 望遠鏡
- Sensorlink Ampstik
- Sensorlink 變壓器表

Seattle Department of Transportation（西雅圖交通局）
- Acyclica

Seattle Fire Department（西雅圖消防局）
- 電腦輔助發送

Seattle Police Department（西雅圖警察局）
- 911 通話紀錄錄音機
- 電腦輔助發送
- CopLogic

無法親自前來？

造訪 www.seattle.gov/privacy 發表線上評論或將您的意見傳送至 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124。開放評論期：2019 年 2 月 5 日至 3 月 5 日。

如果您需要任何便利服務，請透過 Surveillance@seattle.gov 聯絡我們。要獲得更多資訊，請造訪 Seattle.gov/privacy。

此次活動中的調查、簽入表和照片被視為公共紀錄，可能會被公開披露。有關更多資訊，請查閱 Public Records Act（資訊公開法）RCW 第 42.56 章或造訪 Seattle.gov/privacy。提交的所有意見都將包含在監視影響報告內。

City of Seattle

Appendix C: Meeting Sign-in Sheet(s)

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☒ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☒ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

☐ Include Middle Eastern

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☒ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☒ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☒ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☑ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☑ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☒ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☒ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☑ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☒ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☒ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☑ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☑ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☑ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

2

Queen Anne

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☑ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☑ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☒ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☒ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☒ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood
- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☑ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity
- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☑ White
- ☐ Prefer not to Identify

Age
- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender
- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood
- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity
- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age
- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender
- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

X

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☒ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☒ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☒ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☒ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☒ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☒ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☑ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

leighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
☒ First Hill
] Georgetown
] Greenwood / Phinney

☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
☒ Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☒ 18-44
☐ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☒ Female
☐ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☑ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
] Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☐ 45-64
☑ 65+
☐ Prefer not to identify

Gender

☐ Female
☑ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

☑ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
] Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☑ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☑ Female
☐ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney
SE KING COUNTY

☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☑ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
✓ Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☑ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☐ Female
☑ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☒ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☒ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☒ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☒ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☒ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☑ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☑ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☑ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☑ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☑ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☑ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Appendix D: Department of Neighborhood Focus Group Notes

Friends of Little Saigon (FOLS)

Please select which technology you wish to comment on:

☐SCL: Binoculars ☐SCL: Sensorlink Transformer Meter (TMS) ☐SFD: Computer-Aided Dispatch ☐SPD:9-11 Call Recorder

☐SCL: Sensorlink Ampstik ☐SDOT: Acyclica ☐SPD: Computer-Aided Dispatch ☒SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

- Will they keep the data safe on coplogic?
- Can it be hacked?
- What if you report your neighbour and your neighbour hacks the system and find out?
- What is the money amount limit for coplogic / Why is there a limit for coplogic?: (a community member says that she believes that the limit $500 or under, but it's hard to have a limit because a lot of packages cost more than $500 such as electronics get stolen and you won't be able to report it online)
- The departement is having all these technologies being used but not letting the public aware of it
- Coplogic is not clear and is confusing to use (what you can report and what you can't report)
- If coplogic is known by the community would they use it ? (Community members agreed that no one would use coplogic because it's not in Vietnamese. Not even people who speak english fluently even use it.
- Many community members don't trust the system)

What value, if any, do you see in the use of this technology?

- Coplogic has been going on for a few years it's not very effective. The only effective thing is that coplogic is doing saving police hours and time.

What do you want City leadership to consider about the use of this technology?

- Most of the time, our community don't report things because they don't trust the system, they often tell someone that they trust a friend. Is there an option that someone and report a crime for someone else?

Other comments:

- The government should be more transparent with the technology system with the public.
- The translation is much far removed from the actual Vietnamese language.

- The translation is very hard to understand, the language is out of context (The flyer is poorly translate)
- Is there resources to support these technologies? Is there translations so that it is accessible for everyone? Will this accommodate everyone?
- Police should have a software that connects them to translation and interpretation right away instead of having to call a translator
- How will other people know of the technology if they can't come to focus group meetings? Such as flyers? Social media? Etc.
- Besides face to face meetings, are there plans to execute this information of the technology and surveillance to the community?
- Will the City of Seattle go to community events, temple, the church to reach out to the community and explain the technologies?
- These technologies are taking a part of our taxes, so everyone should know. It should be for everyone to know, not only catered to one group or population.

Are there any questions you have, or areas you would like more clarification?

- How effective are the tools/technology?
- How many people know of these technologies? Provide statistics
- What are the statistics of the coplogic?
- What is the data and statistics for coplogic and what are people reporting?
- What is the most common crime that they are reporting?
- And how effective is coplogic based on the statistics and data?

City of Seattle

Friends of Little Saigon (FOLS)

Please select which technology you wish to comment on:

☐SCL: Binoculars	☐SCL: Sensorlink Transformer Meter (TMS)	☐SFD: Computer-Aided Dispatch	☒SPD:9-11 Call Recorder
☐SCL: Sensorlink Ampstik	☐SDOT: Acyclica	☒SPD: Computer-Aided Dispatch	☐SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

- CAD did not work from experience. A community member said that they reported that they needed assistance at 10:00pm and no one showed up, then had to call 911 at 12:00am and someone finally showed up at 4:30am
- Why create more options and technologies if the police department and government can not support it? It's a waste of time and money (taxes). Should have enough personals before they implement technology.
- Government should have enough personals to support translation if they choose to translate.

What do you want City leadership to consider about the use of this technology?

- The city should focus on having the community review the technologies that are yet to be implemented.
- The Vietnamese community is not getting the information we need to report crimes

Other comments:

- Engagement is very important. Engaging the community and engaging different demographics.
- Friday night, Saturdays, and Sunday afternoon work the best for the Vietnamese community.
- If the city wants to involve the vietnamese community and engage the Vietnamese community, it is important to accommodate with our community It is important to proofread the translation, have 3 people proofread. Someone
  pre 1975, post 1975 and current Vietnamese language. The government clearly does not proofread the translation.

Council on American Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington
Thursday, Feb. 21, 2019
Technology Discussed: CopLogic

1. Do you have concerns about this specific technology or how it's used?
    - Having used the system myself the one thing I noted was the type of report you can file, they ask questions like if you knew the suspect, and if you're saying no I don't know who did it. and you check a box that says I understand that no one is going to investigate this
        - What is the point of having a system in place than If no one is going to investigate it
        - It is for common things like my car is broken into and stuff was taken out of my car, you can file it if you need a report for insurance. But if you were to call that and report to the police, they wouldn't come for days
    - So for example if I can be a straight up Islamophobe and I can see a Muslim woman and make a bunch of false reports online, and how long would it take for someone to say I see you making all these reports. Because people can make so many different reports, how do you deal with that
        - There are very limited types of reports that it will accept. So if someone wanted to report graffiti and they were reporting more hate crime related graffiti an officer will review the report
        - So I think the review process would be really important
    - Another barrier is that it's an online system so we need to think about wifi access and there is this assumption that everyone has access to internet and computers. And what I'm hearing is that people can just file a report at a click of their finger. And if these people can do that on their computer what stops them from being able to file all these cases about certain groups and individuals.
    - Additional there have been cases in the past where people are abusing reporting system. This one doesn't allow you to report against known suspect but I could see that happening in the future so I wanted that to be mentioned. The other thing under protection is says all activity can be stored and the data Is monitored by lexis nexus… and this company does a lot of research on crime mapping which brings up some of the concerns on like CVE
        - But what you are saying is that lexis nexus does other mapping that it can use this information for
        - Yes, because I want to clarify what is the technological ambition of SPD because I don't think this would work well in the communities that SPD is supposed to served. And I would want a contract review of what lexis nexus does. Will the info stay on the data and server of lexis nexus, what happens to it
    - Another thing is has SPD given Lexis nexus to use this in any of the research data they do, because they put out a lot of information regarding mapping, and crime control. And what information are they allowed to take
    - We have seen recently people doing interesting things when reporting crimes. I think its important to realize that when reporting crime people have a different perception when reporting crime. People will see you in a certain neighborhood and might think they

stole that car, or are doing something bad here. So when we give people the ability to report online we need to be concerned with accessibility about people being able to report freely… and we saw for a year that if an African American person came to use a swimming pool someone can call and say they don't live here. I think SPD is trying alleviate some of those calls they are getting, but I don't think this is the solution to the problem

- What is the logic behind this overall, because is seems like it presents more cons than pros, and what is analytics database you use to look at these reports. Because when I am using government data base I can see where I need more surveillance etc. so we are getting all these open wholes in the system. Is this a right wing Donald trump agenda to watch neighbors of color and surveillance
- I think im more concerned with where does this information end up and how is it used
- What is the usefulness of the information that is not followed up on. And how does it help the people it's actually serving? So for example someone works for an anti-Muslim white supremacy group and they have people in different areas report issues about different Muslim groups in Seattle how do you prove the validity of these information and make sure they aren't just causing harm

2. What value do you think this brings to our city?
    - I think technology saves time, money, makes filing a report easy, I had to do that once it takes a lot of time.
    - I appreciate that it is easier so something like a hit or run or a car breaking in, that's fine.
3. What worries you about how this is used?
    - The only issues I can think of right now is it seems like it would be very easy to make a fraudulent report or a report that is for a small thing that you can make into a big thing, like the things you see go viral on the internet. So now it seems like the barrier to making a police report is smaller
    - I agree I think the bar is lowered and different people are perceived differently. And we have seen how SPD criminalizes different communities for behaviors that don't need to be criminalizing
    - A lot of different kinds of reports have to do with peoples perceived notion, so my concern comes from how do we make sure that this kind of technology isn't used to map our where Muslims live/are, and there types of religious belief. Or isn't being used to monitor them. How do we ensure that this isn't used to map our communities
    - The only comment I have that in the forms I have filled out is it won't allow you to fill out the form if you are naming a specific individual, you can name a group, but a not a person. The following criteria is there no known suspects, it happens in Seattle, so things like thefts. So you can report, graffiti, identity theft, credit card fraud, simple shop lift. So when I click report it says if you have a suspect it says please call. And when I press report it allows me to report anonymously, so I could report against a community with no follow up
        - Well that doesn't stop them from targeting al-Noor masjid, or Safeway in new holly, or new holly gathering hall, and it can target the people in that community. And people don't feel comfortable with increase police presences, so it targets area if not targeting people

- When I was buying the house in Dallas (participant currently still lives/works/plays in Seattle) one of the first things I did was looking at a crime map and based off of that if someone is making a lot of reports can that be used for crime mapping because than that can lower the property value. And if the police isn't following up then how is it being used
- Its definitely possible for people to report inaccurate information

4. What recommendations would you give policy makers at the City about this technology?
    a. But my concern is reporting someone that can really target people of color. And that happens much more threatening to people. So the concept of an upset black women is more intimidating than an upset women that is another race and how many times will behavior like that be reported. Or how many times will a black man be reported against because it seems scary. So I think it lowers the bar when you don't have to talk to an individual when you don't have to talk to a police
    b. My questions are, how accessible are cop logic to people who don't read or speak English. How is SPD going to do what they can to make sure that this doesn't negatively impact communities they are already having issues with like the Sea Tac community that already feels threaten and criminalized by communities.

5. Can you imagine another way to solve the problem this technology solves?
    - So the SPD is very data driven these days and the one thing we repeat is report report report, call 911 and report online whatever you thinking is happening because all of that goes into their data base and is used for them to use resources and put police based off of where there is more crime. The report report report mentality assumes there are good relationships between the community and police, so even if someone doesn't do something bad, I don't know that they would feel comfortable reporting, even if online
    - From the community I have come from I am almost certain that they haven't even used online reporting so how do we make sure that we are giving everyone access to use online reporting. And there are certain crimes that are so common in areas that they don't even report it because they think the police should already know about it
    - I think the department should solely rely on the technology only as a way of collecting info they should still use in personal resources to actively participant in local community and make connections you can't rely only on this technology alone to do this

6. Other comments
    a. Also in this day in age we need to consider that immigration is a issue, and this administrative has blended the different agencies so people have a hard time knowing where SPD starts and ICE starts and those lines have been blurred and that is a real concern for many families

Council on Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington

Thursday, Feb. 21, 2019

Technology Discussed: Binoculars/Spotting Scope

1. Do you have concerns about this specific technology or how it's used?
    . People in our community don't have the access to say or be apart of these conversation. A lot of these people are literate, and might not have the same cultural values. For Muslim women there are a type of consent that you have when you walk outside and are covered in a certain away versus when you are in the privacy of your own home. And people might not have that cultural and religious awareness
    a. I had one quick concerns, as far as the data that is collected using these binoculars, who has access to it
        - Seattle City Light: Information goes into the billing system, which customers can access if they have the automated reader but do not have access to under the current system
    - I know the focus is on binoculars but my mind is on new technologies and when people who are consumers and feel like I am overcharged how do I follow up and get those issues resolved. For systems that are completed based off of technologies how will I know if that data is being altered.
    b.
2. What value do you think this brings to our city?
    . I would just add this is more my general comments I think its good that Seattle city lights is providing notifications to people when this is happening. Are they wearing something visible that show people they are from Seattle city lights? And is there a way for people to complain?
        - Yes they are wearing vests that are very visible. Yes we have a couple different avenues the easiest is to call the customer service line and to submit a complaint there
3. What worries you about how this is used?
    . My primary concerns on my end is if someone is looking into my home with binoculars its a privacy concern. Most Muslim women wear hijab and I don't feel comfortable if someone is using binoculars looking from the outside when we are not wearing the hijab. My concern is that it is a huge invasion of privacy
    a. I have a question as the women expressed the feeling of people reading the meters with binoculars, if the meter has abnormal behavior or is in a different place of the house. Have there been situations where someone sees the person looking at someone house with binoculars, and they might not have gotten notified. Or the meter might be on the opposite side of where they are looking. Are they getting background checks? Or are complaints being followed up

- Seattle City Light: Yes all city employees have background checks, and if a complaint gets called in they will go through disciplinary actions
- What are the average times for disciplinary actions. How long is the process for a full investigation
- Seattle City Light: It's a multiple step process in terms of different levels. There are warnings, and if there was undo actions. Timeline really depends, I'm not sure
- Cause I think that people who go through the different nuances of how privacy can be breach that is just the end all be all of how privacy can breach so I think there needs to be policy put in place so that people don't have their privacy breach and they are being monitored by a pedophile

4. What recommendations would you give policy makers at the City about this technology?
   . When I look at the Seattle city of light they do a lot of estimated guesses and as a consumer they might give you a $500 fee based off of the estimated guesses so I think it is important to have some sort of device that better clearly shows how much you use

5. Can you imagine another way to solve the problem this technology solves?
   . My other question is if its actually not efficient why do you get the option to opt out (of the new automated system). If there is an old school way of doing it that involves a breach of privacy because these are human beings using the binoculars, so If this other option is better why are people having the ability to opt out.
6. Other comments: (Many comments were discussed over Seattle City Light's upcoming change from binocular use to automated meter readers)
   . Who opted out was it home owners?
   a. When we go to a place with 12 tenements do all 12 of them have the ability to opt out or in, or just the owners of the building?
   b. Each home owner has a schedule provided to them and it is a 3 day period which they can come in and look at the system
   c. Is there a cost to them to have the new meter.
      - Seattle City Light: There is no cost with getting the new meter, but there is still a cost If we have to send someone out there to read it
      - What I don't understand is why the new practice is not to just use the new system since that is more accurate and it is doesn't require binoculars
      - What is the cost of opting out
      - Seattle City Light: There is a flat rate
   - I was gonna reiterate when we talk about equity and equitable practices. You can opt out (of the automated system) but there is a fee. And it makes me think

how much of It is a choose if one of these you have to pay for and the other one is free. So that sounds a little problematic when looking at choices of equity. I think choices are great, but also people need to be well informed. Like people within the community need to have more clear information to make the best decision for themselves

- Going back to people who make the decision. I want the person who are living in the house to know what decision is being made. So not just the person who owns the house, but the person living in the home. And not everyone it literate and not everyone speaks English. And its really important that you are giving them information they can actually consume. Instead of giving them notices they cant read

Council on Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington
Thursday, Feb. 21, 2019
Technology Discussed: Acyclica

1. Do you have concerns about this specific technology or how it's used?
    - Where does this data go? Does it go to SDOT? Google maps?
    - My other question is, it said whatever is being transferred is encrypted. All encrypted means to me is getting data from one device to another will be transferred without it being intercepted. What I don't know is, how much information are people getting
    - My concern is related to data, yeah we like to use gps. But what is the perimeter, what is the breach of access. Where is the data being used, and what can that turn into. we might be okay if the data is only being used for traffic related updates, but they might use it for more
    - I also would like to see how acyclica actually does what they do. They are using a lot of words that normally don't know. So I want to know how exactly they are hashing and salting. So for them to be clear about how they doing it. like when whatsapp encrypted they didn't give us the exact code but told us how they are doing it
    - Asking for a greater transparency for how they are doing this
    - I think the purpose of it is really important but the biggest concern is collecting all of this information without consent of passersby.
    - So the specific identifier that acyclica uses it mac addresses? You could potentially use that number to track that phone for the lifetime of the phone, for as long as that phone is on and being used. And that is very concerning.
    - Also I want to understand more where is this data going, and I want to know if this data is going to be used for future projects.
    - I want to ask is this something people opt into
    - People don't even know this is being used

2. What value do you think this brings to our city?
    - I like getting places and I like getting traffic information.
3. What worries you about how this is used?
    - What I don't like is you using my phone to get that information. I want whatever is in my cellphone to be protected. And I wanna know what you can access
    - I think based on Seattle and Seatac's higher up wanting to monitor and map out Muslims and where they are, and I don't like people being able to use our phone to track our location or actions they might think is violent. So based off of Seattle's track record and law enforcement agencies I don't like it
    - People who live outside of Seattle are also being impacted by it anytime they drive in Seattle
    - Could someone "opt out" by having wifi disabled on their device? I don't know if this covers cell towers. Because if it covers cell towers the only thing you could is having your phone on airplane mode

4. What recommendations would you give policy makers at the City about this technology?
    - I think the big question is why aren't we using other vendors, like I mentioned google maps, or waze, in fact komo 4 uses ways. Where other options we're looked at, and what were the trade off there's. And I want to see some transparency between the decision-making processes
    - I don't think this data should be shared with other private agencies, or other interagency programs
    - If all you're looking at is traffic flow, why are you not using the sensors in the road to give traffic flow updates.
    -
5. Can you imagine another way to solve the problem this technology solves?
    - I don't know if this already exists but something that makes it that data can't be used from one technology and use it for a different purposes
    - I think speaking from an industry perspective that is really important to have a processes for. Because all of this data is being used regardless of if you live in Seattle, or people live in different countries even who are visiting. That data is being collected. My understanding is that SDOT doesn't get the data directly. So my concern is how long can acyclica keep this data, use this data. Why wasn't a different option used, one in which some sort of consent can be used, so something like waze, google maps where people can opt in can get that information.
    - Road sensors or ways to count cars
    - I think its better to count cars than phones, because there is some expectation that your car will be monitored.
    - Using vehicle level granularity

Entre Hermanos

Please select which technology you wish to comment on:

☐SCL: Binoculars	☐SCL: Sensorlink Transformer Meter (TMS)	☐SFD: Computer-Aided Dispatch	☐SPD:9-11 Call Recorder
☐SCL: Sensorlink Ampstik	☒SDOT: Acyclica	☐SPD: Computer-Aided Dispatch	☐SPD: CopLogic

1) What concerns, if any, do you have about the use of this technology?

El uso de wifi en Acyclica porque pueden obtener toda la información de los teléfonos.

Si vale la pena la inversión

Enfocando al grupo: La tecnología ya está instalada. que les preocupa de su uso?

El tráfico sigue igual.

Quien usa o almacena la información.

La preocupación es la colección de data.

Colección y almacenamiento de información es la mayor preocupación.

No es la colección de data lo alarmante sino los recursos (dinero utilizado) ya que o la tecnología no están funcionando porque el tráfico sigue igual. No hay cambio con la nueva tecnología, esos gastos no son válidos ya que no hay resultados. Esos gastos pudieran ser utilizados para la comunidad.

También tienen que ver si la tecnología emite radiación o alguna otra cosa dañina; perjudicial a la salud.

El gobierno tiene todos los datos.

No necesitan esta tecnología para tener los datos porque ya existen métodos para eso, incluso aplicaciones o alguna otra cosa.

La otra preocupación del grupo es que no haya un cambio al problema que se quiere resolver. En el caso de Acrylica sería el mejorar el tráfico.

- Tecnologías como esta necesitan recolectar más opiniones de expertos.
- Sería bueno que la información sea compartida con la comunidad. (Transparencia en fines y objetivos de la tecnología y datos guardados, tácticas implementadas.)

2) What do you want City leadership to consider about the use of this technology?

Hay lugares donde no se necesitan. En algunas partes de Magnolia, Queen Anne, Northgate, no se ocupan.

Seguimiento de pregunta: En las comunidades donde viven los latinos que tanto se ocupa Acyclica?

Participante no cree que allí se ocupan.

Hablaron sobre la necesitad de puntos estratégicos y calles con más necesidad de ayuda por causa del tráfico.

What do you think about this technology in particular ?

Bien, la tecnología ayuda con la velocidad o el movimiento de los coches.

La información se guarda y analizan por donde viajas o cuantas veces cruzas este rastreo.

Si es solo para ver el tráfico está bien.

Está bien en algunas partes. Puede que sea algo bueno. Pero puede que esta tecnología pueda compartir información personal que puede ser utilizada de otra forma en especial si hay Hacking (forma negativa, uso de datos).

La tecnología en sí no es tan grande (de tamaño) para ser algo visualmente desagradable. La información captada a través de estos medios puede que ayude a conducir el tráfico de mejor manera pero también puede que tome información personal.

Are there any questions you have, or areas you would like more clarification? ●

La tecnología no es un router, sino colección de data para planeaciones urbanas.

Participante: “quiero creer” “convencerme” que los sensores están allí para ayudar con el tráfico.

No se sabe cuándo las instalaron, los resultados deberían de ser públicos. Si la tecnología es para aliviar el flujo de tráfico entonces por qué no extienden el programa? O por qué no hay mejoramiento del tráfico?

Alternatives to this technology

- Alguna pantalla que indique cuáles vías son alternativas puede reemplazar esto.
- Cambios al límite de velocidad puede que alivie el flujo del tráfico.
- Dejar de construir tanto.
- Rediseño de calles ayudaría flujo de tráfico.
- El rediseñar las vías servirá para las futuras generaciones.

City of Seattle

Entre Hermanos

Please select which technology you wish to comment on:

☒SCL: Binoculars	☒SCL: Sensorlink Transformer Meter (TMS)	☐SFD: Computer-Aided Dispatch	☐SPD:9-11 Call Recorder
☐SCL: Sensorlink Ampstik	☐SDOT: Acyclica	☐SPD: Computer-Aided Dispatch	☐SPD: CopLogic

1) What concerns, if any, do you have about the use of this technology?

Los binoculares son preocupantes si la persona no tiene ética. Es preocupante que una persona vea a través de binoculares a que una tecnología mida el uso de la electricidad

Al grupo le incomoda el uso de binoculares

Sensorlynk específicamente la preocupación sería que le quita el trabajo a una persona.

Si es para detectar robo el grupo cree que hay otras maneras de saber quien roba

que no tan solo será para leer la electricidad sino para obtener otros tipos de información si cámaras fueran usadas

2) What value, if any, do you see in the use of this technology?

Ahorro de energía

Record y datos mas precisos

Oportunidad de trabajo a quien utiliza los binoculares

Estabiliza los precios de la electricidad

3) What do you want City leadership to consider about the use of this technology?

: Usar background check, uso de uniforme por trabajadores, cámara en binoculares.

What do you think about this technology in particular ?

Sensorlink Si

Binoculares son invasivos

Are there any questions you have, or areas you would like more clarification? ●

La confianza en estos medidores serán confiables? Serán efectivos?

El uso de binoculares se puede acompañar de una cámara añadida

Alternatives to this technology

Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad

City of Seattle

Entre Hermanos

Please select which technology you wish to comment on:

☐SCL: Binoculars ☐SCL: Sensorlink Transformer Meter (TMS) ☐SFD: Computer-Aided Dispatch ☐SPD:9-11 Call Recorder

☐SCL: Sensorlink Ampstik ☐SDOT: Acyclica ☐SPD: Computer-Aided Dispatch ☒SPD: CopLogic

1) What concerns, if any, do you have about the use of this technology?

Las fallas electrónicas son preocupantes especialmente en reportes policiacos.

Las preocupaciones es que el reporte no salió, no llegó por cualquier razón.

No todos podrán o saben usar las computadoras.

Fallas de los algoritmos de cada demanda es alarmante.

Que y cuando determina la urgencia de respuesta

Las personas le temen a los policías. Y este medio puede ayudar a que el miedo disminuya.

La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

2) What value, if any, do you see in the use of this technology?

La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

El uso de computadora está bien para las denuncias.

Si personas usan esta tecnología y es analizada en tiempo real por otras personas no hay problema.

Es otro método para denunciar

Está de acuerdo con el uso de computadoras para denunciar solo que no todos son capaz de usar este método/tecnología.

3) What do you want City leadership to consider about the use of this technology?
Que sea multi-idioma, implementar audio, implementar sistemas que ayuden a múltiples personas con diversas capacidades/necesidades

Si es usada de manera adecuada y como han dicho está bien.

El uso de la tecnología es bueno para dar respuesta para todas las cosas y personas

What do you think about this technology in particular ?

Grupo están de acuerdo con su uso.

Puede salvar una vida.

Los riesgos y acciones determinan la urgencia de la intermisión policiaca.

Alguna gente se siente más capaz de presentar una queja a través de este sistema, la tecnología en uso tiene validez.

Bueno para la violencia doméstica.

Are there any questions you have, or areas you would like more clarification?

La computadora decidirá la importancia/urgencia del reporte/emergencia dando a llevar acciones de emergencia.

Gravedad de emergencia es determina por tecnología.

La definición de emergencia es diferente con cada persona.

Cada uno tiene la definición de vigilancia, pero ¿que tal la definición de emergencia?

SITUATIONS TO APPLY ITS USE

Una pelea en la calle, un malestar corporal, cuestiones de vida, abuso doméstico

Si nos basamos en la definición de emergencia sólo en cuanto estemos en peligro inmediato o en tiempos mínimos/ de transcurrencia alarmante/peligrosa el uso de será implementado o limitado solo a instantes inmediatos de peligro.

Para reportar algo que ya sucedió o que son recurrentes.

Basado en el concepto de emergencia, las personas pueden tomar el método adecuado para reportar su caso y a través del medio necesario.

Los reportes no son anónimos.

Los datos son recolectados aun, a pesar de la opción escogida.

Alternatives to this technology

Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad

Entre Hermanos

City of Seattle
Surveillance

Inicio

Resumen: El departamento de vecindarios quiere saber la opinión de este grupo. Ellos verán videos de un minuto y medio y encontrarán folletos en sus mesas donde encontraran más información sobre lo visto.

Demográficos:

Ocho personas participaron, una de West Seattle, una de First Hill, dos de Ravenna/Laurelhurst y cuatro de King County (outside Seattle).

Cuatro personas se consideraron hispano o latino, una como india americana o nativa de Alaska, y tres no opinaron.

Cinco personas marcaron 18-44 como su rango de edad, dos marcaron 45-64 como el suyo y una no opinó.

Cinco personas marcaron masculino como género, una como transgénero, una como femenino, y otra no opinó.

Otra Información Importante:

- Preguntas serán hechas.
- Habrá una hoja para poder conversar sobre videos de interés
- Se les agradeció por venir.
- El concepto de vigilancia será manejado como la ciudad de Seattle lo maneja.
- Tom: Agradeció a los invitados por venir

Surveillance. In 2017 city council passed an ordinance to see what technology fit the definition of surveillance. The information gathered by these surveillance technologies are as follows: to “observe or analyze the movements, behaviors, or actions of identifiable individuals in a manner” which "is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice.”

Presentador: Preguntó si la conversación en inglés fue entendida.

Grupo: Concordó.

Tom: Do not let information on videos stop you from making comments or raising questions.

Presentador: Dio a entender el concepto de vigilancia como ha sido interpretada por la ciudad de Seattle. Fue analizada de esta manera: “La vigilancia es definida como tecnologías que observan o analizan los movimientos, comportamientos, o acciones de individuales identificables de una manera que razonablemente levanta inquietudes sobre libertades civiles, la libertad de expresión o asociación, igualdad racial o justicia social.”

- Los movimientos de la gente son observados a través de esta tecnología y puede que para algunas personas esto sea incómodo.
- Las cámaras de policía no califican como tecnologías de vigilancia en este tema.
- La presentación mostrada en la pantalla a través de los videos será transmitida en inglés.
- Se pidió que todos se traten con respeto y que opinen y que su nombre sea mencionado e incluso la vecindad donde viven.

El Grupo

Participante vino porque quiere obtener más información y dar su opinión. Es de Seattle.

Participante viene de Shoreline/Seattle para ver cuánto la tecnología entra afecta

Participante vino porque quiere saber qué información es colectada por el gobierno y para qué usan esa información. Puede que la información obtenida a través de la tecnología sea usada para perseguir a personas de color/minorías/personas marginadas.

Participante vino de First Hill, porque quiere ver el punto de vista de la ciudad y ver que opiniones surgirán.

Participante viene de Seatac porque tiene interés en el tema y porque la seguridad es importante y quiere saber a dónde llega la información.

Participante vine en Ravenna/Northgate, quiere ver que tan confiable es la tecnología y para qué es utilizada. Perjudicial o beneficial?

Participante vine en Seatac y vino porque es un tema muy interesante ya que se tiene que saber/mantener informado de lo que hacen los gobernantes.

Participante vino de Burien por la importancia del tema y la privacidad.

Presentador: La tecnología no es nueva. Ya está siendo usada. Y quieren saber el formato para que las futuras tecnologías tengan.

El video de Seattle Department of Transportation de Acyclica fue mostrado

Esta tecnología es un sensor que detecta el wifi. Es un sensor que detecta la tecnología wifi.

Seattle Metering Tool fue mostrada

Nadie del grupo sabe del tema más el presentador no hablará a fondo de esto para no influenciar opiniones.

Video de Fire Department's Computer Aided Dispatch fue mostrado

El 9-1-1 logging recorder video fue mostrado

Aclaración: Información impresa fue entregada explicando cada una de las tecnologías.

Video de Coplogic fue mostrado

El grupo no conocía que se puede reportar a la policía a través de su página/en línea.

El video de Seattle Police Computer Aided Dispatch fue mostrado

Esta tecnología es similar a la de los bomberos.

Se preguntó cuál video era de interés para analizar

Se acordó el análisis de Acyclica, Binoculares/Sensorlink, y Coplogic

Las Preguntas que sea harán serán las siguientes:

¿Qué piensan de este sistema de tecnología en específico y el motivo de usarla?
¿Cuál creen que sea el aporte de esta tecnología a la cuidad?
¿Qué preocupación les causa el uso que se le dará a este sistema?
¿Qué recomendarían a el grupo de políticos de la cuidad responsables de tomar las decisiones de implementar estas tecnologías?
¿Qué otra manera habría de resolver el problema que esta tecnología esta designada a resolver?

La Acyclica

Pregunta: ¿Qué piensan de este sistema de tecnología en específico y el motivo de usarla? (Como se usa y cuál es el uso)

- Bien, la tecnología ayuda con la velocidad o el movimiento de los coches.
- La información se guarda y analizan por donde viajas o cuantas veces cruzas este rastreo.
- Si es solo para ver el tráfico está bien.

- Está bien en algunas partes. Puede que sea algo bueno. Pero puede que esta tecnología pueda compartir información personal que puede ser utilizada de otra forma en especial si hay Hacking (forma negativa, uso de datos).

- La tecnología en sí no es tan grande (de tamaño) para ser algo visualmente desagradable. La información captada a través de estos medios puede que ayude a conducir el tráfico de mejor manera pero también puede que tome información personal.

Pregunta: Qué es lo que aporta esta tecnología a la ciudad?

- Seria algo bueno el aporte por la agilidad del tráfico solo si la tecnología está sincronizada con los semáforos, de otra manera no es útil si no aporta para el mejoramiento del tráfico.

- Participante dice que hay alternativas para esquivar el tráfico.

- Participante opina que la tecnología es interesante ya que usa google maps y está de acuerdo con el mejoramiento del tráfico.

- Si el objetivo es de mejorar el tráfico está de acuerdo. Pero también quiere saber en qué lugar(es) estarán los aparatos, si algunas personas serán beneficiadas más que otras.

Pregunta: Qué preocupaciones tienen con posible uso/uso potencial de esta tecnología?

- Le preocupa el uso de wifi en Acyclica porque pueden obtener toda la información de los teléfonos.

- Si el potencial puede ser aplicada a la inversión.

Enfocando al grupo: La tecnología ya está instalada, que les preocupa de su uso?

- El tráfico sigue igual.

- Quien usa o almacena la información.

- La preocupación es la colección de data.

Más de la mitad de grupo opina que esa (el almacén y colección de información) es la preocupación.

- Participante no está de acuerdo. No es la colección de data lo alarmante sino los recursos (dinero utilizado) ya que o la tecnología no están funcionando porque el tráfico sigue igual. No hay cambio con la nueva tecnología, esos gastos no son válidos ya que no hay resultados. Esos gastos pudieran ser utilizados para la comunidad.

- También tienen que ver si la tecnología emite radiación o alguna otra cosa dañina; perjudicial a la salud.

- El gobierno tiene todos los datos.

- Opinión de otro participante: No necesitan esta tecnología para tener los datos porque ya existen métodos para eso, incluso aplicaciones o alguna otra cosa.

La otra preocupación del grupo es que no haya un cambio al problema que se quiere resolver. En el caso de Acrylica sería el mejorar el tráfico.

- Tecnologías como esta necesitan recolectar más opiniones de expertos.

- Sería bueno que la información sea compartida con la comunidad. (Transparencia en fines y objetivos de la tecnología y datos guardados, tácticas implementadas.)

Pregunta: Le dirían algo a los políticos algo del lugar donde se encuentran estos aparatos?

- Hay lugares donde no se necesitan. En algunas partes de Magnolia, Queen Anne, Northgate, no se ocupan.

Seguimiento de pregunta: En las comunidades donde viven los latinos que tanto se ocupa Acyclica?

- Participante no cree que allí se ocupan.

Hablaron sobre la necesitad de puntos estratégicos y calles con más necesidad de ayuda por causa del tráfico.

Presentrador: Crees que Acylica es como el router de google?

- La tecnología no es un router, sino colección de data para planeaciones urbanas.

- Participante: “quiero creer” “convencerme” que los sensores están allí para ayudar con el tráfico.

- No se sabe cuándo las instalaron, los resultados deberían de ser públicos. Si la tecnología es para aliviar el flujo de tráfico entonces por qué no extienden el programa? O por qué no hay mejoramiento del tráfico?

Otra pregunta: Alguna otra tecnología que pueda ser utilizada en vez de Acyclica?

Alternativas:

- Alguna pantalla que indique cuáles vías son alternativas puede reemplazar esto.
- Cambios al límite de velocidad puede que alivie el flujo del tráfico.
- Dejar de construir tanto.
- Rediseño de calles ayudaría flujo de tráfico.
- El rediseñar las vías servirá para las futuras generaciones.

Tecnologia #2

Sensorlink/Binoculares

Pregunta: Que opina el grupo de la tecnología?

- Los binoculares son preocupantes si la persona no tiene ética. Es preocupante que una persona vea a través de binoculares a que una tecnología mida el uso de la electricidad.

- Un sensor que detecta la electricidad sería mejor.

- Al grupo le incomoda el uso de binoculares.

Pregunta: Qué opinas sobre la tecnología medidora de electricidad (sensorlink) y que sea usada en tu casa?

- No le incomoda o afecta a dos participantes.

- La preocupación sería que le quita el trabajo a una persona.

- Los binoculares son invasivos.

- Para que usar binoculares si es que se puede llegar a el hogar y ver el medidor en persona, pidiendo permiso? Si la tecnología es usa para ver que las personas se roban la electricidad, creen que no saben quiénes roban?

- El grupo cree que si saben.

Pregunta: Cual creen que sea el aporte que esta tecnología?

- El video dice que 3 millones de dólares son ahorrados.

Pregunta: De qué manera beneficia esto a la cuidad/ciudadanos/comunidad?

- El robo de la luz es preocupante.

- Si ya llevan el record y datos y le hacen saber a la comunidad puede que ahorren dinero.

- Uso de binoculares puede dar trabajo a una persona y dinero puede ser ahorrado con esta tecnología.

- La tecnología trae gasto de electricidad para poder ver gastos de luz? Si pretende evitar el robo entonces los gastos de la factura eléctrica deberían de seguir estables.

Pregunta: La confianza en estos medidores serán confiables? Serán efectivos?

- Ayuda a la precisión, a bajar precios.

- Que quiten los binoculares sería una sugerencia, o usar binoculares que graban con video.

- Si ya tienen récord sobre la energía (consumo, gastos, etc.), el robo de energía no es suficiente para establecer este tipo de tecnología ya que puede ser identificado el robo o alguna otra anomalía dependiendo en el nivel alto o bajo o repentino analizado/visto/detectado por métodos convencionales ya establecidos.

- Otra recomendación: Usar background check, uso de uniforme por trabajadores, cámara en binoculares.

- Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad

- .La preocupación es que no tan solo será para leer la electricidad sino para obtener otros tipos de información si cámaras fueran usadas.

Tecnologia #3 Coplogic

- Esta tecnología no solo el ahorro de tiempo, sino el ahorro de tiempo policial ya que ellos trabajarían en otras cosas

- El uso de computadora está bien para las denuncias.

- Si personas usan esta tecnología y es analizada en tiempo real por otras personas no hay problema.

Enfoque: Lo que estamos queriendo dialogar es el uso del internet y las denuncias.

- Es otro método para denunciar

- Está de acuerdo con el uso de computadoras para denunciar solo que no todos son capaz de usar este método/tecnología.

Pregunta: En que ayuda a la comunidad?

- Por qué usar estos métodos?
- Grupo están de acuerdo con su uso.
- Puede salvar una vida.
- Los riesgos y acciones determinan la urgencia de la intermisión policiaca.
- Alguna gente se siente más capaz de acudir a través de este sistema la tecnología en uso tiene validez.
- Bueno para la violencia doméstica.
- Las fallas electrónicas son preocupantes especialmente en reportes policiacos.
- Las preocupaciones es que el reporte no salió, no llegó por cualquier razón.
- No todos podrán o saben usar las computadoras.
- Fallas de los algoritmos o cuando o que promueve urgencia de cada demanda es alarmante.
- Criterio de demandas y que clase de preocupación de parámetros son confiables tienen que ser cuestionados/analizados, y que/quien es digno de prioridad o importancia o de ayuda.

Pregunta: De qué manera este uso beneficiaria a la comunidad?

- Personas pueden ser discriminadas
- Las personas le temen a los policías. Y este medio puede ayudar a que el miedo disminuya.
- La computadora decidirá la importancia/urgencia del reporte/emergencia dando a llevar acciones de emergencia.
- Gravedad de emergencia determina uso de tecnología.

Pregunta: Alguna inquietud sobre el uso de esta tecnología?

- La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

Pregunta: En qué situación usarán esta tecnología?

- Una pelea en la calle, un malestar corporal, cuestiones de vida, abuso doméstico
- Cada uno tiene la definición de vigilancia, pero que tal la definición de emergencia?
- La definición de emergencia es diferente con cada persona.
- Si nos basamos en la definición de emergencia sólo en cuanto estemos en peligro inmediato o en tiempos mínimos/ de transcurrencia alarmante/peligrosa el uso de será implementado o limitado solo a instantes inmediatos de peligro

Pregunta: Para qué sirve el reporte de la computadora?

- Para reportar algo que ya sucedió o que son recurrentes.
- Basado en el concepto de emergencia, las personas pueden tomar el método adecuado para reportar su caso y a través del medio necesario.
- Los reportes no son anónimos.
- Los datos son recolectados aun, a pesar de la opción escogida.

Pregunta: Qué les recomendarían a los políticos?

- Que sea multi-idioma, implementar audio, implementar sistemas que ayuden a múltiples personas con diversas capacidades/necesidades

Pregunta: Algún otro comentario en general sobre la tecnología de vigilancia?

- Si es usada de manera adecuada y como han dicho está bien.

- El uso de la tecnología es bueno para dar respuesta para todas las cosas y personas.

Consejo:

- Den información más información sobre lo que están haciendo. (transparencia/divulgación de información)

- Que haya más transparencia.

Ser transparentes sobre la colección de datos, para que haya discusiones y decisiones Informadas, en todas las tecnologías implementadas/por implementar.

City of Seattle

Byrd Barr Place

2/28/2019 Surveillance Technology Focus Group

Thursday, February 28, 2019
1:42 PM

Disclaimer: some of these notes are written in first-person. These should not be considered direct quotes

Videos:

- Acyclica: sensors recognize when a wifi enabled device is in range of it. Attached to street lights
- 911 recorder: records the conversation with the person calling 911, and conversation with the dispatched officers
- CopLogic: Online police report, treated as a regular policy report
- Computer Aided Dispatch
- Seattle City Light: Binoculars for meter readers; sensor to see if someone is stealing electricity

Tom: Read definition of surveillance

Craig: invasion of privacy?

- Electric one: I never even know they had the sensor one.

Community Member: used to be in the tech industry for thirty years. Writing a book about surveillance and technology
Wanda: I like the online police report. If someone is experiencing a crisis or trauma, you can go ahead and report it.

- Surveillance, I understand the concern, but overall I think it's a good thing. There is good and bad in any location, you'll find people who are taking advantage of it, but hopefully there are systems in place.
- Used to work nights, and catching the bus at night is scary. Having the cameras and police out when catching the bus helps, I appreciate that. No one likes to be watched, but if it's gonna keep people safe, that's a good thing.

Mercy: security is a great safety issue
Craig: there are some parts of the neighborhood/city that need to be watched, and some that need to be left alone
Wanda: as long as it's even
Craig: Sometimes it's not even
Both: There are hot spots though

Which of the surveillance technologies do you think could be abused to pinpoint specific communities?

IG: The Computer Aided Dispatch

Talking about the International District:

- Lots of businesses and residential crammed together in a larger space
- Talking about a great community member who died; if they had surveillance technology them, maybe they would have found his killer

"Some neighborhoods need to be watched"

- Gangs; drug use

Tom: getting back to CAD, how do we feel about the information that is stored

- Craig: there are concerns, but who is allowed to see it, how is it stored? That's a concern
    - Is it used for BOLOs? Is it everyone who is in the area, all of the police officers? Or is there some discretion as to which police officers would be given the information?
- Wanda: plenty of people are arrested who "fit a description"
    - Discussion about the racial discrimination: how people who think that "all [insert race here] look alike".
    - Individuals may think like that, but police officers have the capability to ruin someone's life.
- Marjorie: just recently got a smart phone, and it's new to me that someone could know where I'm going and I wouldn't be aware of it
    - Without my consent.
- Mercy: grew up with the idea that big brother is watching you
    - Tracking how many times I go to the library seems like a waste of money
    - People who are not law abiding citizens, they are the ones to be worried
- Craig: What about selling weed, coke, etc. Should they be worried?
    - Mercy: well at least in Seattle, it's ok to sell
- Mercy: big brother is watching. We already know that, it's just more obvious now
- There is a lot of technology that we are not made aware of

Tom: So acyclica, is it worth it? Some people worried it's tracking, is it something that we can live without?

- Should we put up signs that this road is tracked?
    - Viron: Maybe
    - Mercy: let people out there know that you're on camera.
    - Viron: does it work if your device is not turned on?

Tom: what do you want to tell the city council about tech that is collecting personal information?

- Wanda: they should get our individual consent
- Martha: putting it on the ballot doesn't mean that you are getting individual consent, because if you vote no but it still passes, you didn't give your consent
- Deana: there are some places around Capitol Hill that I don't feel safe at at night
    - Talking about fire department responding to a fire in her building: when one building alarm system goes off, it goes directly to the fire department - affects multiple buildings.
        - Response time is very good.
    - I choose to turn off the GPS tracking, because I don't need people to know where I'm at
        - If others are watching where I'm at, that's an invasion of privacy. I should be able to walk out my front door and go wherever I want without anyone knowing.
- Location privacy: you can tell a lot about a person based on where they go, and tracking that can build a pretty extensive profile of who you are

- IG: now that I know they are tracking, I will turn it off.

Mr. Surveillance: Surveillance is always secret, and it's an aggressive act. It's meant to exert power over others.

Do you think any individual could raise enough concern that it would change anything?

- Resounding no
- Maybe with a larger group
    - Maybe with the whole city

SCL binoculars:

- Craig: they should warn their customers and let them know they are coming into their yard/looking through binoculars.
- Wanda: as long as they aren't looking in people's windows.
    - When we're walking down the street, it's a little different. Certain neighborhoods do need more surveillance than others

Regarding being watched in public:

- Eydie: in public, it depends on how long. If it's a short period of time, that's one thing, but if you're tracked the whole time you're out, it's unreasonable.
    - I don't know what the solutions would be.
    - Even when the meter read just walks into your yard, it's unnerving.
    - What's the purpose of tracking it this way?
- Mercy: (referring to the acyclica) Why are they doing it all the time? Have they not gotten the information yet?
    - They should already know what the traffic flow would be.
    - We lost a lane to the bicyclist
- Craig: facial recognition used on the street is bad.
- Vyron: sometimes you can't walk down the street and shake someone's hand without getting in trouble
- Mr. Surveillance: The technology has gotten ahead of the law, and it means they have to pay less people

Tom: Are we willing to accept more technology to have less police?

- Craig: how about just making it even? Police have an image to people of color; they are afraid of why they are going to be there. We can police ourselves
- Wanda: I disagree. There are some who think there should be less, but there are also a lot of people who worry about walking down the street
    - As a woman and DV survivor, I appreciate the police and appreciate living in a country where I can call a number for help.
    - I have a big problem with the shooting of unarmed black men, but as an individual I still appreciate the police.
    - But I have a problem being tracked, and I have a problem being watched in my home.

- General comment: The number of police being on the corner is a touchy situation
    - Knowing the police that are on your corner makes a difference. They can police the community better if there is more of a relationship between the two.
- Craig: it has to be both, even. You can't trade off the technology for the police.
- Mr. Surveillance: The trend is they want to go to more technology and less police.

Tom: If right now we have lots of technology, and we want a balance, then how do we do that?

- Craig: keep it the way it is but clean up the police department. Make sure the people who are working there are good at their jobs, not biased or discriminating

CopLogic: making police reports online

- Craig: I think it's stupid.
    - Would use that technology for stupid crimes
- Mercy: you could report your neighbor for silly things
    - Anonymous reporting of crimes that could target people for things they might not call 911 for
- Wanda: there were some lines of traffic where I saw cars lined up with their windows smashed in; nothing taken, but glass all over the place.
    - Police response when called: maybe you should get a cheaper type of car
    - Would he have said that to us if we were a different skin color, or lived in a different neighborhood?
- IG: I think it's a bad thing: someone could make up a story and the officer didn’t have to check it.
- Marjorie: I think the online reporting could be abused

Appendix E: All Comments Received from Members of the Public

ID: 10617592348
Submitted Through: Survey Monkey
Date: 3/25/2019 12:51:06 PM
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Sensorlink Check Meter Device
What concerns, if any, do you have about the use of this technology?
Medium Concern: The draft SIR says that the data is retrieved from the device "via secure radio protocol", but the SIR never explains that in more detail. Radio frequencies are not inherently secure, so the SIR should specify how this communication channel is supposedly secured so as to prevent other (knowledgeable) passerby from retrieving the data. Other Concerns: Originally, one of my other concerns was that the Check Meter Device (aka SensorLink Transformer Meter System (TMS)) would collect more types of data and at a finer granularity of occurrence than what the normal functioning household meter would collect. However, the SCL staff at the SIR tech fair said it collects the same kinds of data as a normal meter, just that it's located upstream, thus addressing my concerns on that. With that in mind, most of my concerns are alleviated (aside from the radio protocol details) by the fact that the CDT crew is small ("five journey-level engineers"), the "CDT owns six SensorLink TMS units", that the "CDT only investigates specific, metered locations previously identified and properly documented as sites of suspected current diversion", and that mis-use/abuse of this technology would likely not be compliant with IBEW Local 77 & Energy Northwest's "Code of Excellence Program" (http://www.ibew77.com/Letter%20of%20Agreement%20IBEW%20Code%20of%20Excellence%20Energy%20NW.pdf). Additionally, even with those items in mind, SCL might be using the TMS devices and enforcement mechanisms at location/for households disproportionately based on race or other minority characteristics. To that end, I was happy to see in the SIR that "City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible." Hopefully, there are sufficient other programs/discounts for low-income individuals such that people never feel the need to resort to manipulating their electrical system (but I'm not familiar enough with SCL's offerings for low-income individuals, nor have I been low-income while living in Seattle, so I can't make that claim with 100% certainty).
What value, if any, do you see in the use of this technology?
There is a direct monetary cost to current diversion, thus identifying it and recouping the costs helps the city save money.
What do you want City leadership to consider about the use of this technology?
City leadership should ask to review SCL's "equity analysis of past enforcement locations". Additionally, (if not included in said analysis) City leadership should specifically inquire as to what percentage of people/households that were enforcement locations would also be considered low-income. If that percentage is high, then that likely means SCL may cause people to be jailed for effectively being poor (and resourceful); and SCL may have inadequate support offerings for people who are low-income.
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

City of Seattle

ID: 10617585382
Submitted Through: Survey Monkey
Date: 3/25/2019 12:48:12 PM
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars / Spotting Scope
What concerns, if any, do you have about the use of this technology?
My concerns are largely alleviated by the fact that the "binoculars are standard, commercial-grade, unpowered binoculars...[without] any special enhancements requiring power (e.g., night-vision or video-recording capabilities)", the CDT crew is small ("five journey-level engineers"), the binoculars are used "for approximately one minute at a time in those cases where an initial investigation has been authorized by the Current Diversion Coordinator", they're only used " to read a meter from a distance when the CDT is otherwise unable to access physically the meter for the purpose of inspection upon suspected current diversion", and that mis-use/abuse of this technology would likely not be compliant with IBEW Local 77 & Energy Northwest's "Code of Excellence Program" (http://www.ibew77.com/Letter%20of%20Agreement%20IBEW%20Code%20of%20Excellence%20Energy%20NW.pdf). Additionally, even with those items in mind, SCL might be using the binoculars and enforcement mechanisms at location/for households disproportionately based on race or other minority characteristics. To that end, I was happy to see in the SIR that "City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible." All things considered then, I'm hopeful that SCL is on the right track. Hopefully, there are sufficient other programs/discounts for low-income individuals such that people never feel the need to resort to manipulating their electrical system (but I'm not familiar enough with SCL's offerings for low-income individuals, nor have I been low-income while living in Seattle, so I can't make that claim with 100% certainty).
What value, if any, do you see in the use of this technology?
There is a direct monetary cost to current diversion, thus identifying it and recouping the costs helps the city save money.
What do you want City leadership to consider about the use of this technology?
City leadership should ask to review SCL's "equity analysis of past enforcement locations". Additionally, (if not included in said analysis) City leadership should specifically inquire as to what percentage of people/households that were enforcement locations would also be considered low-income. If that percentage is high, then that likely means SCL may cause people to be jailed for effectively being poor (and resourceful); and SCL may have inadequate support offerings for people who are low-income.
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

City of Seattle

ID: 10617574681
Submitted Through: Survey Monkey
Date: 3/25/2019 12:45:12 PM
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Ampstick
What concerns, if any, do you have about the use of this technology?
My concerns are largely alleviated by the fact that there's only 4 Ampstick devices, "they are deployed by hand for approximately ten minutes at a time, only when suspected diversion cases occur", and can only measure one 'line' at a time. Additionally, even with those items in mind, SCL might be using the Ampsticks and enforcement mechanisms at location/for households disproportionately based on race or other minority characteristics. To that end, I was happy to see in the SIR that "City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible." All things considered then, I'm hopeful that SCL is on the right track. Hopefully, there are sufficient other programs/discounts for low-income individuals such that people never feel the need to resort to manipulating their electrical system (but I'm not familiar enough with SCL's offerings for low-income individuals, nor have I been low-income while living in Seattle, so I can't make that claim with 100% certainty).
What value, if any, do you see in the use of this technology?
There is a direct monetary cost to current diversion, thus identifying it and recouping the costs helps the city save money.
What do you want City leadership to consider about the use of this technology?
City leadership should ask to review SCL's "equity analysis of past enforcement locations". Additionally, (if not included in said analysis) City leadership should specifically inquire as to what percentage of people/households that were enforcement locations would also be considered low-income. If that percentage is high, then that likely means SCL may cause people to be jailed for effectively being poor (and resourceful); and SCL may have inadequate support offerings for people who are low-income.
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

ID: 10617441686
Submitted Through: Survey Monkey
Date: 3/25/2019 11:51:11 AM
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars / Spotting Scope
What concerns, if any, do you have about the use of this technology?
none
What value, if any, do you see in the use of this technology?
It's a good way to spot problems and get readings.
What do you want City leadership to consider about the use of this technology?
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

ID: 10600927069
Submitted Through: Survey Monkey
Date: 3/18/2019
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars
What concerns, if any, do you have about the use of this technology?
What a joke. The city has spent millions of dollars converting to digital meters that automatically report usage. Nobody needs binoculars to read them!
What value, if any, do you see in the use of this technology?
Zero
What do you want City leadership to consider about the use of this technology?
Forget it.
Do you have any other comments?
No
Are there any questions you have, or areas you would like clarification?

ID: 10
Submitted Through: Focus Group
Date: 2/28/2019
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars
What concerns, if any, do you have about the use of this technology?
the use of the binoculars can be an invasion of privacy. Period of three days is too vast a window to give note. The lack of knowledge in different standards of privacy by different tenants
What value, if any, do you see in the use of this technology?
What do you want City leadership to consider about the use of this technology?
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

ID: 9
Submitted Through: Focus Group
Date: 2/28/2019
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars
What concerns, if any, do you have about the use of this technology?
ensure that all tenants are aware of the use of binoculars
What value, if any, do you see in the use of this technology?
none. It honestly appears outdated especially with automatic meters being available
What do you want City leadership to consider about the use of this technology?
I would recommend phasing it out completely. If not, ensure that all tenants know that this decision is being made for them.
Do you have any other comments?
I would not assume that all consumers are literate. Have other ways to communicate with individuals such as phone call, news outlets
Are there any questions you have, or areas you would like clarification?

ID: 3
Submitted Through: Focus Group
Date: 2/27/2019
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars, SCL: CheckMeter, SCL: AmpFork, SFD: CAD, SPD: CAD, SPD: 911 Logging Recorder
What concerns, if any, do you have about the use of this technology?
That would be good with advanced technology
What value, if any, do you see in the use of this technology?
Yes, around the city.
What do you want City leadership to consider about the use of this technology?
Need good train to people who use new technologies
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

ID: 10550713652
Submitted Through: Survey Monkey
Date: 2/23/2019 12:12:23 PM
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars
What concerns, if any, do you have about the use of this technology?
This is playing outrageous. Well we are telling the public is that it is okay for a city worker to come and use binoculars to look into your private property.
What value, if any, do you see in the use of this technology?
This really is barbaric there are certain technologies that their intermediate benefit might be greater than the risk that provide a much more simple solution then this solution. This solution a binocular use can possibly be interpreted for many things ho
What do you want City leadership to consider about the use of this technology?
It's just not right.
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

Appendix F: Department Responses to Public Inquiries

City Light received the following questions for Group 2 surveillance technologies during the public comment period of Feb. 5, 2019 to March 26, 2019. City Light's answers to the questions, which solely related to City Light's use of binoculars for current diversion detection, are presented below.

Do Seattle City Light Current Diversion employees wear something visible that shows customers they are from Seattle City Light?

Seattle City Light employees who are working in the field can be identified by their Seattle City Light ID badge and a hard hat.

If a City Light customer wants to file a complaint about a City Light employee, how do they do that?

A customer can file a complaint about a City Light employee by contacting Customer Care at (206) 684-3000, via email, mail, or in person at the Customer Service Center in the Seattle Municipal Tower located at 700 Fifth Ave., 4th floor lobby, Seattle, WA 98104.

Has there been a situation where a customer sees a City Light employee looking at someone's house with binoculars and the customer may not have been notified?

No advance notification is provided to the public, as doing so may compromise the detection of current diversion on a single, previously suspected service-drop location. Current Diversion staff view locations that are in public view, so it is possible other customers have observed this work. However, staff use binoculars for approximately one-minute at a time and only for City Light business purposes.

Has there been a situation where the meter was located on the opposite side of where the City Light employee was looking?

The Current Diversion team only investigates specific meters and other implicated electrical equipment at locations previously identified and documented as sites of suspected current diversion. Binoculars are used only to make determinations about whether current diversion is likely taking place, and, in certain instances, to view implicated and potentially dangerous electrical equipment.

Do City Light employees get background checks?

City Light conducts job-related background checks prior to hire in order to ensure a safe and secure work environment in which employees, the public, resources, and assets are protected, while protecting the integrity and confidentiality of information gathered during the evaluation. In most cases, a background check will be conducted for the finalist following a contingent offer of employment. Offer letters issued prior to completion of the background check will notify the finalist that the offer is contingent upon successful completion of any and all required background checks. In addition, City Light personnel whose work duties require having critical

access to City Light physical and logical assets must have a background check prior to being granted such access, which is renewed at least once every four years.

If a City Light customer files a complaint against an employee, are complaints being followed up? What is the average time for disciplinary action for a City Light employee? How long is the process for a full investigation?

Yes. City Light customer complaints about employee conduct are generally escalated to the People & Culture team at City Light for further action in order to ensure that City Light employees are serving customers reliably and with integrity. Appropriate next steps to address employee conduct are determined on a case-by-case basis. The complaining customer may not be informed of the specific action taken by City Light, due to the confidential nature of personnel matters. However, City Light is committed to employee accountability and providing excellent customer service.

When a full fact-finding investigation is necessary, it is City Light's objective to complete it as promptly as possible while ensuring that the investigation is fair, complete, and impartial. In the event of harassment, discrimination, or retaliation allegations, it is City Light's objective to complete investigations within 90 days unless compelling circumstances require more time. The duration of investigations is often dependent upon the availability and cooperation of witnesses, the volume of relevant documents, as well as the complexity of the subject-matter at issue. Resulting disciplinary and follow-up actions after an investigation are completed as promptly as possible while respecting the due process rights of City Light employees.

What is the purpose of tracking current diversion by using binoculars?

Binoculars may be used to address meter access issues, such as locked gates, unsafe premises, or threatening dogs. The binoculars enable Current Diversion staff to evaluate if a meter has been tampered with to substantiate suspicions of current diversion.

Appendix G: Letters from Organizations or Commissions

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

March 12th, 2019

Seattle City Council
600 4th Ave
Seattle, WA 98104

Re: Surveillance Ordinance Group 2 Public Comment

We would like to first thank City Council for passing one of the strongest surveillance technology policies in the country, and thank Seattle IT for facilitating this public review process.

These public comments were prepared by volunteers from the Community Technology Advisory Board (CTAB) Privacy & Cybersecurity Committee, as part of the surveillance technology review defined in Ordinance 125376. These volunteers range from published authors, to members of the Seattle Privacy Coalition, to industry experts with decades of experience in the information security and privacy sectors.

We reviewed and discussed the Group 2 Surveillance Impact Reports (SIRs) with a specific emphasis on privacy policy, access control, and data retention. Some recurring themes emerged, however, that we believe will benefit the City as a whole, independent of any specific technology:

- **Interdepartmental sharing of privacy best practices**: When we share what we've learned with each other, the overall health of the privacy ecosystem goes up.
- **Regular external security audits**: Coordinated by ITD (Seattle IT), routine third-party security audits are invaluable for both hosted-service vendors and on-premises systems.
- **Mergers and acquisitions**: These large, sometimes billion-dollar ownership changes introduce uncertainty. Any time a vendor, especially one with a hosted service, changes ownership, a thorough review of any privacy policy or contractual changes should be reviewed.
- **Remaining a Welcoming City**: As part of the Welcoming Cities Resolution, no department should comply with a request for information from Immigration and Customs Enforcement (ICE) without a criminal warrant. In addition, the privacy of all citizens should be protected equally and without consideration of their immigration status.

Sincerely,

Privacy & Cybersecurity Committee volunteers
Torgie Madison, Co-Chair
Smriti Chandashekar, Co-Chair
Camille Malonzo
Sean McLellan
Kevin Orme
Chris Prosser
Rabecca Rocha
Adam Shostack
T.J. Telan

Community Technology Advisory Board
Steven Maheshwary, CTAB Chair
Charlotte Lunday, CTAB Co-Vice Chair
Torgie Madison, CTAB Co-Vice Chair
Smriti Chandashekar, CTAB Member
Mark DeLoura, CTAB Member
John Krull, CTAB Member
Karia Wong, CTAB Member

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SFD: Computer-Aided Dispatch (CAD)

Comments

The use of a centralized Computer-Aided Dispatch (CAD) system is essential to protecting the health and safety for all Seattle citizens. The National Fire Protection Association (NFPA) standards outline specific alarm answering, turnout, and arrival times[1] that could only be accomplished in a city of this size with a CAD system.

In addition, with over 96,000 SFD responses per year (2017)[2], only a computerized system could meet the state's response reporting guidelines established in RCW 35A.92.030[3].

CentralSquare provides the dispatch service used by SFD. CentralSquare is a new entity resulting from the merger of Superion, TriTech, Zuercher, and Aptean[4] in September 2018.

Recommendations

- Tritech, the underlying technology supplying SFD with CAD services, has been in use since 2003 [SIR 4.3], making it 16 years old. As with any technology, advancements in security, speed, usefulness, and reliability come swiftly. Due to the age of the technology, we recommend conducting a survey into the plausibility of replacing Tritech as SFD's CAD solution.

- Tritech was merged very recently into CentralSquare in one of the largest-ever government technology mergers to date. Due diligence should be exercised to ensure that this vendor is keeping up to date with industry best practices for security and data protection, and that their privacy policies are still satisfactory after the CentralSquare merger. We recommend ensuring that the original contracts and privacy policies have remained unchanged as a result of this merger.

---

[1] "NFPA Standard 1710." https://services.prod.iaff.org/ContentFile/Get/30541
[2] "2017 annual report - Seattle.gov." https://www.seattle.gov/Documents/Departments/Fire/FINAL%20Annual%20Report_2017.pdf
[3] "RCW 35A.92.030: Policy statement—Service ... - Access WA.gov." https://app.leg.wa.gov/rcw/default.aspx?cite=35A.92.030
[4] "Superion, TriTech, Zuercher, and Aptean's Public Sector Business to " 5 Sep. 2018, https://www.tritech.com/news/superion-tritech-zuercher-and-apteans-public-sector-business-to-form-centra

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SDOT: Acyclica

Comments

Traffic congestion is an increasingly major issue for our city. Seattle is the fastest-growing major city in the US this decade, at 18.7% growth, or 114,00 new residents[5]. Seattle ranks sixth in the nation for traffic congestion[6]. The need for intelligent traffic shaping and development has never been greater. Acyclica, a service provided by Western Systems and now owned by FLIR[7], is an implementation of surveillance technology specifically designed to address this problem.

We were happy to see the 2015 independent audit of Acyclica's systems [SIR 8.2]. This is an excellent industry best practice, and one that we'll be recommending to other departments throughout this document.

In addition, we are pleased to see the hashing function's salt value rotated every 24-hours [SIR 4.10]. This ensures that even the 10-year retention policy [SIR 5.2] cannot be abused to correlate multiple commute sessions and individually identify a person.

Recommendations

- FLIR Systems' acquisition of Acyclica is a recent development (September 2018). We recommend verifying that the Western Systems terms [SIR 3.1] still apply. If they have been superseded by new terms from FLIR Systems, those should be subject to an audit by SDOT and Seattle IT. Specifically, section 2.5.1 of Western Systems' terms must still apply:

  > 2.5.1. It is the understanding of the City that the data gathered are encrypted to fully eliminate the possibility of identifying individuals or vehicles. In no event shall City or Western Systems and its subcontractors make any use of the data gathered by the devices for any purpose that would identify the individuals or vehicles included in the data.

- FLIR Systems is known primarily as an infrared technology vendor. Special care should be taken if FLIR/Acyclica attempt to couple IR scanning with WiFi/MAC sniffing. Implementation of an IR system would necessitate a new public surveillance review.

---

[5] "114,000 more people: Seattle now decade's fastest-growing big city in ...." 24 May. 2018, https://www.seattletimes.com/seattle-news/data/114000-more-people-seattle-now-this-decades-fastest-growing-big-city-in-all-of-united-states/
[6] "INRIX Global Traffic Scorecard." http://inrix.com/scorecard/
[7] "FLIR Systems Acquires Acyclica | FLIR Systems, Inc.." 11 Sep. 2018, http://investors.flir.com/news-releases/news-release-details/flir-systems-acquires-acyclica

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SCL: Binoculars, Check Meter, SensorLink

Comments

As these three technologies are serving the same team and mission objectives, we will review them here in a combined section.

The mission of the Current Diversion Team (CDT) is to investigate and gather evidence of illegal activity related to the redirection and consumption of electricity without paying for its use. As such, none of these technologies surveil the public at large. They instead target specific locations and equipment, albeit without the associated customer's knowledge.

It appears as though all data collected through the Check Meter Device and SensorLink Amp Fork are done without relying on a third-party service, so the usual scrutiny of a vendor's privacy policies does not apply.

Recommendations

- **Binoculars**: We have no recommendations for the use of binoculars.
- **Check Meter Device & SensorLink Amp Fork**: As noted in the comments above, we have no further recommendations for the use of the Check Meter Device and SensorLink Amp Fork technologies.
- **Racial Equity**: As with any city-wide monitoring practice, it can be easy to more closely scrutinize one neighborhood over another. Current diversion may be equally illegal (and equally prevalent) across the city, but the enforcement of this law may be unevenly applied. This could introduce racial bias by disproportionately burdening specific neighborhoods with a higher level of surveillance.

  As described, DPP 500 P III-416 section 5.2[8] asserts that all customers shall receive uniform consideration [SIR RET 1.7]. To ensure this policy is respected, we encourage City Light to track and routinely review the neighborhoods where CDT performs investigations, with a specific emphasis on racial equity. This information should be made publicly available.

  When asked at the February 27th Surveillance Technology public meeting, SDOT indicated that no tracking is currently being done on where current diversion is enforced.

[8] "SCL DPP 500 P III-416 Current Diversion - Seattle.gov." 11 Jan. 2012, http://www.seattle.gov/light/policies/docs/III-416%20Current%20Diversion.pdf

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: 911 Logging Recorder

Comments

This is a technology that the general public would likely already assume is in place. Some of the more sensational 911 call logs have been, for example, played routinely on the news around the country. Since it would not alarm the public to know that 911 call recording is taking place, our recommendations will focus primarily on data use, retention, and access control.

Call logging services are provided by NICE Ltd., an Israeli company founded in 1986. This vendor has had a troubling history with data breaches. For example, a severe vulnerability discovered in 2014 allowed unauthorized users full access to a NICE customer's databases and audio recordings[9]. Again, in 2017, a NICE-owned server was set up with public permissions, exposing phone numbers, names, and PINs of 6 million Verizon customers[10].

Recommendations

- SIR Appendix K includes a CJIS audit performed in 2017. SIR section 4.10 also mentions that ITD (Seattle IT) periodically performs routine monitoring of the SPD systems.

  However, given the problematic history with the quality of the technology vendor, if any of the NICE servers, networks, or applications were installed by the vendor (or installation was overseen/advised by the vendor), we recommend an external audit of the implementation of the call logging technology.

- SIR sections 3.3 and 4.2 outline the SPD-mandated access control and data retention policies, however it is not apparent if there is a policy that strictly locks down the use of this technology to a well-defined list of allowed cases. We recommend formally documenting the allowed 911 Logging use cases, and creating a new SIR for any new desired applications of this technology.

  With a 90-day retention policy [SIR 4.2], and with SPD receiving 900,000 calls per year[11], there are about 220,000 audio recordings existing at any given time. This is enough for a data mining, machine learning, or voice recognition project.

---

[9] "Backdoor in Call Monitoring, Surveillance Gear — Krebs on Security." 28 May. 2014, https://krebsonsecurity.com/2014/05/backdoor-in-call-monitoring-surveillance-gear/
[10] "Nice Systems exposes 14 million Verizon customers on open AWS ...." 12 Jul. 2017, https://www.techspot.com/news/70106-nice-systems-exposes-14-million-verizon-customers-open.html
[11] "9-1-1 Center - Police | seattle.gov." https://www.seattle.gov/police/about-us/about-policing/9-1-1-center

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: Computer-Aided Dispatch (CAD)

Comments

As mentioned in the section "SFD: Computer-Aided Dispatch (CAD)" and the section "SPD: 911 Logging Recorder", these dispatch technologies are mandatory for functional emergency services of a city this size. No other system would be able to meet the federal- and state-mandated response times and reporting requirements.

SIR section 4.10 mentions that ITD (Seattle IT) performs routine inspections of the Versaterm implementation.

Versaterm, founded in 1977, provides the technology used by SPD's CAD system. SPD purchased this technology in 2004. In September of 2016, there was a legal dispute between Versaterm and the City of Seattle over a Public Records Act (PRA) disclosure of certain training and operating manuals[12]. The court ruled in favor of Versaterm.

Recommendations

- It is not immediately clear what use cases are described in SIR 2.5 describing data access by "other civilian staff whose business needs require access to this data". All partnerships and data flows between SPD and businesses should be explicitly disclosed.

- This system has been in place for 15 years. As with any technology, advancements in security, speed, usefulness, and reliability come swiftly. Due to the age of the technology, and the potential damaged relationship between Seattle and Versaterm due to the aforementioned legal dispute, we recommend conducting a survey into the plausibility of replacing Versaterm as SPD's CAD solution.

- As mentioned in the introduction to this document, Seattle has adopted the Welcoming Cities Resolution[13]. In honoring this resolution, we recommend that SPD never disclose identifying information, from CAD or any system, to Immigrations and Customs Enforcement (ICE) without a criminal warrant.

[12] "Versaterm Inc. v. City of Seattle, CASE NO. C16-1217JLR | Casetext." 13 Sep. 2016, https://casetext.com/case/versaterm-inc-v-city-of-seattle-2
[13] "Welcoming Cities Resolution - Council | seattle.gov." http://www.seattle.gov/council/issues/past-issues/welcoming-cities-resolution

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: CopLogic

Comments

Track 1 - Public reporting of no-suspect, no-evidence, non-emergency crimes

CTAB understands that in cases where no evidence or suspect is available, a crime should be reported (for statistical or insurance purposes) but does not require the physical appearance of an SPD officer.

Track 2 - Retail Loss Prevention

This track is more problematic, as it could be used by retailers as a method to unreasonably detain, intimidate, or invade the privacy of a member of the public accused of, but not proven guilty of, shoplifting.

Recommendations

- **Track 2**: If not already done, retailers should be trained and informed that having a CopLogic login does not allow them to act as if they are law enforcement officers. Members of the public suspected of shoplifting need to have an accurate description of their rights in order to make informed decisions before providing identifying information. Retailers are also held to a lower standard than SPD regarding racial bias. It is virtually guaranteed that people of color are disproportionately apprehended and entered into the retail track of CopLogic.

  We recommend discontinuing Track 2 entirely.

- **Track 1 & 2**: If not already done, SPD, in coordination with Seattle IT, should perform or hire a company to perform an audit of the vendor's systems. If this audit has not been performed in the 8 years since purchasing this system, it should absolutely be done before the 10-year mark in 2020.
- **Track 1 & 2**: It is not immediately clear in the SIR or LexisNexis's Privacy Policy what CopLogic does with these records long-term, after SPD has imported them into their on-premises system. A written statement from LexisNexis on how this data is used, mined, or sold to affiliates/partners should be acquired by SPD.
- **Track 1 & 2**: We recommend migrating CopLogic to an on-premises solution. We found the LexisNexis privacy policy to be obfuscated and vague[14]. Such sensitive information should not be protected by trust alone.

[14] "Privacy Policy | LexisNexis." 7 May. 2018, https://www.lexisnexis.com/en-us/terms/privacy-policy.page

City of Seattle

March 20, 2019

RE: ACLU-WA Comments Regarding Group 2 Surveillance Technologies

ACLU
AMERICAN CIVIL LIBERTIES UNION
Washington

901 Fifth Ave, Suite #630
Seattle, WA 98164
(206) 624-2184
aclu-wa.org

Tana Lin
Board President

Michele Storms
Executive Director

Shankar Narayan
Technology & Liberty Project Director

Dear Seattle IT:

On behalf of the ACLU of Washington, I write to offer our comments on the surveillance technologies included in Group 2 of the Seattle Surveillance Ordinance process. We are submitting these comments by mail and electronically because they do not conform to the specific format of the online comment form provided on the CTO's website, and because the technologies form groups in which some comments apply to multiple technologies.

These comments should be considered preliminary, given that the Surveillance Impact Reports (SIR) for each technology leave a number of significant questions unanswered. Specific unanswered questions for each technology are noted in the comments relating to that technology, and it is our hope that those questions will be answered in the updated SIR provided to the Community Surveillance Working Group and to the City Council prior to their review of that technology. In addition to the SIR, our comments are also based on independent research relating to the technology at hand.

The 8 technologies in Group 2 are covered in the following order.

I. Acyclica (SDOT)

II. CopLogic (SPD)

III. Computer-Aided Dispatch & 911 Logging Recorder Group

1. Computer-Aided Dispatch (SPD)
2. Computer-Aided Dispatch (SFD)
3. 911 Logging Recorder (SPD)

IV. Current Diversion Technology Group

1. Check Meter Device (Seattle City Light)
2. SensorLink Amp Fork (Seattle City Light)
3. Binoculars/Spotting Scope (Seattle City Light)

I. Acyclica - SDOT

Background

Acyclica technology is a powerful location-tracking technology that raises a number of civil liberties concerns because of its ability to uniquely identify individuals and their daily movements. Acyclica (via its hardware vendor, Western Systems), manufactures Intelligent Transportation System (ITS) sensors called RoadTrend that are used by the Seattle Department of Transportation for the stated purpose of traffic management. These RoadTrend sensors collect encrypted media access control (MAC) addresses, which are transmitted by any Wi-Fi enabled device including phones, cameras, laptops, and vehicles. Collection of MAC addresses, even when hashed (a method of de-identifying data irreversibly),[1] can present locational privacy challenges.

Experts analyzing a dataset of 1.5 million individuals found that just knowing four points of approximate spaces and times that individuals were near cell antennas or made a call were enough to uniquely identify 95% of individuals.[2] In the case of Acyclica's operation in Seattle, the dataset is comprised of MAC addresses recorded on at least 301 intersections,[3] which allows Acyclica to generate even more precise location information about individuals. Not only do the RoadTrend sensors pick up the MAC addresses of vehicle drivers and riders, but these sensors can also pick up the MAC addresses of all nearby individuals, including pedestrians, bicyclists, and people in close structures (e.g., apartments, offices, and hospitals). Acyclica technology's location tracking capabilities means that SDOT's use of Acyclica can not only uniquely identify individuals with ease, but can also create a detailed map of their movements. This raises privacy concerns for Seattle residents, who may be tracked without their consent by this technology while going about their daily lives.

These location-tracking concerns are exacerbated by the lack of clarity around whether SDOT has a contract with Acyclica (see below). Without a contract, data ownership and scope of data sharing and repurposing by Acyclica is unclear. For example, without contractual restrictions, Acyclica

[1] Hashing is a one-way function that scrambles plain text to produce a unique message digest. Unlike encryption—which is a two-way function, allowing for decryption—what is hashed cannot be un-hashed. However, hashed location data can still be used to uniquely identify individuals. While it is infeasible to compute an input given only its hash output, pre-computing a table of hashes is possible. These types of tables consisting of pre-computed hashes and their inputs are called rainbow tables. With a rainbow table, if an entity has a hash, then they only need to look up that hash in their table to then know what the original MAC address was.
[2] Montjoye, Y., Hidalgo, C., Verleysen, M., and Blondel, V. 2013. Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports.* 3:1375.
[3] The SIR states that SDOT has 301 Acyclica units installed throughout the City. However, an attached location excel sheet in Section 2.1 lists 389 Acyclica units, but only specifies 300 locations.

would be able to share the raw data (i.e., the non-aggregated, hashed data before it is summarized and sent to SDOT) with any third parties, and these third parties would be able to use the data in any way they see fit, including combining the data with additional data such as license plate reader or facial recognition data. Acyclica could also share the data with law enforcement agencies that may repurpose the data, as has happened with other City data. For example, in 2018, U.S. Immigration and Customs Enforcement (ICE) approached Seattle City Light with an administrative subpoena demanding information on a particular customer location, including phone numbers and information on related accounts.[4] ICE also now has agency-wide access to a nationwide network of license plate readers controlled by Vigilant Solutions,[5] indicating the agency may seek additional location data for immigration enforcement purposes in the future. Data collected via Acyclica should never be used for law enforcement purposes.

The uncertainty around the presence or absence of a contract contributes to two key issues: (1) lack of a clearly defined purpose of use of Acyclica technology; and (2) lack of clear restrictions on the use of Acyclica technology that track that purpose. With no contract, SDOT cannot enforce policies restricting the use of Acyclica technology to the intended purpose.

There are also a number of contradictory statements in the SIR concerning the operation of Acyclica technology,[6] as well as discrepancies between the SIR, the information shared at the technology fair (the first public meeting to discuss the Group 2 technologies),[7] and ACLU-WA's conversation with the President of Acyclica, Daniel Benhammou. All these leave us with concerns over whether SDOT fully understands (and the SIR reflects) the capabilities of the technology. In addition, there remain a number of critical unanswered questions that the final SIR must address (set forth below).

Of additional concern is the recent acquisition of Acyclica by FLIR Systems, an infrared and thermal imaging company funded by the U.S. Department of Defense.[8] As of March 2019, FLIR has discontinued Acyclica RoadTrend sensors.[9] Neither the implications of the FLIR acquisition nor the discontinuation of the RoadTrend sensors are mentioned in the SIR—but if the sensors used will change, the SIR should make clear how that will impact the technology.

a. Specific Concerns

- *Inadequate Policies Defining Purpose of Use.* Policies cited in the SIR are vague,

[4] https://crosscut.com/2018/02/immigration-officials-subpoena-city-light-customer-info
[5] https://www.theverge.com/2018/3/1/17067188/ice-license-plate-data-california-vigilant-solutions-alpr-sanctuary
[6] Explained in further detail in 1. Acyclica – SDOT *Major Concerns* below.
[7] http://www.seattle.gov/tech/initiatives/privacy/events-calendar#/?i=3
[8] https://www.crunchbase.com/acquisition/flir-systems-acquires-acyclica--e6043a1a#section-overview
[9] https://www.flir.com/support/products/roadtrend#Specifications

short, and impose no meaningful restrictions on the purposes for which Acyclica devices may be used.[10] Section 1.1 of the abstract set forth in the SIR states that Acyclica is used by over 50 agencies to "to help to monitor and improve traffic congestion." Section 2.1 is similarly vague, providing what appear to be examples of some types of information the technology produces (e.g., calculated average speeds) in order to facilitate outcomes (correcting traffic signal timing, providing information to travelers about expected delays, and allowing SDOT to meet traffic records and reporting requirements)—but it's not clear this list is exhaustive. Section 2.1 fails to describe the purpose of use, all the types of information Acyclica provides, and all the types of work that Acyclica technology facilitates. All these must be clarified.

- *Lack of Clarity on Whether Acyclica and SDOT have a Written Contract.* The SIR does not state that any contract exists, and in the 2018 conversation ACLU-WA had with Benhammou, he stated that there was no contract between the two parties. However, at the 2019 technology fair, the SDOT representative affirmatively stated that SDOT has a contract with Acyclica. As previously mentioned, the lack of a contract limits SDOT's ability to restrict the scope of data sharing and repurposing. The only contractual document provided appears to be a terms sheet in Section 3.0 detailing SDOT's terms of service with Western Systems (the hardware vendor that manufactures the Acyclica RoadTrend sensors), which states that Western Systems only deals with the maintenance and replacement of the hardware used to gather the data, and not the data itself.

- *Lack of Clarity on Data Ownership.* At the technology fair, the SDOT representative stated that SDOT owns all the data collected (including the raw data), but the SIR only states that the aggregated traffic data is owned by SDOT. In the 2018 conversation, Benhammou stated that Acyclica owns all the raw data. There is an apparent lack of clarity between SDOT and Acyclica concerning ownership of data that must be addressed.

- *Data Retention Periods are Unclear.* Section 5.2 of the SIR states that there is a 10-year internal deletion requirement for the aggregated traffic data owned by SDOT, but pg. 37 of the SIR states that "the data is deleted within 24 hours to prevent tracking devices over time." In the 2018 interview, Benhammou stated that Acyclica retains all non-aggregated data indefinitely. It is unclear whether the different retention periods stated in the SIR are referring to different types of data. The lack of clarity on data retention periods also relates to the lack of clarity on data ownership given that data retention periods may depend on data ownership.

[10] As noted in 1. Acyclica – SDOT *Background* above.

- *Inaccurate Descriptions of Anonymization/Data Security Practices.* The SIR appears to use the terms "encryption" and "hashing" interchangeably in some parts of the SIR, making it difficult to clearly understand Acyclica's practices in this area. For example, Section 7.2 states: "Contractually, Acyclica guarantees that the data gathered is encrypted to fully eliminate the possibility of identifying individuals or vehicles." But by design, encryption allows for decryption with a key, meaning anyone with that key and access to the data can identify individuals. (Also, if there is no contract between SDOT and Acyclica, the use of 'contractually' is misleading). This language is also used in the terms sheet detailing SDOT's contract with Western Systems (in Section 2.5.1 in the embedded contract). The SIR compounds this confusion with additional contradictory statements. For example, the SIR states in multiple sections that the data collected by the RoadTrend sensors are encrypted and hashed on the actual sensor. However, according to a letter from Benhammou provided by SDOT representatives at the technology fair,[11] the data is never hashed on the sensor—the data is only hashed after being transmitted to Acyclica's cloud server. These contradictory descriptions cause concern.

- *No Restrictions on Non-City Data Use.* Section 6.3 of the SIR states that there are no restrictions on non-City data use. However, there are no policies cited making clear the criteria for such use, any inter-agency agreements governing sharing of Acyclica data with non-City parties, or why the data must be shared in the first place.

- *Not All Locations of Acyclica Devices are Specified.* Section 2.1 of the SIR states that there are 301 Acyclica locations in Seattle. However, in the embedded excel sheet detailing the serial numbers and specific intersections in which Acyclica devices are installed, there are 389 serial numbers, but only 300 addresses/locations specified. The total number and the locations of Acyclica devices collecting data in Seattle is unclear. This gives rise to the concern that there are unspecified locations in which Acyclica devices are collecting MAC addresses.

- *No Mention of RoadTrend Sensor Discontinuation.* As noted in the background,[12] Acyclica has been acquired by FLIR, an infrared and thermal imaging company. As of March 2019, FLIR's product webpage states that the Acyclica RoadTrend sensors (those currently used by SDOT) have been discontinued.[13] From the information we have, it is unclear if SDOT will be able to continue using the RoadTrend sensors described in the 2019 SIR. Given that FLIR sensors, such as the TrafiOne, have capabilities that go much farther than those of the

[11] Included in Appendix 1.
[12] As noted in 1. Acyclica – SDOT *Background* above.
[13] https://www.flir.com/support/products/roadtrend#Specifications

RoadTrend sensors (e.g., camera technology and thermal imaging)[14] as well as potentially different technical implementations, their use would give rise to even more serious privacy and misuse concerns. Neither the implications of the FLIR acquisition nor the discontinuation of the RoadTrend sensors are mentioned in the SIR.

- *No Mention of Protecting MAC Addresses of Non-Drivers/Riders (e.g., people in nearby buildings).* The Acyclica sensors will pick up the MAC addresses of all nearby individuals, regardless of whether they are or are not driving or riding in a vehicle. The SIR does not mention any steps taken to reduce the privacy infringements on non-drivers/riders.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- For what specific purpose or purposes will Acyclica be used, and what policies state this?
- Does SDOT have a contract with Acyclica, and if so, why is the contract not included in the SIR?
- Who owns the raw, non-aggregated data collected by Acyclica devices?
- What is the retention period for the different types of collected data (aggregated and non-aggregated)—for both SDOT and Acyclica?
- Provide accurate descriptions of Acyclica's data security practices, including encryption and hashing, consistent with the letter from Daniel Benhammou, including any additional practices that prevent reidentification.
- What third parties will access Acyclica's data, for what purpose, and under what conditions?
- Why are 89 locations not specified in the embedded Acyclica locations sheet in Section 2.1 of the SIR?
- Will SDOT continue to use Acyclica RoadTrend Sensors, and for how long? If SDOT plans to switch to other sensors, which ones, and how do their capabilities differ from the RoadTrend Sensors?
- Did SDOT consider any other alternatives when deciding to acquire Acyclica? Did SDOT consider other, more privacy protective traffic management tools in use (for example, inductive-loop detectors currently used by the Washington State Department of Transportation and the US

[14] https://www.flir.com/support/products/trafione#Resources

Department of Transportation)?[15]

- How does SDOT plan to reduce the privacy infringements on non-drivers/riders?

c. Recommendations for Regulation:

At this stage, pending answers to the questions set forth above, we can make only preliminary recommendations for regulation of Acyclica. We recommend that the Council adopt, via ordinance, clear and enforceable rules that ensure, at a minimum, the following:

- There must be a binding contract between SDOT and Acyclica.
- The contract between SDOT and Acyclica must include the following minimum provisions:
  - A data retention period of 12 hours or less for any data Acyclica collects, within which time Acyclica must aggregate the data, submit it to SDOT, and delete both non-aggregated and aggregated data.
  - SDOT receives only aggregated data.
  - SDOT owns all data, not Acyclica.
  - Acyclica cannot share the data collected with any other entity besides SDOT for any purpose.
- The ordinance must define a specific purpose of use for Acyclica technology, and all use of the tool and its data must be restricted to that purpose. For example: Acyclica may only be used for traffic management purposes, defined as activities concerning calculating average travel times, regulating traffic signals, controlling traffic disruptions, determining the placement of barricades or signals for the duration of road incidents impeding normal traffic flow, providing information to travelers about traffic flow and expected delays, and allowing SDOT to meet traffic records and reporting requirements.
- SDOT must produce an annual report detailing its use of Acyclica, including details how SDOT used the data collected, the amount of data collected, and for how long it was retained and in what form.

II. CopLogic – SPD

[15] https://www.fhwa.dot.gov/publications/research/operations/its/06108/03.cfm

Background

CopLogic (LexisNexis's Desk Officer Reporting System-DORS)[16] is a technology owned by LexisNexis and used by the Seattle Police Department to allow members of the public and retailers to submit online police reports regarding non-emergency crimes. Members of the public and retailers can submit these reports through an online portal they can access via their phone, tablet, or computer. Community members can report non-emergency crimes that have occurred within the Seattle city limits, and retail businesses that participate in SPD's Retail Theft Program may report low-level thefts that occur in their businesses when they have identified a suspect. This technology is used by SPD for the stated purpose of freeing up resources in the 9-1-1 Center, reducing the need for a police officer to be dispatched for the sole purpose of taking a police report.

This technology gives rise to potential civil liberties concerns because it allows for the collection of information about community members, unrelated to a specific incident, and without any systematic method to verify accuracy or correct inaccurate information. In addition, there is lack of clarity surrounding data retention and data sharing by LexisNexis, and around how CopLogic data will be integrated into SPD's Records Management System.

a. Concerns

- *Lack of Clarity on CopLogic/LexisNexis Data Collection and Retention.* There is no information in the SIR or in the contract between SPD and LexisNexis detailing the data retention period by LexisNexis (Section 5.2 of the SIR). This lack of clarity stems in part from an unclear description of what's provided by LexisNexis—it's described as an online portal, but the SIR and the contract provided appears to contemplate in Section 4.8 that LexisNexis will indeed access and store collected data. If true, the nature of that access should be clarified, and data restrictions including clear access limitations and retention periods should accordingly be put in place. Once reports are transferred over to SPD's Records Management System (RMS), the reports should be deleted by CopLogic/LexisNexis.

- *Lack of Clarity on LexisNexis Data Sharing with Other Agencies or Third Parties.* If LexisNexis does access and store data, it should do so only for purposes of fulfilling the contract, and should not share that data with third parties. But the contract between SPD and LexisNexis does not make clear whether LexisNexis is prohibited entirely from sharing data with other entities (it does contain a restriction on "transmit[ting]" the data, but without reference to third parties.

[16] https://risk.lexisnexis.com/products/desk-officer-reporting-system

- *No Way to Correct Inaccurate Information Collected About Community Members.* Community members or retailers may enter personally-identifying information about third parties without providing notice to those individuals, and there is no immediate, systematic method to verify the accuracy of information that individuals provide about third parties. There are also no stated measures in the SIR to destroy improperly collected data.

- *Lack of clarity on how the CopLogic data will be integrated with and analyzed within SPD's RMS.* At the technology fair, SPD stated that completed complaints will go into Mark43[17] when it is implemented. ACLU-WA has previously raised concerns about the Mark43 system, and it should be made clear how CopLogic data will enter that system, including to what third parties it will be made available.[18]

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What data does LexisNexis collect and store via CopLogic? What are LexisNexis's data retention policies for CopLogic data?

- Are there specific policies restricting LexisNexis from sharing CopLogic data with third parties? If so, what are they?

- Is there any way to verify or correct inaccurate information collected about community members?

- How will CopLogic data be integrated with Mark43?

c. Recommendations for Regulation:

Pending answers to the questions set forth above, we can make only preliminary recommendations for regulation of CopLogic. SPD should adopt clear and enforceable policies that ensure, at a minimum, the following:

- After CopLogic data is transferred to SPD's RMS, LexisNexis must delete all CopLogic data.

- LexisNexis is prohibited from using CopLogic data for any purpose other than those set forth in the contract, and from sharing CopLogic data with third parties.

[17] https://www.aclu-wa.org/docs/aclu-letter-king-county-council-regarding-mark-43
[18] A Records Management System (RMS) is the management of records for an organization throughout the records-life cycle. New RMSs (e.g., Mark43) may have capabilities that allow for law enforcement agencies to track and analyze the behavior of specific groups of people, leading to concerns of bias in big data policing, particularly for communities of color.

- Methods are available to the public to correct inaccurate information entered in the CopLogic portal.
- Measures are implemented to delete improperly collected data.

III. Computer-Aided Dispatch & 911 Logging Recorder Group

Overall, concerns around the Computer-Aided Dispatch (CAD) and 911 Logging Recorder technologies focus on use of the technologies and/or collected data them for purposes other than those intended, over-retention of data, and sharing of that data with third parties (such as federal law enforcement agencies). Therefore, for all of these technologies as appropriate, we recommend that the responsible agency should adopt clear and enforceable rules that ensure, at a minimum, the following:

- The purpose of use must be clearly defined, and its operation and data collected must be explicitly restricted to that purpose only.
- Data retention must be limited to the time needed to effectuate the purpose defined.
- Data sharing with third parties, if any, must be limited to those held to the same restrictions.
- Clear policies must govern operation, and all operators should be trained in those policies.

Specific comments follow:

1. Computer-Aided Dispatch – SPD

Background

CAD is a software package (made by Versaterm) utilized by the Seattle Police Department's 9-1-1 Center that consists of a set of servers and software deployed on dedicated terminals in the 9-1-1 center, in SPD computers, and as an application on patrol vehicles' mobile data computers and on some officers' smart phones. The stated purpose of CAD is to assist 9-1-1 Center call takers and dispatchers with receiving requests for police services, collecting information from callers, and providing dispatchers with real-time patrol unit availability. Concerns include lack of clarity surrounding data retention and data sharing with third parties.

a. Concerns:

- *Lack of clarity on data retention within CAD v. RMS.* While the SIR makes clear that at some point, CAD data is transferred to SPD's RMS, it is unclear what data, if any, the CAD system itself retains and for how long. If the CAD system does retain some data (for example, call logs)

independent of the RMS, and that data is accessible to the vendor, appropriate data protections should be put in place. But because the SIR usually references "data collected by CAD," it is unclear where that data resides.

- *Lack of a policy defining purpose of the technology and limiting its use to that purpose*: Unlike SFD's similar system, SPD appears to have no specific policy defining the purpose of use for CAD and limiting its use to that purpose.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- Does the CAD system itself store data? If so, what data and for how long? Who can access that data?

c. Recommendations for Regulation:

Depending on the answer to the question above, appropriate data protections may be needed as described above. In addition, SPD should adopt a policy similar to SFD's, clearly defining purpose and limiting use of the tool to that purpose.

2. Computer-Aided Dispatch – SFD

Background

Computer Aided Dispatch (CAD) is a suite of software packages used by SFD and made by Tritech that provide unit recommendations for 911 emergency calls based on the reported problem and location of a caller. The stated purpose of CAD is to allow SFD to manage emergency and non-emergency call taking and dispatching operations. The technology allows SFD to quickly enable personnel to execute rapid aid deployment.

Generally and positively, SFD clearly defines the purpose of use, restricts CAD operation and data collection to that purpose only, limits sharing with third parties, and specifies policies on operation and training. However, SFD must clarify what data is retained within CAD, data retention policies, and provide information about its data sharing partners.

d. Concerns

- *Lack of clarity on data retention within CAD*. It is unclear what data, if any, the CAD system itself retains and for how long. If the CAD system does retain some data (for example, call logs) and that data is accessible to the vendor, appropriate data protections should be put in place.
- *Lack of clarity on data retention policies*. At the technology fair, we learned that CAD data is retained indefinitely. It is not clear what justifies indefinite retention of this data.

- *Lack of clarity on data sharing partners.* In Section 6.3 of the SIR, SFD states that in rare case where CAD data is shared with partners other than those specifically named in the SIR, a third-party nondisclosure agreement is signed. However, there are no examples or details of who those partners are and the purposes for which CAD data would be shared.

e. Outstanding Questions That Must be Addressed in the Final SIR:

- Does the CAD system itself store data? If so, what data and for how long? Who can access that data?
- Who are SFD's data sharing partners? For what purpose is data shared with them?

f. Recommendations for Regulation:

Depending on the answer to the question regarding if the CAD system itself stores data, appropriate data protections may be needed as described above. SFD should adopt a clear policy requiring deletion of CAD data no longer needed. In addition, depending on how data is shared, SFD should adopt a policy that clearly limits what for what purposes CAD data would be shared, and with what entities.

3. 911 Logging Recorder – SPD

Background

The NICE 911 logging recorder is a technology used by SPD to audio-record all telephone calls to SPD's 9-1-1 communications center and all radio traffic between dispatchers and patrol officers. The stated purpose of the 9-1-1 Logging Recorder is to allow SPD to provide evidence to officers and detectives who investigate crimes and the prosecutors who prosecute offenders. These recordings also provide transparency and accountability for SPD, as they record in real time the interactions between 9-1-1 call takers and callers, and the radio traffic between 9-1-1 dispatchers and police officers. The NICE system also supports the 9-1-1 center's mission of quickly determining the nature of the call and getting the caller the assistance they need as quickly as possible with high quality, consistent and professional services.

Concerns include lack of clarity surrounding data retention schedules and data sharing with third parties.

a. Concerns

- *Lack of clarity on data retention.* Section 4.2 of the SIR states: "Recordings

requested for law enforcement and public disclosure are downloaded and maintained for the retention period related to the incident type." Similar to other technologies noted above, it is unclear whether the 9-1-1 system itself stores these recordings, or if they are stored on SPD's RMS. If the former, it should be made clear how the technology vendor accesses these recordings and for what purpose, if at all.

- *More clarity needed on data sharing with third parties.* There are no details or examples of the "discrete pieces of data" that are shared outside entities and individuals as referenced in Section 6.0 of the SIR.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What is SPD's data retention schedule for data stored in the NICE system, if any?
- What "discrete pieces of data" does SPD share with third parties?

c. Recommendations for Regulation:

SPD should adopt a clear policy requiring deletion of data no longer needed. In addition, depending on how data is shared, SPD should adopt a policy that clearly limits what for what purposes data would be shared, and with what entities.

IV. Current Diversion Technology Group – Seattle City Light

The technologies in this group—the Check Meter device (SensorLink TMS), the SensorLink Amp Fork, and the Binoculars/Spotting Scope raise civil liberties concerns primarily due to lack of explicit, written policies imposing meaningful restrictions on use of the technologies. While the purpose of the current diversion technologies appears clear—to assess whether suspected diversions of current have occurred and/or are continuing to occur—there are no explicit policies in the SIR detailing restrictions on what can and cannot be recorded by these technologies.

Below are short descriptions of the technologies, followed by concerns and recommendations.

Background

1. Check Meter Device (SensorLink TMS)

The SensorLink TMS device measures the amount of City Light-provided electrical energy flowing through the service-drop wire over time, digitally capturing the instantaneous information on the device for later retrieval by the Current Diversion Team via the use of a secure wireless protocol.

The stated purpose of use is to allow Seattle City Light to maintain the integrity of its electricity distribution system, to determine whether suspected current diversions have taken place, and to provide the valuation of the diverted energy to proper authorities for cost recovery.

2. SensorLink Amp Fork

The SensorLink Amp Fork is an electrical device mounted on an extensible pole allowing a circular clamp to be placed around the service-drop wire that provides electrical service to a customer location via its City Light-provided meter. The device then displays instantaneous readings of the amount of electrical energy (measured in amperage, or "amps") that the Current Diversion Team may compare against the readings displayed on the meter, allowing them to determine if current is presently being diverted.

The stated purpose of use of the Amp Fork is to allow Seattle City Light to assess whether suspected diversions of current have occurred and/or are continuing to occur. The Amp Fork allows the Utility to determine the valuation of the energy illegally diverted, which supports City Light's mission of recovering this value for ratepayers via a process called "back-billing."

3. Binoculars/Spotting Scope

The binoculars are standard, commercial-grade, unpowered binoculars. They do not contain any special enhancements requiring power (e.g., night-vision or video-recording capabilities). They are used to read a meter from a distance when the Current Diversion Team is otherwise unable to access physically the meter for the purpose of inspection upon suspected current diversion.

The stated purpose of the binoculars is to allow Seattle City Light to inspect meters and other implicated electrical infrastructure at a distance. If a determination of diversion is sustained, data may be used to respond to lawful requests from the proper law enforcement authorities for evidence for recovering the value of the diverted energy.

a. Concerns Regarding all Three Current Diversion Technologies

- *Absence of explicit, written policies imposing meaningful restrictions on use.* At the technology fair, a Seattle City Light representative stated that these technologies are used only for the purpose of checking current diversions, but could not confirm that Seattle City Light had clear, written policies for what data could and could not be recorded (e.g., an employee using the binoculars to view non-meter related information). The absence of written, specific policies increases the risk of unwarranted surveillance of individuals. There is also no mention in the SIRs of

specific data protection policies in place to safeguard the data (e.g., encryption, hashing, etc.).

- *Seattle City Light's records retention schedule is mentioned in the SIRs, but details about it are omitted.* It is unclear how long Seattle City Light retains data collected, and for what reason.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What enforceable policies, if any, apply to use of these three technologies?
- What is Seattle City Light's data retention schedule?

c. Recommendations for Regulation:

Seattle City Light must create clear, enforceable policies that, at a minimum:

- Define purpose of use for each technology and restrict its use to that purpose.
- Clearly state what clear data protection policies exist to safeguard stored data, if any, and ensure the deletion of data collected by the technology immediately after the relevant current diversion investigation has closed.

Thank you for your consideration, and please don't hesitate to contact me with questions.

Best,

Shankar Narayan
Technology and Liberty Project Director

Jennifer Lee
Technology and Liberty Project Advocate

15

Appendix 1: Benhammou Letter

16

City of Seattle

Acyclica

February 6th, 2015

RE: Acyclica data privacy standards

To whom it may concern:

The purpose of this letter is to provide information regarding the data privacy standards maintained by Acyclica. Acyclica is a traffic information company specializing in traffic congestion information management and analysis. Among the various types of data sources which make of Acyclica's traffic data portfolio including GPS probe data, video detection and inductive loops, Acyclica also utilizes our own patent-pending technology for the collection of Bluetooth and Wifi MAC addresses. MAC or Media Access Control addresses are unique 48-bit numbers which are associated with devices with Bluetooth and/or Wifi capable devices.

While MAC addresses themselves are inherently anonymous, Acyclica goes to great lengths to further obfuscate the original source of data through a combination of hashing and encryption to all but guarantee that information derived from the initial data bears no trace of any individual.

Acyclica's technology for collecting MAC addresses for congestion measurement operates by detecting nearby MAC addresses. The MAC addresses are then encrypted using GPG encryption before being transmitted to the cloud for processing. Encrypting the data prior to transmission means that no MAC addresses are ever written where they can be retrieved from the hardware. Once the data is received by our servers, the data is further anonymized using a SHA-256 algorithm which makes the raw MAC address nearly impossible to decipher from the hashed output. Furthermore, any customer seeking to download data for further investigation or integration through our API can only ever view the hashed MAC address.

Acyclica occasionally provides data to partners to help enhance the quality of congestion information. The information which is provided to such partners is received through API calls which only return aggregated information about traffic data over a given period such as the average travel-time over a 5-minute period. Aggregating the data provides a final layer of anonymization by reporting on the collective trend of all vehicles rather than the specific behavior of a single vehicle.

As always questions, comments and concerns are welcome. Please do let me know if we can provide further clarity and transparency on our internal operations with regards to data processing and privacy standards. We take the privacy of the public very seriously and always treat our customers and the data with the utmost respect.

Regards,

Daniel Benhammou
President
Acyclica Inc.

Appendix H: Comment Analysis Methodology

Overview

The approach to comment analysis includes combination of qualitative and quantitative methods. A basic qualitative text analysis of the comments received, and a subsequent comparative analysis of results, were validated against quantitative results. Each comment was analyzed in the following ways, to observe trends and confirm conclusions:

1. Analyzed collectively, as a whole, with all other comments received
2. Analyzed by technology
3. Analyzed by technology and question

A summary of findings are included in Appendix B: Public Comment Demographics and Analysis. All comments received are included in Appendix E: All Individual Comments Received.

Background on Methodological Framework

A modified Framework Methodology was used for qualitative analysis of the comments received, which "*…approaches [that] identify commonalities and differences in qualitative data, before focusing on relationships between different parts of the data, thereby seeking to draw descriptive and/or explanatory conclusions clustered around themes" (Gale, N.K., et.al, 2013).* Framework Methodology is a coding process which includes both inductive and deductive approaches to qualitative analysis.

The goal is to classify the subject data so that it can be meaningfully compared with other elements of the data and help inform decision-making. Framework Methodology is "not designed to be representative of a wider population, but purposive to capture diversity around a phenomenon" (*Gale, N.K., et.al, 2013).*

Methodology

Step One: Prepare Data

1. Compile data received.
    a. Daily collection and maintenance of 2 primary datasets.
        i. Master dataset: a record of all raw comments received, questions generated at public meetings, and demographic information collected from all methods of submission.
        ii. Comment analysis dataset: the dataset used for comment analysis that contains coded data and the qualitative codebook. The codebook contains the qualitative codes used for analysis and their definitions.
2. Clean the compiled data.
    a. Ensure data is as consistent and complete as possible. Remove special characters for machine readability and analysis.
    b. Comments submitted through SurveyMonkey for "General Surveillance"

remained in the "General Surveillance" category for the analysis, regardless of content of the comment. Comments on surveillance generally, generated at public meetings, were categorized as such.

c. Filter data by technology for inclusion in individual SIRs.

Step Two: Conduct Qualitative Analysis Using Framework Methodology

1. Become familiar with the structure and content of the data. This occurred daily compilation and cleaning of the data in step one.
2. Individually and collaboratively code the comments received, and identify emergent themes.
   I. Begin with deductive coding by developing pre-defined codes derived from the prescribed survey and small group facilitator questions and responses.
   II. Use clean data, as outlined in Data Cleaning section above, to inductively code comments.
      A. Each coder individually reviews the comments and independently codes them.
      B. Coders compare and discuss codes, subcodes, and broad themes that emerge.
      C. Qualitative codes are added as a new field (or series of fields) into the Comments dataset to derive greater insight into themes, and provide increased opportunity for visualizing findings.
   III. Develop the analytical framework.
      A. Coders discuss codes, sub-codes, and broad themes that emerge, until codes are agreed upon by all parties.
      B. Codes are grouped into larger categories or themes.
      C. The codes are be documented and defined in the codebook.
   IV. Apply the framework to code the remainder of the comments received.
   V. Interpret the data by identifying differences and map relationships between codes and themes, using R and Tableau.

Step Three: Conduct Quantitative Analysis

1. Identify frequency of qualitative codes for each technology overall, by questions, or by themes:
   I. Analyze results for single word codes.
   II. Analyze results for word pair codes (for context).
2. Identify the most commonly used words and word pairs (most common and least common) for all comments received.
   I. Compare results with qualitative code frequencies and use to validate codes.
   II. Create network graph to identify relationships and frequencies between

words used in comments submitted. Use this graph to validate analysis and themes.

3. Extract CSVs of single word codes, word pair codes, and word pairs in text of the comments, as well as the corresponding frequencies for generating visualizations in Tableau.

Step Four: Summarization

1. Visualize themes and codes in Tableau. Use call out quotes to provide context and tone.
2. Included summary information and analysis in the appendices of each SIR.

Appendix I: Supporting Policy Documentation

Appendix J: CTO Notification of Surveillance Technology

Thank you for your department's efforts to comply with the new Surveillance Ordinance, including a review of your existing technologies to determine which may be subject to the Ordinance. I recognize this was a significant investment of time by your staff; their efforts are helping to build Council and public trust in how the City collects and uses data.

As required by the Ordinance (SMC 14.18.020.D), this is formal notice that the technologies listed below will require review and approval by City Council to remain in use. This list was determined through a process outlined in the Ordinance and was submitted at the end of last year for review to the Mayor's Office and City Council.

The first technology on the list below must be submitted for review by March 31, 2018, with one additional technology submitted for review at the end of each month after that. The City's Privacy Team has been tasked with assisting you and your staff with the completion of this process and has already begun working with your designated department team members to provide direction about the Surveillance Impact Report completion process.

Please let me know if you have any questions.

Thank you,
Michael Mattmiller

Technology	Description	Proposed Review Order
Binoculars/Spotting Scope	The spotting scope is used to read meters from a distance when direct access to the meter is obstructed. Scopes are used by SCL's Current Diversion team to conduct investigations. Use of this technology may occur without informing a domicile's resident(s).	1
SensorLink Amp Fork	The SensorLink Amp Fork is used by SCL's Current Diversion team to measure the load on line-side entrance conductors, allowing SCL to determine the total amount of power being consumed at a service location. This tool provides an instantaneous reading to the group conducting the investigation. Use of this technology may occur without informing a domicile's resident(s).	2
Check Meter Device	This device measures the total amount of power being consumed at a service location where current diversion is confirmed or suspected. The device is set at the transformer and is used when a prolonged reading is desired by the Current Diversion team. Use of this technology may occur without informing a domicile's resident(s).	3

City of Seattle

2019 Surveillance Impact Report

Current Diversion Team: SensorLink Amp Fork

Seattle City Light

City of Seattle

Table of Contents

Submitting Department Memo 3
Surveillance Impact Report ("SIR") overview 7
Privacy Impact Assessment 8
Financial Information 19
Expertise and References 21
Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet 22
Privacy and Civil Liberties Assessment 36
CTO Response 42
Appendix A: Glossary 48
Appendix B: Meeting Notice(s) 50
Appendix C: Meeting Sign-in Sheet(s) 58
Appendix D: Department of Neighborhood Focus Group Notes 83
Appendix E: All Comments Received from Members of the Public 115
Appendix F: Department Responses to Public Inquiries 123
Appendix G: Letters from Organizations or Commissions 125
Appendix H: Comment Analysis Methodology 149
Appendix I: Supporting Policy Documentation 152
Appendix J: CTO Notification of Surveillance Technology 153

City of Seattle

Submitting Department Memo

Seattle City Light

MEMO

APRIL 16, 2019

TO
Seattle City Council

FROM
Julie Moore, Public Information Officer

SUBJECT
Summary of Surveillance Impact Reports for Three Current Diversion Detection Technologies

---

Seattle City Light's three current diversion detection technologies are undergoing review pursuant to Seattle Municipal Code, Chapter 14.18, *Acquisition and Use of Surveillance Technologies*.

The utility's Current Diversion Team (CDT) is responsible for investigating when electricity is being used but unaccounted for by City Light's billing system, and hence, not paid for. The three technologies City Light's CDT employs are:

1. Standard, commercial-grade, unpowered binoculars.
2. The SensorLink Ampstik.
3. The SensorLink Transformer Meter System.

Formal policies and procedures governing current diversion activity are described in City Light's Department Policy and Procedure (DPP) P III-416, *Current Diversion*. The CDT manager is responsible for ensuring City Light staff comply with the DPP and all existing rules.

TECHNOLOGIES

The utility's CDT members are the only staff who use the three technologies to investigate current diversion, and always upon preexisting and/or reported suspicion and with the approval of the current diversion coordinator. Suspicion of current diversion can take a variety of forms, such as a neighbor's report of questionable circumstances, a meter reader's observation of a tampered meter, or a billing specialist's observation of unusual or zero consumption.

CDT members who investigate potential current diversions drive standard City Light-marked vehicles and can be identified by their City Light ID badge and a hard hat.

1) BINOCULARS

When distance is a barrier to close physical inspection, CDT members may use binoculars to examine meters in assessing if current diversion is taking place. Binoculars may also be used to determine if potentially dangerous alterations to City Light's electrical infrastructure exist. The binoculars do not collect data, and do not contain any special enhancements requiring power (e.g., night vision, video-recording capabilities). Data derived from observations via CDT binoculars are accessible only by CDT members.

When used, CDT members use the binoculars for approximately one minute at a time. CDT members view locations that are in public view and the binoculars do not digitally record anything. Furthermore, the CDT only investigates specific meters and other implicated electrical equipment where current diversion is suspected. Therefore, the risk of staff inadvertently capturing data related to other customers is extremely low.

Data obtained by means of binoculars—which consist of notes made by staff based on their binocular-facilitated observations—are stored in a secure folder on City Light's digital network drive. The data, as well as overall incident reports, are accessible only by CDT members and the current diversion coordinator. Data will be retained per City Light records retention schedules. The current diversion coordinator has responsibility for ensuring compliance with data retention requirements.

The limited number of binoculars and of CDT members makes the routine tracking of this equipment relatively straight forward. Binoculars are issued to CDT members and are stored in their official vehicles. These vehicles are operated, locked, and stored in accordance with utility security procedures.

2) SENSORLINK AMPSTIK

The SensorLink Ampstik ("Ampstik") is a hand-held tool used to detect instantaneous current flow through a service drop. Specifically, it is an electrical device mounted on an extensible pole (up to 40' to 50') that allows a circular clamp to be placed around a service-drop wire. The wire is the same wire that provides electrical service to a customer location via a City Light-provided meter. The device then displays instantaneous readings of the amount of electrical energy flow as measured in amperage or "amps." The CDT member may then compare those reads against the readings displayed on the electric meter, allowing staff to determine if current is presently being diverted. Because the device delivers a point-in-time reading, it is deployed by hand for approximately 10 minutes at a time. The Ampstik ultimately allows the utility to determine the valuation of the energy illegally diverted, which supports City Light's mission of recovering this value for the ratepayers via a process called "back-billing."

Risk of inadvertent or improper collection is low for two reasons. First, the CDT only investigates specific, metered locations previously identified as sites of suspected current diversion. Second, Ampstik devices are used only on those service-drop lines that are delivering electrical service to the suspected location.

The limited number of this equipment and of CDT members makes the routine tracking of the Ampstik devices relatively straight forward. Ampstiks are issued to CDT members and are stored in their official vehicles. These vehicles are operated, locked, and stored in accordance with

utility security procedures. City Light records Ampstik serial numbers and their assignments to CDT members, along with their deployment status.

CDT members who are journey-level electrical workers trained to use Ampstiks may collect and access this data. This data may be accessed only by CDT staff and the current diversion coordinator, and are stored in a secure folder on City Light's digital network drive. Data will be retained per City Light records retention schedules. The current diversion coordinator has responsibility for ensuring compliance with data retention requirements.

3) SENSORLINK TRANSFORMER METER SYSTEM (TMS)

The SensorLink Transformer Meter System ("TMS") is a device that measures the amount of electrical energy flowing through a service-drop wire over time. It digitally captures the instantaneous information for later retrieval by the CDT member(s) via a secure wireless protocol. TMS devices are housed in a black, weatherproof box of approximately four square inches, and have an external City Light inventory control number so that line workers know what function the device serves. These devices are typically installed on an electric pole adjacent to a transformer for a period of one week to one month depending on the specific case needs and crew availability. These units ultimately allow the utility to determine the valuation of the energy illegally diverted, which supports City Light's mission of recovering this value for the ratepayers via a process called "back-billing."

The CDT owns six TMS units, which are deployed on the basis of case number and need. Deployment level on a given case can vary from none (zero) to all (six). Once a case is properly opened, CDT members may check the devices out without prior additional authorization, although in nearly all circumstances, the current diversion coordinator is aware of deployment due to position responsibilities. City Light records TMS serial numbers and their assignments to CDT members, along with their deployment status.

Risk of inadvertent or improper collection is low for two reasons. First, the CDT member only investigates specific, metered locations previously identified and properly documented as a site of suspected current diversion. Second, TMS devices are used only on those service-drop lines that are delivering electrical service to a suspected location.

The SensorLink TMS device is not "visible to the public" in any conventional sense, although to a trained eye, it may be visible near a transformer on an electrical pole. CDT members, who are journey-level electrical workers trained in the placement, use, and removal of the device, may collect the data. The quantitative data – accumulated consumption (in kilowatt hours), average volts (current strength), average amps (current flow), and interval consumption (in kilowatt hours per a pre-defined time unit) – are accessed by CDT members remotely using a secure radio protocol and a specific, password-protected software program.

Data obtained by means of the TMS are stored in a secure folder on City Light's digital network drive, accessible only by CDT members and City Light management. Data stored in the TMS are deleted after its retrieval by the CDT staff and/or upon its removal from the electrical pole. In other words, no data remains in the TMS once its use for a specific current diversion case has been completed. Data will be retained per City Light record retention schedules. The current

diversion coordinator has responsibility for ensuring compliance with data retention requirements.

DATA SHARING & AUDITING

Data collected from the use of the three technologies may be shared with other government staff in two instances. When a determination is made that current diversion has taken place, a valuation of the stolen energy is shared with City Light's billing division so that the utility can "back-bill" and recover the diverted energy costs from the appropriate customer. Also, data is shared with police investigators and/or prosecutors for the purposes of law enforcement or legal action in complex or aggravated cases (e.g., when large sums of energy have been diverted/stolen, or where there is a safety risk to the public). This policy is formally laid out in City Light's DPP 500 P III-416. In both instances, data sharing is required for City Light to recover stolen energy costs. In the latter case (i.e., information sharing with police investigators) data sharing may also be required in order to protect public safety, since unauthorized alterations to the electrical system can pose a serious, and at times, lethal danger to the public.

To safeguard CDT data, the current diversion coordinator will request Seattle IT to provide audit data, so that City Light may complete an audit to ensure that access rights are assigned only to authorized staff.

IMPORTANCE OF TECHNOLOGIES – SUPPORTING CITY LIGHT'S MISSION

One of City Light's core missions as an electric utility is to recoup the costs of the energy provided to customers. This is required by Seattle Municipal Code 21.49.100, *Application and Contract Provisions*. Additionally, as a general rule the Washington State Constitution's Article VIII, Section 7 prohibits the gifting of public funds. Since all three technologies enable City Light to recover unaccounted for electricity costs, they contribute to the department's mission of being legally compliant. Translated into monetary value, the utility recovered over $1.6 million in 2017 using these technologies. This would otherwise be a substantial financial loss for the City.

City of Seattle

Surveillance Impact Report ("SIR") overview

About the Surveillance Ordinance

The Seattle City Council passed Ordinance 125376, also referred to as the "Surveillance Ordinance," on September 1, 2017. SMC 14.18.020.b.1 charges the City's executive with developing a process to identify surveillance technologies subject to the ordinance. Seattle it, on behalf of the executive, developed and implemented a process through which a privacy and surveillance review is completed prior to the acquisition of new technologies. This requirement, and the criteria used in the review process, are documented in Seattle it policy pr-02, the "surveillance policy".

How this Document is Completed

This document is completed by the requesting department staff, support and coordinated by the Seattle information technology department ("Seattle it"). As Seattle it and department staff complete the document, they should keep the following in mind.

1. Responses to questions should be in the text or check boxes only; all other information (questions, descriptions, etc.) Should **not** be edited by the department staff completing this document.
2. All content in this report will be available externally to the public. With this in mind, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.

Surveillance Ordinance Review Process

The following is a high-level outline of the complete SIR review process.

Upcoming for Review	Initial Draft	Open Comment Period	Final Draft	Working Group	Council Review
The technology is upcoming for review, but the department has not begun drafting the surveillance impact report (SIR).	Work on the initial draft of the SIR is currently underway.	The initial draft of the SIR and supporting materials have been released for public review and comment. During this time, one or more public meetings will take place to solicit feedback.	During this stage the SIR, including collection of all public comments related to the specific technology, is being compiled and finalized.	The surveillance advisory working group will review each SIR's final draft and complete a civil liberties and privacy assessment, which will then be included with the SIR and submitted to Council.	City Council will decide on the use of the surveillance technology, by full Council vote.

Privacy Impact Assessment

Purpose

A Privacy Impact Assessment ("PIA") is a method for collecting and documenting detailed information collected in order to conduct an in-depth privacy review of a program or project. A PIA asks questions about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. It also requests information about policies, training and documentation that govern use of the technology. The PIA responses are used to determine privacy risks associated with a project and mitigations that may reduce some or all of those risks. In the interests of transparency about data collection and management, the City of Seattle has committed to publishing all PIAs on an outward facing website for public access.

When is a Privacy Impact Assessment Required?

A PIA may be required in two circumstances.

1. When a project, technology, or other review has been flagged as having a high privacy risk.
2. When a technology is required to complete the surveillance impact report process. This is one deliverable that comprises the report.

1.0 Abstract

1.1 Please provide a brief description (one paragraph) of the purpose and proposed use of the project/technology.

Seattle City Light's ("City Light") Current Diversion Team ("CDT") consists of a group of approximately five journey-level engineers who are dispatched to collect data to attempt to determine whether a suspected diversion of current (i.e., alterations to the City Light-owned electrical system by a third-party in order to consume electric power without its being registered by the City Light meter installed for that purpose) has in fact taken place. In support of this mission, the CDT crew uses a hand-held tool to detect instantaneous current flow levels in amps through a service drop ("Amp fork" or "Ampstik"). If a determination of diversion is sustained, data may be used to respond to lawful requests from the proper law enforcement authorities for evidence for recovering the value of the stolen energy.

In conjunction with this technology, two others – binoculars and the SensorLink TMS (check-meter device) – are used by the CDT. As a result, City Light's three retroactive Surveillance Impact Reports ("SIRs") may be, at times, duplicative, so that each report contains the necessary information.

1.2 Explain the reason the project/technology is being created or updated and why the PIA is required.

This technology is used in furtherance of a mission supported by ordinance (SMC 21.49.100, requiring recovery of payment for electric services provided) and an existing City Light department policy procedure (DPP 500 P III-416, hereafter "DPP"). City Light provided the information in the Privacy Impact Assessment to fulfill requirements of the Surveillance Ordinance and so that the public may understand the nature of the CDT and the tools that are essential to its carrying out its mission for the benefit of ratepayers. The Ampstik tool provides data to the CDT crew member for manual recording and without automatic or digital storage of these data.

2.0 Project / Technology Overview

Provide an overview of the project or technology. The overview gives the context and background necessary to understand the purpose, mission and justification for the project / technology proposed

2.1 Describe the benefits of the project/technology.

As described in Section 1, the CDT utilizes Ampstik in order to assess whether suspected diversions of current have occurred and/or are continuing to occur. The Ampstik allows the Utility to determine the valuation of the energy illegally diverted, which supports City Light's mission of recovering this value for the ratepayers via a process called "back-billing."

2.2 Provide any data or research demonstrating anticipated benefits.

In 2017, the CDT's operations, via the use of Ampstik (in combination with the two other technologies under review), City Light recovered $1.6 million. This would otherwise remain a substantial financial loss to the Utility. City Light implemented Ampstik as an efficient and accurate means of assessing amounts of current being diverted after CDT staff studied their use by Portland General Electric, the electric energy provider for the Portland, Oregon area.

2.3 Describe the technology involved.

Ampstik is an electrical device mounted on an extensible pole (up to 40' to 50') which allows a circular clamp to be placed around the service-drop wire that provides electrical service to a customer location via its City Light-provided meter. The device then displays instantaneous readings of the amount of electrical energy (measured in amperage, or "amps") that the CDT may compare against the readings displayed on the meter, allowing them to determine if current is presently being diverted.

2.4 Describe how the project or use of technology relates to the department's mission.

The Ampstik device allows City Light to maintain the integrity of its electricity distribution system, to determine whether suspected current diversions have taken place, and to provide the valuation of the diverted energy to proper authorities for cost recovery. These are supported by ordinance (SMC 21.49.100) and Department Policy and Procedure (DPP). Additionally, provisions of the Washington State Constitution forbid any gift of public funds (Art. VIII, Sec. 7), so this program is central to the public mission of the Utility.

2.5 Who will be involved with the deployment and use of the project / technology?

The CDT members are the only City Light staff who deploy the Ampstik, and always upon pre-existing and/or reported suspicion of current diversion (e.g., neighbor report, unusual or no energy consumption detected upon a routine meter reading by City Light, visual observation of tampered-with meter or other City Light-owned or -maintained electrical equipment). Data derived from the technology are accessible only by the CDT team.

3.0 Use Governance

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities contracting with the City are bound by restrictions specified in the surveillance ordinance and privacy principles and must provide written procedures for how the entity will comply with any restrictions identified.

3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

The limited number of this equipment and of CDT members makes the routine tracking of the Ampstik devices relatively straight-forward. Ampstiks are issued to CDT members, and stored in their official vehicles. These vehicles are operated, locked, and stored in accordance with Utility security procedures. Ampstiks' serial numbers are recorded and the CDT member to whom they are assigned, as well as their deployment status, are logged.

3.2 List the legal standards or conditions, if any, that must be met before the project / technology is used.

Routine deployment in support of making an internal determination as to current diversion is not subject to additional prior legal authorization. The formal rule regarding CDT operations is contained in Seattle City Light Department Policy & Procedure DPP 500 P III-416.

3.3 Describe the policies and training required of all personnel operating the project / technology, and who has access to ensure compliance with use and management policies.

In addition to routine privacy and security training undergone by all City Light employees per Seattle IT policy, the CDT manager has responsibility for ensuring compliance with all existing rules and procedures.

4.0 Data Collection and Use

4.1 Provide details about what information is being collected from sources other than an individual, including other IT systems, systems of record, commercial data aggregators, publicly available data and/or other City departments.

No additional information is collected by the CDT in making its determinations, nor is any third-party or other aggregation taking place.

4.2 What measures are in place to minimize inadvertent or improper collection of data?

Risk of inadvertent or improper collection is low for two reasons. First, the CDT only investigates specific, metered locations previously identified as sites of suspected current diversion. And second, Ampstik devices are used only on those service-drop lines that are delivering electrical service to the suspected location.

4.3 How and when will the project / technology be deployed or used? By whom? Who will determine when the project / technology is deployed and used?

Ampstik devices are used throughout the year based on suspected cases of current diversion, by the CDT staff and with the approval of the Current Diversion Coordinator. As mentioned above, these can be triggered in several ways, for example neighbor report to the customer service bureau or other City Light representatives; recognition by billing specialists of highly out-of-the-ordinary meter readings; or observations by meter and other crews of tampering with metering or other electrical service provision equipment.

4.4 How often will the technology be in operation?

Because Ampstiks deliver a point-in-time reading to CDT staff, they are deployed by hand for approximately ten minutes at a time, only when suspected diversion cases occur.

4.5 What is the permanence of the installation? Is it installed permanently, or temporarily?

Ampstiks are held in place by CDT members temporarily for a period of time up to ten minutes.

4.6 Is a physical object collecting data or images visible to the public? What are the markings to indicate that it is in use? What signage is used to determine department ownership and contact information?

Ampstiks are not installed, as they are used by hand for up to ten minutes at a time. CDT staff who operate them are deployed in standard City Light-marked vehicles and wear identifying gear. No special notification is made to the public. Providing notification of Ampstik use to the public may risk defeating its purpose of detecting a diversion of current on a single suspected service-drop.

4.7 How will data that is collected be accessed and by whom?

CDT members, who are journey-level electrical workers trained in the use of the Ampstik, may collect and access this data. Additionally, the Current Diversion Coordinator may access the data.

4.8 If operated or used by another entity on behalf of the City, provide details about access, and applicable protocols.

City Light is the only entity operating or using the technology.

4.9 What are acceptable reasons for access to the equipment and/or data collected?

The Ampstik is used only to make determinations about whether a current diversion is likely to be taking place, and the device is used for up to ten minutes at a time. Once collected, the data may be accessed for purposes of continuing the investigation into whether current diversion has taken place; these data are, again, accessed only by the CDT team.

4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

Data obtained by means of the Ampstik are stored in a private folder on City Light's digital file locations. The data, as well as incident reports, are accessible only by CDT members and its Current Diversion Coordinator.

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

Data obtained by means of the Ampstik device are stored in a private folder on City Light's digital file locations, accessible only by CDT members and SCL management.

5.2 How will the owner allow for departmental and other entities, to audit for compliance with legal deletion requirements?

City Light will make CDT file locations and staff available for properly authorized entities wishing to ensure compliance. Data will be retained per City Light records retention schedules.

5.3 What measures will be used to destroy improperly collected data?

To the extent permitted by the Washington State Public Disclosure Law, any improperly collected data will be deleted from City Light's digital file locations, and hard-copy documents will be destroyed.

5.4 which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

The Current Diversion Coordinator has responsibility for this function.

6.0 Data Sharing and Accuracy

6.1 Which entity or entities inside and external to the City will be data sharing partners?

Data, or information derived from the data, may be shared with other parties in two instances, both of which are public entities. These are (1) when a determination is made that current diversion has taken place, in which case a valuation of the stolen energy is sent to the customer billing division of City Light for "back-billing" to the customer for cost recovery, and (2) when police investigators and/or prosecutors require evidence for further proceedings in complex or aggravated cases, as when large sums of energy have been diverted/stolen, or where there is a safety risk to the public.

6.2 Why is data sharing necessary?

In both cases, this is required for City Light to recoup stolen energy costs. In the second case (information sharing with police investigators) it may also be required to protect public safety, since unauthorized alterations to the electrical system can pose a serious and at times lethal danger to the public.

6.3 Are there any restrictions on non-City data use?

Yes ☒ No ☐

6.3.1 If you answered yes, provide a copy of the department's procedures and policies for ensuring compliance with these restrictions.

Data are collected and maintained for Seattle City Light use and may only be shared with outside entities for the purposes of law enforcement or legal action by the relevant jurisdictional authority. This policy is formally laid out in Seattle City Light Department Policy & Procedure DPP 500 P III-416.

6.4 How does the project/technology review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?

City Light anticipates no additional data-sharing, as the CDT's mission is fixed. Additional changes would require review the Current Diversion Coordinator. Law enforcement, as mentioned in 6.3, may request these data and findings but only pursuant to a subpoena or a request pursuant to the Public Disclosure Law (based upon probable cause, see RCW 42.56.335).

6.5 Explain how the project/technology checks the accuracy of the information collected. If accuracy is not checked, please explain why.

As the data come from the Ampstik device are designed to measure accurately in a scientific manner the amount of energy passing through it, these data are not checked further, beyond regular maintenance of the equipment to ensure proper functioning.

6.6 Describe any procedures that allow individuals to access their information and correct inaccurate or erroneous information.

Upon a proper finding of current diversion, customers are back-billed to recoup these losses. DPP 500 P III-416 provides that "all customers shall receive uniform consideration and courtesy in all matters involving actual or suspected current diversion." Customers are notified of findings and offered opportunities to respond and/or object.

7.0 Legal Obligations, Risks and Compliance

7.1 What specific legal authorities and/or agreements permit and define the collection of information by the project/technology?

One of City Light's core missions as an electric utility is to recoup the costs of the energy it provides to its customers as part of its operations (as required in SMC 21.49.100 and the general rule against gifts of public funds found in the Washington State Constitution at Article VIII, Section 7).

7.2 Describe what privacy training is provided to users either generally or specifically relevant to the project/technology.

CDT members are trained in how to store information in private folders on City Light's digital storage locations, in addition to the general privacy and security training required by Seattle IT.

7.3 Given the specific data elements collected, describe the privacy risks identified and for each risk, explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

The Ampstik is designed only to measure specific, individual service-drops directly linking the customer suspected of current diversion to City Light's electric services. As such, there is no additional privacy risk present.

7.4 Is there any aspect of the project/technology that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?

City Light has considered but does not anticipate such objections, since the data collected are used for one purpose only, and are not shared for any other reason.

8.0 Monitoring and Enforcement

8.1 Describe how the project/technology maintains a record of any disclosures outside of the department.

When a report is sent to law enforcement, it does not include power consumption information. Law enforcement then relies upon the Public Disclosure Law to request power records, if they decide to do so, and City Light would provide that information pursuant to that request. This may be effectuated either by a subpoena or by a request from law enforcement based upon probable cause and pursuant to the Washington Public Disclosure Law (see RCW 42.56.335).

8.2 What auditing measures are in place to safeguard the information, and policies that pertain to them, as well as who has access to the audit data? Explain whether the project/technology conducts self-audits, third party audits or reviews.

To safeguard the information, the Current Diversion Coordinator will request Seattle IT to provide audit data, so that City Light may complete an audit to ensure that access rights are assigned only those who should have access to the shared drive containing customer/current-diversion data.

Financial Information

Purpose

This section provides a description of the fiscal impact of the surveillance technology, as required by the surveillance ordinance.

1.0 Fiscal Impact

Provide a description of the fiscal impact of the project/technology by answering the questions below.

1.1 Current or potential sources of funding: initial acquisition costs.

Current ☒ potential ☐

Date of initial acquisition	Date of go live	Direct initial acquisition cost	Professional services for acquisition	Other acquisition costs	Initial acquisition funding source
2013 & 2015	Same	$4,400	None	None	City Light

Notes:

City Light initially obtained the Ampstik device technology in 2013. A reorder was placed in 2015. City Light now owns four such devices.

1.2 Current or potential sources of funding: on-going operating costs, including maintenance, licensing, personnel, legal/compliance use auditing, data retention and security costs.

Current ☒ potential ☐

Annual maintenance and licensing	Legal/compliance, audit, data retention and other security costs	Department overhead	IT overhead	Annual funding source
None	See notes	None	None	City Light

Notes:

Compliance and audit costs are internal, as detailed above, and are therefore part of Current Diversion Team's normal workflow and procedures. There are no costs directly related to the "use" or "maintenance" of the four Ampstik devices. Were there to arise a maintenance cost, it would be borne by City Light.

1.3 Cost savings potential through use of the technology

In 2017, through the use of the Current Diversion Team's three technologies – including the Ampstik – City Light was able to recover $1.6 million in stolen energy costs.

1.4 Current or potential sources of funding including subsidies or free products offered by vendors or governmental entities

None identified.

Expertise and References

Purpose

The following information is provided to ensure that Council has a group of experts to reference while reviewing the completed surveillance impact report ("SIR"). Any individuals or agencies referenced must be made aware ahead of publication that their information has been included. All materials must be available for Council to access or review, without requiring additional purchase or contract.

1.0 Other Government References

Please list any other government bodies that have implemented this technology and can speak to the implementation of this technology.

Agency, municipality, etc.	Primary contact	Description of current use
Portland General Electric	N/A	Same use as City Light

2.0 Academics, Consultants, and Other Experts

Please list any experts in the technology under consideration, or in the technical completion of the service or function the technology is responsible for.

Agency, municipality, etc.	Primary contact	Description of current use
N/A	N/A	N/A

3.0 White Papers or Other Documents

Please list any authoritive publication, report or guide that is relevant to the use of this technology or this type of technology.

Title	Publication	Link
SensorLink Ampstik Specification Sheet	Ampstik%20Datasheet%20V02.pdf	Weblink to PDF document

Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet

Purpose

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit ("RET") in order to:

- Provide a framework for the mindful completion of the SIR in a way that is sensitive to the historic exclusion of vulnerable and historically underrepresented communities. Particularly, to inform the public engagement efforts departments will complete as part of the surveillance impact report.
- Highlight and mitigate any impacts on racial equity from the adoption and the use of the technology.
- Highlight and mitigate any disparate impacts on individuals or vulnerable communities.
- Fulfill the public engagement requirements of the surveillance impact report.

Adaptation of the RET for Surveillance Impact Reports

The RET was adapted for the specific use by the Seattle Information Technology Departments' ("Seattle IT") Privacy Team, the Office of Civil Rights ("OCR"), and Change Team members from Seattle IT, Seattle City Light, Seattle Fire Department, Seattle Police Department, and Seattle Department of Transportation.

Racial Equity Toolkit Overview

The vision of the Seattle Race and Social Justice Initiative ("RSJI") is to eliminate racial inequity in the community. To do this requires ending individual racism, institutional racism and structural racism. The RET lays out a process and a set of questions to guide the development, implementation and evaluation of policies, initiatives, programs, and budget issues to address the impacts on racial equity.

1.0 Set Outcomes

1.1. Seattle City Council has defined the following inclusion criteria in the surveillance ordinance, and they serve as important touchstones for the risks departments are being asked to resolve and/or mitigate. Which of the following inclusion criteria apply to this technology?

☐ The technology disparately impacts disadvantaged groups.

☐ There is a high likelihood that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service.

☒ The technology collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection.

☐ The technology raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice.

1.2 What are the potential impacts on civil liberties through the implementation of this technology? How is the department mitigating these risks?

Because Ampstik, in conjunction with the other two diversion technologies being reviewed, are designed to measure electric current at one connection point assigned to one customer, no impacts on civil liberties are anticipated from the technologies themselves. At the same time, City Light is aware that the methods and procedures surrounding the use or installation of an otherwise non-offensive technology is just as important. For that reason, we ensure that our staff are clearly identified as Seattle City Light employees when in the field; there is no surreptitious operation in the field.

1.3 What are the risks for racial or ethnicity-based bias through each use or deployment of this technology? How is the department mitigating these risks?

Include a description of any issues that may arise such as algorithmic bias or the possibility for ethnic bias to emerge in people and/or system decision-making.

City Light is committed to equitable enforcement of all its legal mandates, in the same way that it is committed to equity in its provision of clean, affordable, and reliable power for its customers. City Light aims to ensure that the enforcement mechanisms similarly equitable, in that they should be not only unbiased but also equitably enforced. For that reason, City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible.

1.4 Where in the City is the technology used or deployed?

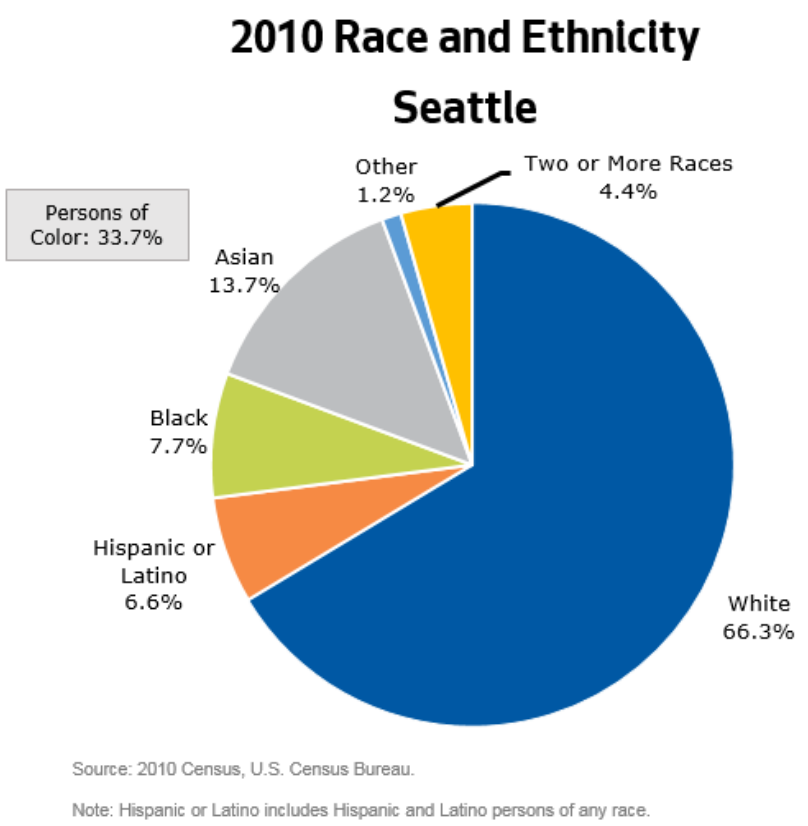
☒ all Seattle neighborhoods

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County.

If possible, please include any maps or visualizations of historical deployments / use.

Seattle City Light's service territory extends beyond the boundary of the City of Seattle. Other areas include: Burien, Lake Forest Park, Normandy Park, Renton, SeaTac, Shoreline, Tukwila, and areas of unincorporated King County.

1.4.1 What are the racial demographics of those living in this area or impacted by these issues?



1.4.2 How does the Department to ensure diverse neighborhoods, communities, or individuals are not specifically targeted through the use or deployment of this technology?

DPP 500 P III-416 provides that "all customers shall receive uniform consideration and courtesy in all matters involving actual or suspected current diversion." City Light aims to ensure that the enforcement mechanisms are equitable, in that they should be not only unbiased but also equitably enforced. For that reason, City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible.

1.5 How do decisions around data sharing have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

Data is collected for Seattle City Light use and may only be shared with outside entities for the purposes of law enforcement or legal action by the relevant jurisdictional authority. This policy is formally laid out in Seattle City Light Department Policy & Procedure DPP 500 P III-416. As stated previously, City Light aims to ensure that the enforcement mechanisms are equitable, in that they should be not only unbiased but also equitably enforced. For that reason, City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible.

1.6 How do decisions around data storage and retention have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

Data is maintained for Seattle City Light use and may only be shared with outside entities for the purposes of law enforcement or legal action by the relevant jurisdictional authority. This policy is formally laid out in Seattle City Light Department Policy & Procedure DPP 500 P III-416. As stated previously, City Light aims to ensure that the enforcement mechanisms are equitable, in that they should be not only unbiased but also equitably enforced. For that reason, City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible.

1.7 What are potential unintended consequences (both negative and positive potential impact)? What proactive steps can you can / have you taken to ensure these consequences do not occur.

One of City Light's core missions as an electric utility is to recoup the costs of the energy it provides to its customers as part of its operations (as required in SMC 21.49.100 and the general rule against gifts of public funds found in the Washington State Constitution at Article VIII, Section 7). Per DPP 500 P III-416,"all customers shall receive uniform consideration and courtesy in all matters involving actual or suspected current diversion." As stated previously, City Light aims to ensure that the enforcement mechanisms are equitable, in that they should be not only unbiased but also equitably enforced. For that reason, City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible.

2.0 Public Outreach

2.1 Organizations who received a personal invitation to participate.

Please include a list of all organizations specifically invited to provide feedback on this technology.

1. ACLU of Washington	2. Ethiopian Community Center	3. Planned Parenthood Votes Northwest and Hawaii
4. ACRS (Asian Counselling and Referral Service)	5. Faith Action Network	6. PROVAIL
7. API Chaya	8. Filipino Advisory Council (SPD)	9. Real Change
10. API Coalition of King County	11. Friends of Little Saigon	12. SCIPDA
13. API Coalition of Pierce County	14. Full Life Care	15. Seattle Japanese American Citizens League (JACL)
16. CAIR	17. Garinagu HounGua	18. Seattle Neighborhood Group
19. CARE	20. Helping Link	21. Senior Center of West Seattle
22. Central International District Business Improvement District	23. Horn of Africa	24. Seniors in Action
25. Church Council of Greater Seattle	26. International ImCDA	27. Somali Family Safety Task Force
28. City of Seattle Community Police Commission (CPC)	29. John T. Williams Organizing Committee	30. South East Effective Development
31. City of Seattle Community Technology Advisory Board	32. Kin On Community Health Care	33. South Park Information and Resource Center SPIARC
34. City of Seattle Human Rights Commission	35. Korean Advisory Council (SPD)	36. STEMPaths Innovation Network
37. Coalition for Refugees from Burma	38. Latina/o Bar Association of Washington	39. University of Washington Women's Center
40. Community Passageways	41. Latino Civic Alliance	42. United Indians of All Tribes Foundation
43. Council of American Islamic Relations - Washington	44. LELO (Legacy of Equality, Leadership, and Organizing)	45. Urban League
46. East African Advisory Council (SPD)	47. Literacy Source	48. Wallingford Boys & Girls Club
49. East African Community Services	50. Millionair Club Charity	51. Washington Association of Criminal Defense Lawyers
52. Education for All	53. Native American Advisory Council (SPD)	54. Washington Hall
55. El Centro de la Raza	56. Northwest Immigrant Rights Project	57. West African Community Council
58. Entre Hermanos	59. OneAmerica	60. YouthCare
61. US Transportation expertise	62. Local 27	63. Local 2898
64. (SPD) Demographic Advisory Council	65. South Seattle Crime Prevention Coalition (SSCPC)	66. CWAC
67. NAAC		

2.2 Additional Outreach Efforts

Department	Outreach Area	Description
ITD	Social Media Outreach Plan: Twitter	Directed Tweets and Posts related to Open Public Comment Period for Group 2 Technologies, as well as the BKL event.
SPD, SFD, OPCD, OCR, SPL, SDOT, SPR, SDCI, SCL, OLS, Seattle City Council	Social Media Outreach Plan: Twitter	Tweets and Retweets regarding Group 2 comment period and/or BKL event.
ITD	Press Release	Press release sent to several Seattle media outlets.
ITD	Ethnic Media Press Release	Press Release sent to specific ethnic media publications.
ITD	Social Media Outreach Plan: Facebook Event Post	Seattle IT paid for boosted Facebook posts for their BKL event.
ITD	CTAB	Presented and utilized the Community Technology Advisory Board (CTAB) network and listserv for engaging with interested members of the public
ITD	Blog	Wrote and published a Tech Talk blog post for Group 2 technologies, noting the open public comment period, BKL event, and links to the online survey/comment form.
ITD	Technology Videos	Seattle IT worked with the Seattle Channel to produce several short informational/high level introductory videos on group 2 technologies, which were posted on seattle.gov/privacy. And used at a number of Department of Neighborhoods-led focus groups.

2.3 Scheduled public meeting(s).

Meeting notes, sign-in sheets, all comments received, and questions from the public will be included in Appendix B, C, D, E, F, G, H and I. Comment analysis will be summarized in section 3.0 Public Comment Analysis.

Location	Bertha Knight Landes Room, 1st Floor City Hall 600 4th Avenue, Seattle, WA 98104
Time	February 27, 2018; 6 p.m. – 8 p.m.
Capacity	100+
Link to URL Invite	BKL Event Invitation

2.4 Scheduled focus Group Meeting(s)

Meeting 1

Community Engaged	Council on American-Islamic Relations - Washington (CAIR-WA)
Date	Thursday, February 21, 2019

Meeting 2

Community Engaged	Entre Hermanos
Date	Thursday, February 28, 2019

Meeting 3

Community Engaged	Byrd Barr Place
Date	Thursday, February 28, 2019

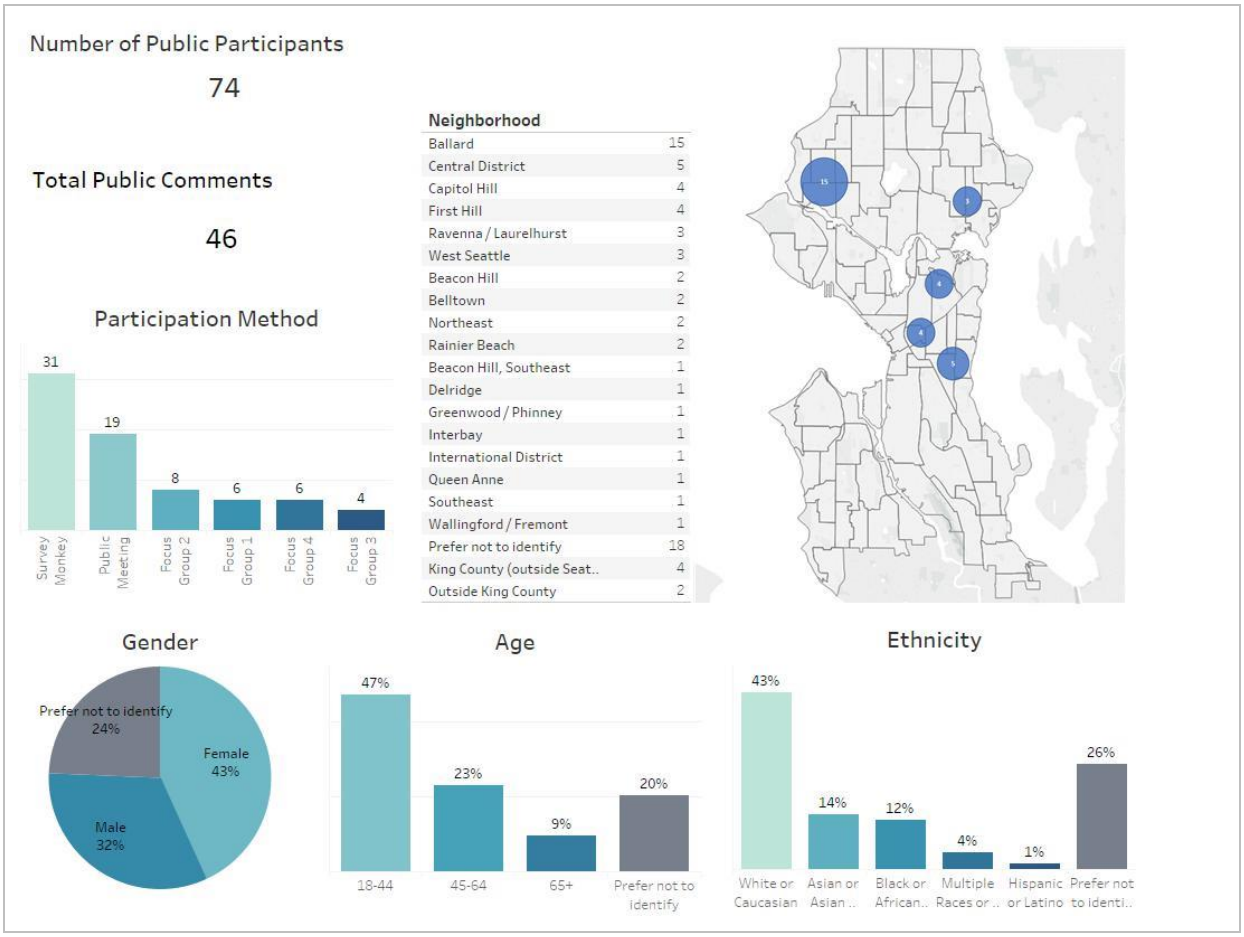
Meeting 4

Community Engaged	Friends of Little Saigon
Date	Wednesday, February 27, 2019

3.0 Public Comment Analysis

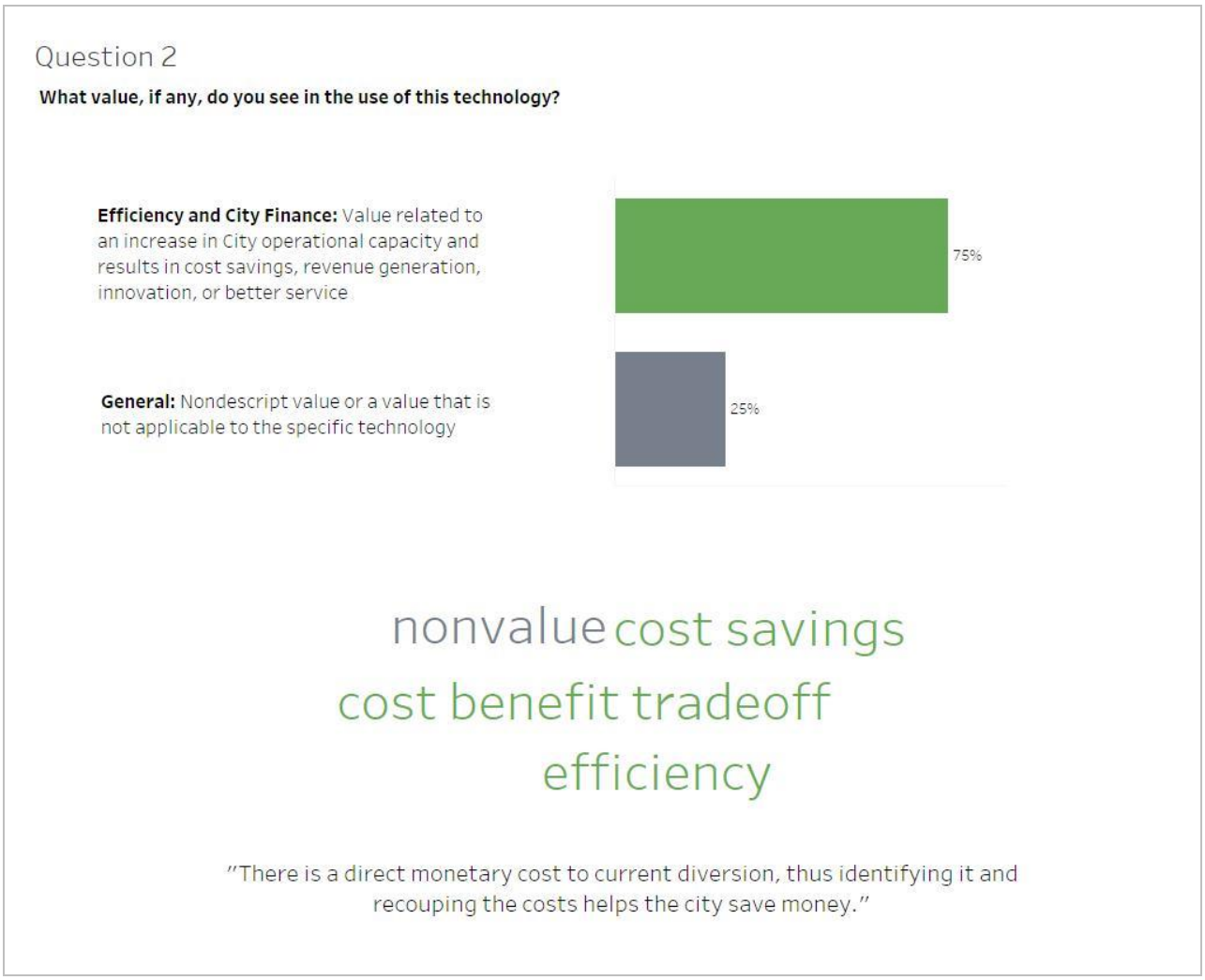
Please note, due to the nature of the comments received and the related purpose of the Seattle City Light technologies, this comment analysis reflects comments received for the SCL Binoculars/Spotting Scope, SensorLink Amp Fork, and Check Meter Device.

3.1 Summary of Response Volume



3.2 Question One: What concerns, if any, do you have about the use of this technology?

3.3 Question Two: What value, if any, do you see in the use of this technology?



3.4 Question Three: What do you want City leadership to consider about the use of this technology?

Question 3

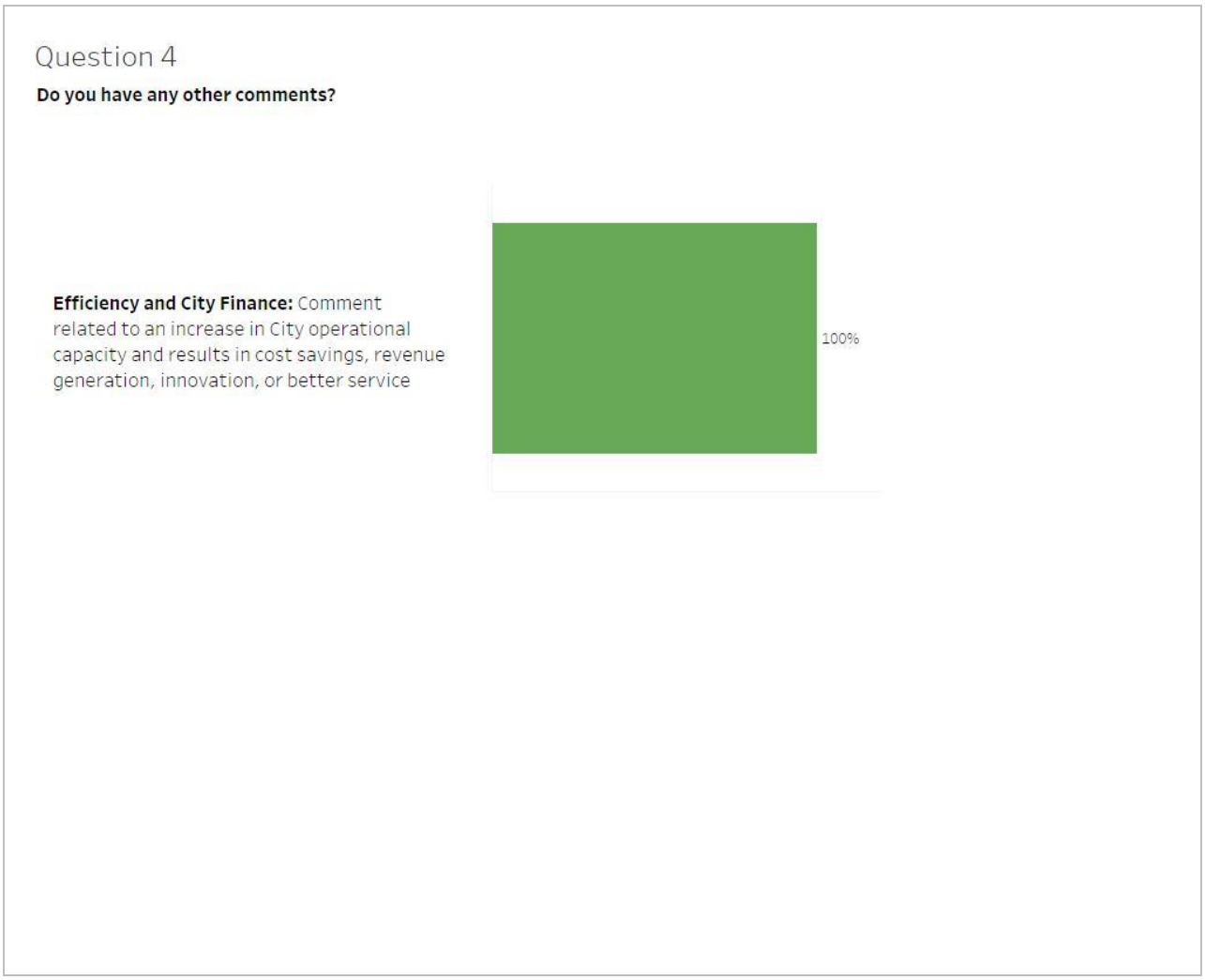
What do you want City leadership to consider about the use of this technology?

Increase policy, enforcement, and oversight: Recommendations related to department and City policy, oversight, accountability, transparency, audit, and policy enforcement.

oversight
reporting statisticscease use

"City leadership should specifically inquire as to what percentage of people/households that were enforcement locations would also be considered low-income. If that percentage is high, then that likely means SCL may cause people to be jailed for effectively being poor (and resourceful); and SCL may have inadequate support offerings for people who are low-income."

3.5 Question Four: Do you have any other comments?



4.0 Equity Annual Reporting

4.1 What metrics for this technology be reported to the CTO for the annual equity assessments?

Seattle City Light is currently working to finalize these metrics.

Privacy and Civil Liberties Assessment

Purpose

This section shall be completed after public engagement has concluded and the department has completed the racial equity toolkit section above. The privacy and civil liberties assessment is completed by the community surveillance working group ("working group"), per the surveillance ordinance which states that the working group shall:

"Provide to the executive and the City Council a privacy and civil liberties impact assessment for each SIR that must be included with any departmental request for surveillance technology acquisition or in-use approval. The impact assessment shall include a description of the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities. The CTO shall share with the working group a copy of the SIR that shall also be posted during the period of public engagement. At the conclusion of the public engagement period, the CTO shall share the final proposed SIR with the working group at least six weeks prior to submittal of the SIR to Council for approval. The working group shall provide its impact assessment in writing to the executive and the City Council for inclusion in the SIR within six weeks of receiving the final proposed SIR. If the working group does not provide the impact assessment before such time, the working group must ask for a two-week extension of time to City Council in writing. If the working group fails to submit an impact statement within eight weeks of receiving the SIR, the department and City Council may proceed with ordinance approval without the impact statement."

Working Group Privacy and Civil Liberties Assessment

The Working Group's Privacy and Civil Liberties Impact Assessment for this technology is below, and is also included in the Ordinance submission package, available as an attachment.

From: Seattle Community Surveillance Working Group (CSWG) To: Seattle City Council

Date: June 4, 2019

Re: Privacy and Civil Liberties Impact Assessment for Check Meter Device, SensorLink Amp Fork, and Binoculars/Spotting Scope (Current Diversion Technologies, SDOT)

Executive Summary

On April 25, 2019, the CSWG received the Surveillance Impact Reports (SIRs) on three Current Diversion Technologies (Check Meter Device, SensorLink Amp Fork, and Binoculars/Spotting Scope) used by Seattle City Light (SCL) included in Group 2 of the Seattle Surveillance Ordinance technology review process. This document is CSWG's Privacy and Civil Liberties Impact Assessment for these technologies as set forth in SMC 14.18.080(B)(1), which we provide for inclusion in the final SIRs submitted to the City Council.

This document first provides recommendations in this executive summary, then provides background information, key concerns, and outstanding questions on the current diversion technologies.

Our assessment of the three current diversion technologies (Check Meter Device, SensorLink Amp Fork, and Binoculars/Spotting Scope) focuses on two key issues:

(1) The use of these systems and the data collected by them for purposes other than those intended;
(2) Over-collection and over-retention of data.

While the stated purposes of the three current diversion technologies may be relatively innocuous, it is important to note that these technologies may be used to gather identifying information about individuals. Particularly in the absence of written, explicit policies governing what these technologies can and cannot be used for, the data collected by these technologies may compromise the privacy of individuals and may be misused to target individuals and communities. It is important that these technologies have explicit protections limiting the use of these tools to their intended purpose.

Recommendations

We recommend that the Council and SCL adopt clear and enforceable rules that ensure, at a minimum, the following:

(1) Define purpose of use for each technology and restrict its use to that purpose.
(2) Ensure there are clear data protection policies to safeguard stored data.
(3) Ensure the deletion of data collected by the technology immediately after the relevant current diversion investigation has closed.

Background on the Three Current Diversion Technologies

The Check Meter Device, the SensorLink Amp Fork, and the Binoculars/Spotting Scope are technologies used by SCL's Current Diversion Team to investigate when electricity is being used without being paid for.

The Check Meter Device is a device that measures the amount of electrical energy flowing through a service-drop wire over time. It digitally captures the information for later retrieval by the Current Diversion Team member(s) via a wireless protocol. These devices are typically installed on an electric pole adjacent to a transformer for a period of one week to one month. The stated purpose of this technology is to determine the valuation of the energy illegally diverted.

The SensorLink Amp Fork is a hand-held electrical device used to detect current flow. It is mounted on an extensible pole (up to 40' to 50') that allows a circular clamp to be placed around a wire. The device then displays instantaneous readings of the amount of electrical energy flow. The Current Diversion Team member may then compare those reads against the readings displayed on the electric meter, allowing staff to determine if current is being diverted.

The Binoculars/Spotting Scope is a device used to determine if current diversion is taking place when distance is a barrier to physical inspection. Binoculars may also be used to determine if potentially dangerous alterations to City Light's electrical infrastructure exist. The relevant SIR states that the binoculars do not collect data, and do not contain any special enhancements requiring power (e.g., night vision or video-recording capabilities).[1]

Key Concerns Regarding all Three Current Diversion Technologies

Seattle City Light's policy:

(1) **Does not include explicit, written restrictions on use.** An April 3, 2019 email from Seattle City Light to the ACLU stated that "Seattle City Light does not have any formal, explicit, written policies on what the technologies can be used for."[2] The email states that Section 3.0 (Use Governance) of the SIRs describes SCL's standards, but this section does not contain meaningful restrictions on use. The absence of written, specific policies increases the risk of misuse.

(2) **Does not include specific data protection provisions.** For example, the draft SIR for the Check Meter Device (SensorLink Transformer Meter System) says that the data is retrieved from the device "via secure radio protocol," but the SIR does not explain further. Radio frequencies are not inherently secure, so the policy should define how this data is secured, including when it is on the Check Meter Device and once it is stored off the device.

(3) **Includes an unjustifiably long data retention period.** According to Seattle City Light, the retention period for current diversion data collected is at least 6 years.[3] Such a lengthy retention period for electricity diversion investigation records is unnecessary. Data should be deleted as soon as an investigation is closed.

In addition, all three SIRs state: "City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible." This equity analysis should be provided for public review.

[1] 2019 Surveillance Impact Report SCL Check Meter Device, pages 3-6.

[2] See pages 3-4 for Seattle City Light Response to ACLU-WA on April 3, 2019.

[3] Ibid.

City of Seattle

Seattle City Light

700 5th Ave. | P.O. Box 34023 | Seattle WA 98124-4023
TEL (206) 684-3000 TTY/TDD (206) 684-3225 FAX (206) 625-3709
seattle.gov/light
twitter.com/SEACityLight facebook.com/SeattleCityLight

April 3, 2019

Shankar Narayan, Technology and Liberty Project Director
Jennifer Lee, Technology and Liberty Project Advocate
American Civil Liberties Union – Washington
901 Fifth Ave, Suite 630
Seattle, WA 98164

Dear Shankar and Jennifer,

We have received your letter dated March 20, 2019 with comments on the three Seattle City Light technologies included in Group 2 of the Seattle Surveillance Ordinance process. We appreciate your feedback, which will be considered as the Surveillance Impact Reports (SIRs) are finalized.

In the meantime, I can offer the below information related to your two questions:

What enforceable policies, if any, apply to use of these three technologies?

Current Diversion Detection Technology Policies: Seattle City Light does not have any formal, explicit, written policies on what the technologies can be used for. However, City Light's draft 2019 Surveillance Impact Reports (SIRs) outline the non-written standards for use of the technologies. Please refer to Section 3.0, "Use Governance," of the attached SIRs for the three current diversion technologies, as they describe City Light's standards.

Also, please know that City Light has formally adopted a Department Policy & Procedure (DPP P III-416, "Current Diversion") governing the prevention, detection, reporting, investigation, and correction of illegal, unauthorized, or inadvertent diversions of electric current, and the recovery of associated lost revenues and costs. Please see the attached DPP.

What is Seattle City Light's data retention schedule?

City Light follows the record retention period presented in the following chart.

An equal employment opportunity, affirmative action employer. Accommodations for people with disabilities provided upon request.

Retention Schedule	Series Title and Description	DAN #	Retention and Disposition Action (Primary Record Copy)	Designation
Utility Services Power Distribution	ELECTRICITY DIVERSION INVESTIGATION RECORDS Inquiry regarding problems or discrepancies with meters, either from meter reader or other parties. Investigation records may include: site visit dates, notes regarding location, pictures of meter or surrounding area, consumption history, special meter read, and service order for technical support.	UT55-05G-07 Rev. 0	Investigation closed plus 6 years	Non-Archival Non-Essential OPR

Please let me know if you have additional questions.

Sincerely,

Julie Moore
Public Information Officer
Seattle City Light

City of Seattle

CTO Response

Memo

Date: 11/17/2020

To: Seattle City Council, Transportation and Utilities Committee

From: Saad Bashir

Subject: CTO Response to the Surveillance Working Group SCL Current Diversion Technologies SIR Review

---

To the Council Transportation and Utilities Committee,

I look forward to continuing to work together with Council and City departments to ensure transparency about the use of surveillance technologies and finding a mutually agreeable means to use technology to improve City services while protecting the privacy and civil rights of the residents we serve. Specific concerns in the Working Group comments about SCL's Current Diversion Technologies are addressed in the attached document.

As provided in the Surveillance Ordinance, SMC 14.18.080, this memo outlines the Chief Technology Officer's (CTO's) response to the Surveillance Working Group assessment on the Surveillance Impact Report for Seattle City Light's Current Diversion Technologies, including the Check Meter Device, SensorLink Amp Fork, and Binoculars/Spotting Scope.

Background

The Information Technology Department (ITD) is dedicated to the Privacy Principles and Surveillance Ordinance objectives to provide oversight and transparency about the use and acquisition of specialized technologies with potential privacy and civil liberties impacts. All City departments have a shared mission to protect lives and property while balancing technology use and data collection with negative impacts to individuals. This requires ensuring the appropriate use of privacy invasive technologies through technology limitations, policy, training and departmental oversight.

The CTO's role in the SIR process has been to ensure that all City departments are compliant with the Surveillance Ordinance requirements. As part of the review work for surveillance technologies, ITD's Privacy Office has facilitated the creation of the Surveillance Impact Report documentation, including collecting comments and suggestions from the Working Group and members of the public about these technologies. IT and City departments have also worked collaboratively with the Working Group to answer additional questions that came up during their review process.

Technology Purpose

Seattle City Light's Current Diversion Team (CDT) consists of a group of approximately five journey-level engineers who are dispatched to collect data to attempt to determine whether a suspected diversion of current (i.e., alterations to the City Light-owned electrical system by a third-party in order to consume electric power without it being registered by the City Light meter installed for that purpose) has taken place. Diversion alterations can result in injury to people and can damage SCL equipment and Infrastructure. Further, SCL is required by law (SMC 21.49.100) to collect payment for utility use and so investigates and remediates any loss of payment created by such situations.

In support of this mission, the CDT crew uses a Check Meter Device, SensorLink Amp Fork, and Binoculars/Spotting Scope. If a determination of diversion is sustained, data may be used to respond to lawful requests from the proper law enforcement authorities for evidence for recovering the value of the diverted energy.

Working Group Concerns

In their review, the Working Group has raised concerns about these Current Diversion Technologies being used in a privacy impacting way, including use of these systems for other than their stated purpose, and over-collection and over-retention of the data collected.

1) The use of these systems and the data collected by them for purposes other than those intended.
2) Over-collection and over-retention of data.

The policy and training enacted by SCL and limitations from the technologies themselves provide adequate mitigation for the potential privacy and civil liberties concerns raised by the Working Group about the use of this important operational technology.

Response to Specific Concerns: SCL Current Diversion Technologies

Concern: Use of these systems and the data collected by them for purposes other than those intended.

CTO Assessment: SCL's Department Policy & Procedure, DPP P III-416 outlines the process for determining why and how the department investigates suspected current diversion. This policy includes how evidence (such as data collected from current diversion technologies) must be handled and who is authorized to receive a report. Some of the technologies are not capable of sharing data outside of additional manual observations, and any data as a part of the investigation is securely stored and only accessible by members of the Current Diversion Team. This body of policy and operational documentation provides detail about how the technology is used and how any data collected is managed, and it is our assessment that the documentation provides adequate protections.

SIR Response:
Check Meter Device
Section 3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

"The CDT owns six SensorLink TMS units, which are deployed on the basis of case number and need. Deployment level on a given case can vary from none (zero) to all (six). Once a case is properly opened, CDT crew members may check them out without prior additional authorization, though the Current Diversion Coordinator is under nearly all circumstances aware of deployment due to position responsibilities. Serial numbers are recorded and the CDT member to whom they are assigned, as well as their deployment status, are logged."

Section 4.2 What measures are in place to minimize inadvertent or improper collection of data?

"Risk of inadvertent or improper collection is low for two reasons. First, the CDT only investigates specific, metered locations previously identified and properly documented as sites of suspected current diversion. And second, SensorLink TMS devices are used only on those service-drop lines that are delivering electrical service to the suspected location."

Amp Fork

Section 3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

"The limited number of this equipment and of CDT members makes the routine tracking of the Ampstik devices relatively straight-forward. Ampstiks are issued to CDT members, and stored in their official vehicles. These vehicles are operated, locked, and stored in accordance with Utility security procedures. Ampstiks' serial numbers are recorded and the CDT member to whom they are assigned, as well as their deployment status, are logged."

Section 4.2 What measures are in place to minimize inadvertent or improper collection of data?

"Risk of inadvertent or improper collection is low for two reasons. First, the CDT only investigates specific, metered locations previously identified as sites of suspected current diversion. And second, Ampstik devices are used only on those service-drop lines that are delivering electrical service to the suspected location."

Binoculars

Section 3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

"The limited number of this equipment and of CDT members makes the routine tracking of the binoculars relatively straight-forward. Binoculars are issued to CDT members, and stored in their official vehicles. These vehicles are operated, locked, and stored in accordance with Utility security procedures."

Section 4.2 What measures are in place to minimize inadvertent or improper collection of data?

"Risk of inadvertent or improper collection is low. The CDT only investigates specific meters and other implicated electrical equipment at locations previously identified and properly documented as sites of suspected current diversion."

Concern: Data Protection Policies

CTO Assessment: The data storage location and access controls are adequate for protecting information collected by these technologies during current diversion investigations. All users that have access to this data have an authorized and specified use for the data. For those devices that are capable of collecting data, none is retained on the device, and any data stored would be kept in line with the department retention policy.

SIR Response:

Check Meter Device

Section 4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

"Data obtained by means of the SensorLink TMS device are stored in a private folder on City Light's digital file locations, accessible only by CDT members and management. Data stored in the SensorLink TMS device itself are deleted after its observations are retrieved by the CDT and/or upon its removal from the electrical pole (i.e., no data remain on the SensorLink TMS once its use for a given determination of current diversion has been completed and before it is therefore made available to other CDT staff for subsequent deployment)."

Amp Fork

Section 4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

"Data obtained by means of the Ampstik are stored in a private folder on City Light's digital file locations. The data, as well as incident reports, are accessible only by CDT members and its Current Diversion Coordinator."

Binoculars

Section 4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

"Data obtained by means of binoculars (which consist of notes made by staff based on their binocular-facilitated observations) are stored in a private folder on City Light's digital file locations. The data, as well as overall incident reports, are accessible only by CDT members and its Current Diversion Coordinator."

Concern: Overcollection and over retention of data

CTO Assessment: SCL follows legally required retention periods that ensure that only data that is necessary to complete an investigation is preserved after the investigation in case of any dispute. The data is protected and only accessible by those who are related to the investigation

SIR Response:
Check Meter Device
Section 4.7 How will data that is collected be accessed and by whom?

"CDT members, who are journey-level electrical workers trained in the placement, use, and removal of the SensorLink TMS device, may collect this data. The quantitative data – accumulated consumption (in kilowatt-hours), average volts (current strength), average amps (current flow), and interval consumption (in kilowatt-hours per a pre-defined time-unit) – are accessed by CDT crew members remotely using a secure radio protocol and a specific, password-protected software program, known as Steelhead."

Section 4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

"Data obtained by means of the SensorLink TMS device are stored in a private folder on City Light's digital file locations, accessible only by CDT members and management. Data stored in the SensorLink TMS device itself are deleted after its observations are retrieved by the CDT and/or upon its removal from the electrical pole (i.e., no data remain on the SensorLink TMS once its use for a given determination of current diversion has been completed and before it is therefore made available to other CDT staff for subsequent deployment)."

Amp Fork
Section 4.7 How will data that is collected be accessed and by whom?

"CDT members, who are journey-level electrical workers trained in the use of the Ampstik, may collect and access this data. Additionally, the Current Diversion Coordinator may access the data."

Section 4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

"Data obtained by means of the Ampstik are stored in a private folder on City Light's digital file locations. The data, as well as incident reports, are accessible only by CDT members and its Current Diversion Coordinator."

Binoculars
Section 4.7 How will data that is collected be accessed and by whom?

"CDT members, who are journey-level electrical workers trained in the proper use this equipment, may collect these data. These consist of meter reads and, in certain instances, other implicated electrical equipment that poses a present danger to the public or the electrical system integrity."

Section 4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

"Data obtained by means of binoculars (which consist of notes made by staff based on their binocular-facilitated observations) are stored in a private folder on City Light's digital file locations. The data, as well as overall incident reports, are accessible only by CDT members and its Current Diversion Coordinator."

SCL's Required Retention period

Retention Schedule	Series Title and Description	DAN #	Retention and Disposition Action (Primary Record Copy)	Designation
Utility Services Power Distribution	ELECTRICITY DIVERSION INVESTIGATION RECORDS Inquiry regarding problems or discrepancies with meters, either from meter reader or other parties. Investigation records may include: site visit dates, notes regarding location, pictures of meter or surrounding area, consumption history, special meter read, and service order for technical support.	UT55-05G-07 Rev. 0	Investigation closed plus 6 years	Non-Archival Non-Essential OPR

Appendix A: Glossary

Accountable: (taken from the racial equity toolkit.) Responsive to the needs and concerns of those most impacted by the issues you are working on, particularly to communities of color and those historically underrepresented in the civic process.

Community outcomes: (taken from the racial equity toolkit.) The specific result you are seeking to achieve that advances racial equity.

Contracting equity: (taken from the racial equity toolkit.) Efforts to achieve equitable racial outcomes in the way the City spends resources, including goods and services, consultants and contracting.

DON: "department of neighborhoods."

Immigrant and refugee access to services: (taken from the racial equity toolkit.) Government services and resources are easily available and understandable to all Seattle residents, including non-native English speakers. Full and active participation of immigrant and refugee communities exists in Seattle's civic, economic and cultural life.

Inclusive outreach and public engagement: (taken from the racial equity toolkit.) Processes inclusive of people of diverse races, cultures, gender identities, sexual orientations and socio-economic status. Access to information, resources and civic processes so community members can effectively engage in the design and delivery of public services.

Individual racism: (taken from the racial equity toolkit.) Pre-judgment, bias, stereotypes about an individual or group based on race. The impacts of racism on individuals including white people internalizing privilege, and people of color internalizing oppression.

Institutional racism: (taken from the racial equity toolkit.) Organizational programs, policies or procedures that work to the benefit of white people and to the detriment of people of color, usually unintentionally or inadvertently.

OCR: "Office of Civil Rights."

Opportunity areas: (taken from the racial equity toolkit.) One of seven issue areas the City of Seattle is working on in partnership with the community to eliminate racial disparities and create racial equity. They include: education, health, community development, criminal justice, jobs, housing, and the environment.

Racial equity: (taken from the racial equity toolkit.) When social, economic and political opportunities are not predicted based upon a person's race.

Racial inequity: (taken from the racial equity toolkit.) When a person's race can predict their social, economic, and political opportunities and outcomes.

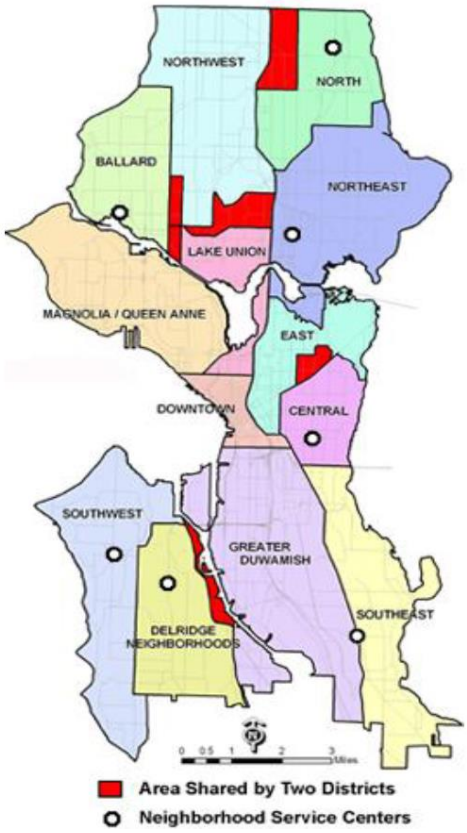
RET: "racial equity toolkit"

Seattle neighborhoods: (taken from the racial equity toolkit neighborhood.) Boundaries defined for the purpose of understanding geographic areas in Seattle.

Stakeholders: (taken from the racial equity toolkit.) Those impacted by proposed policy, program, or budget issue who have potential concerns or issue expertise. Examples might include: specific racial/ethnic groups, other institutions like Seattle housing authority, schools, community-based organizations, change teams, City employees, unions, etc.

Structural racism: (taken from the racial equity toolkit.) The interplay of policies, practices and programs of multiple institutions which leads to adverse outcomes and conditions for communities of color compared to white communities that occurs within the context of racialized historical and cultural conditions.

Surveillance ordinance: Seattle City Council passed ordinance 125376, also referred to as the "surveillance ordinance."



SIR: "surveillance impact report", a document which captures the fulfillment of the Council-defined surveillance technology review process, as required by ordinance 125376.

Workforce equity: (taken from the racial equity toolkit.) Ensure the City's workforce diversity reflects the diversity of Seattle.

City of Seattle

Appendix B: Meeting Notice(s)

City Surveillance Technology Fair

February 27, 2018

6:00 p.m. – 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Join us for a public meeting to comment on a few of the City's surveillance technologies:

Seattle City Light
- Binoculars
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation
- Acyclica

Seattle Fire Department
- Computer Aided Dispatch

Seattle Police Department
- 911 Call Logging Recorder
- Computer Aided Dispatch
- CopLogic

Can't join us in person?

Visit www.seattle.gov/privacy to leave an online comment or send your comment to **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** The Open Comment period is from **February 5 - March 5, 2019.**

Please let us know at Surveillance@seattle.gov if you need any accommodations. For more information, visit Seattle.gov/privacy.

Surveys, sign-in sheets and photos taken at this event are considered a public record and may be subject to public disclosure. For more information see the Public Records Act RCW Chapter 42.56 or visit Seattle.gov/privacy. All comments submitted will be included in the Surveillance Impact Report.

City of Seattle

Giám Sát Thành Phố
Hội Chợ Công Nghệ

ngày 27 tháng 2 năm 2019
6 :00 giờ chiều – 8:00 giờ chiều
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Hãy tham gia cuộc họp công cộng cùng chúng tôi để nhận xét về một số công nghệ giám sát của Thành phố:

Seattle City Light
- Ống nhòm quan sát
- Sensorlink Ampstik
- Đồng hồ đo máy biến áp của Sensorlink

Seattle Department of Transportation (Sở Giao Thông Vận Tải Seattle)
- Acyclica

Seattle Fire Department (Sở Phòng Cháy Chữa Cháy Seattle)
- Hệ Thống Thông Tin Điều Vận Có Máy Tính Trợ Giúp

Seattle Police Department (Sở Cảnh Sát Seattle)
- Hệ Thống Ghi Âm Cuộc Gọi 911
- Hệ Thống Thông Tin Điều Vận Có Máy Tính Trợ Giúp
- CopLogic

Quý vị không thể tới tham dự trực tiếp cùng chúng tôi?

Hãy truy cập www.seattle.gov/privacy và để lại nhận xét trực tuyến hoặc gửi ý kiến của quý vị tới **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** Giai đoạn Góp Ý Mở từ **Ngày 5 tháng 2 - Ngày 5 tháng 3 năm 2019.**

Vui lòng thông báo cho chúng tôi tại Surveillance@seattle.gov nếu quý vị cần bất kỳ điều chỉnh nào. Để có thêm thông tin, hãy truy cập Seattle.gov/privacy.

Các khảo sát, danh sách đăng ký và ảnh chụp tại sự kiện này được coi là thông tin công cộng và có thể được tiết lộ công khai. Để biết thêm thông tin, hãy tham khảo Public Records Act (Đạo Luật Hồ Sơ Công Cộng) RCW Chương 42.56 hoặc truy cập Seattle.gov/privacy. Tất cả các ý kiến đóng góp mà quý vị gửi đến sẽ được đưa vào Báo Cáo Tác Động Giám Sát.

City of Seattle

Eksibisyon ng Teknolohiya Sa Pagmamatyag sa Lungsod

Pebrero 27, 2019

6:00 p.m. - 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Samahan kami para sa isang pampublikong pagpupulong upang magbigay ng komento sa ilan sa mga teknolohiya sa pagmamanman ng Lungsod:

Seattle City Light
- Mga Binocular
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation (Departamento ng Transportasyon ng Seattle)
- Acyclica

Seattle Fire Department (Departamento para sa Sunog ng Seattle)
- Pagdispatsa sa Tulong ng Computer

Seattle Police Department (Departamento ng Pulisya ng Seattle)
- Rekorder ng Pagtawag sa 911
- Pagdispatsa sa Tulong ng Computer
- CopLogic

Hindi kami masasamahan nang personal?

Bumisita sa www.seattle.gov/privacy upang mag-iwan ng online na komento o ipadala ang iyong komento sa **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** Ang panahon ng Bukas na Pagkomento ay sa **Pebrero 5 - Marso 5, 2019.**

Mangyaring ipaalam sa amin sa Surveillance@seattle.gov kung kailangan mo ng anumang tulong. Para sa higit pang impormasyon, bumisita sa Seattle.gov/privacy.

Itinuturing na pampublikong rekord ang mga survey, papel sa pag-sign-in at mga larawan na makukuha sa pangyayaring ito at maaaring mapasailalim sa paghahayag sa publiko. Para sa higit pang impormasyon, tingnan ang Public Records Act (Batas sa Mga Pampublikong Rekord) RCW Kabanata 42.56 o bumisita sa Seattle.gov/privacy. Isasama ang lahat ng isinumiteng komento sa Surveillance Impact Report (Ulat sa Epekto ng Pagmamanman).

City of Seattle

Feria de tecnología de vigilancia ciudadana

27 febrero de 2019

De 6:00 p. m. a 8:00 p. m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Acompáñenos en la reunión pública para dar su opinión sobre algunas de las tecnologías de vigilancia de la ciudad:

Seattle City Light
- Binoculars
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation (Departamento de Transporte de Seattle)
- Acyclica

Seattle Fire Department (Departamento de Bomberos de Seattle)
- Computer Aided Dispatch

Seattle Police Department (Departamento de Policía de Seattle)
- 911 Call Logging Recorder
- Computer Aided Dispatch
- CopLogic

¿No puede asistir en persona?

Visite www.seattle.gov/privacy para dejar un comentario en línea o enviar sus comentarios a **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** El período de comentarios abiertos es desde el **5 de febrero al 5 de marzo de 2019.**

Avísenos en Surveillance@seattle.gov si necesita adaptaciones especiales. Para obtener más información, visite seattle.gov/privacy.

Las encuestas, las planillas de asistencia y las fotos que se tomen en este evento se consideran de dominio público y pueden estar sujetas a la difusión pública. Para obtener más información, consulte la Public Records Act (Ley de Registros Públicos), RCW capítulo 42.56, o visite Seattle.gov/privacy. Todos los comentarios enviados se incluirán en el Informe del efecto de la vigilancia.

City of Seattle

Kormeerida Bandhigga Tiknoolajiyada ee Magaalada

Feebaraayo 27, 2019
6:00 p.m. - 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Nagulasoo biir bandhigga dadweynaha si fikir looga dhiibto dhawr kamid ah aaladaha tiknoolajiyada ee City surveillance:

Seattle City Light
- Binoculars
- Sensorlink Ampstik
- Sensorlink Cabiraha mitirka Gudbiyaha

Seattle Department of Transportation
(Waaxda Gaadiidka ee Seattle)
- Acyclica

Seattle Fire Department
(Waaxda Dab damiska ee Seattle)
- Adeeg Qaybinta Kumbuyuutarka loo adeegsado

Seattle Police Department
(Waaxda Booliiska ee Seattle)
- Qalabka Duuba Wicitaanada 911
- Computer Aided Dispatch
- CopLogic

Nooguma imaan kartid miyaa si toos ah?

Booqo barta www.seattle.gov/privacy si aad fikirkaaga oonleen ahaan uga dhiibato **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.**
Mudada Fikrad Dhiibashadu furantahay waxay kabilaabanaysaa
Feebaraayo 5 - Maarso 5, 2019.

Fadlan noogusoo gudbi ciwaankaan Surveillance@seattle.gov hadaad ubaahantahay hooy laguusii qabto. Wixii macluumaad dheeri ah, booqo Seattle.gov/privacy.

Xog aruurinada, waraaqaha lasaxixaayo iyo sawirada lagu qaado munaasabadaan waxaa loo aqoonsanayaa diiwaan bulsho waxaana suuragal ah in bulshada lagu dhex faafiyo. Wixii macluumaad dheeri ah kafiiri Public Records Act (Sharciga Diiwaanada Bulshada) RCW Cutubkiisa 42.56 ama booqo Seattle.gov/privacy. Dhammaan fikradaha ladhiibto waxaa lagusoo darayaa Warbixinta ugu danbaysa ee Saamaynta Qalabka Muraaqabada.

City of Seattle

城市监控技术博览会

2019 年 2 月 27 日
下午 6:00 至下午 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 9810

加入我们的公众会议，留下您对纽约市监控技术的意见：

Seattle City Light
- 望远镜
- Sensorlink Ampstik
- Sensorlink 变压器表

Seattle Department of Transportation（西雅图交通局）
- Acyclica

Seattle Fire Department（西雅图消防局）
- 计算机辅助调度

Seattle Police Department（西雅图警察局）
- 911 通话记录录音器
- 计算机辅助调度
- CopLogic

无法亲自前来？

访问 www.seattle.gov/privacy 发表在线评论或将您的意见发送至 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124。开放评论期：2019 年 2 月 5 日至 3 月 5 日。

如果您需要任何住宿服务，请通过 Surveillance@seattle.gov 联系我们。要获得更多信息，请访问 Seattle.gov/privacy。

此次活动中的调查、签到表和照片被视为公共记录，可能会被公开披露。有关更多信息，请参阅 Public Records Act（信息公开法）RCW 第 42.56 章或访问 Seattle.gov/privacy。提交的所有意见都将包含在监控影响报告内。

City of Seattle

도시 감시 기술 박람회

2019 년 2 월 27 일
오후 6:00 – 오후 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

공개모임에 참여하시고, 도시 감시 기술과 관련한 의견을 공유해 주십시오.

Seattle City Light
- 쌍안경
- Sensorlink Ampstik
- Sensorlink 변압기 미터

Seattle Department of Transportation(시애틀 교통국)
- Acyclica

Seattle Fire Department(시애틀 소방국)
- 컴퓨터 지원 출동 지시

Seattle Police Department(시애틀 경찰국)
- 911 전화 기록 녹음기
- 컴퓨터 지원 출동 지시
- CopLogic

현장 참여가 어려우신가요?

www.seattle.gov/privacy 를 방문하셔서 온라인 의견을 남기시거나 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124 로 의견을 송부해 주시기 바랍니다. 공개 의견 수렴 기간은 2019 년 2 월 5 일 – 3 월 5 일입니다.

편의사항이 필요하신 경우 Surveillance@seattle.gov 로 문의해 주시기 바랍니다.
자세한 정보는 Seattle.gov/privacy 를 참조해 주십시오.

본 행사에서 수집된 설문 조사, 참가 신청서 및 사진은 공개 기록으로 간주되며 일반에 공개될 수 있습니다. 자세한 사항은 Public Records Act(공공기록물법) RCW 챕터 42.56 을 참조하시거나, Seattle.gov/privacy 를 방문하시기 바랍니다. 제출된 모든 의견은 감시 영향 보고서에 수록됩니다.

City of Seattle

城市監視技術展覽會

2019 年 2 月 27 日
下午 6:00 至下午 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

加入我們的公眾會議，留下您對紐約市監視技術的意見：

Seattle City Light
- 望遠鏡
- Sensorlink Ampstik
- Sensorlink 變壓器表

Seattle Department of Transportation（西雅圖交通局）
- Acyclica

Seattle Fire Department（西雅圖消防局）
- 電腦輔助發送

Seattle Police Department（西雅圖警察局）
- 911 通話紀錄錄音機
- 電腦輔助發送
- CopLogic

無法親自前來？

造訪 www.seattle.gov/privacy 發表線上評論或將您的意見傳送至 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124。開放評論期：2019 年 2 月 5 日至 3 月 5 日。

如果您需要任何便利服務，請透過 Surveillance@seattle.gov 聯絡我們。要獲得更多資訊，請造訪 Seattle.gov/privacy。

此次活動中的調查、簽入表和照片被視為公共紀錄，可能會被公開披露。有關更多資訊，請查閱 Public Records Act（資訊公開法）RCW 第 42.56 章或造訪 Seattle.gov/privacy。提交的所有意見都將包含在監視影響報告內。

City of Seattle

Appendix C: Meeting Sign-in Sheet(s)

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☒ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☒ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

☐ Include Middle Eastern

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☒ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☒ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☒ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☑ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☑ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☒ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☒ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☑ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☒ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☒ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☑ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☑ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☑ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

2

Queen Anne

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☑ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☑ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☒ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- [x] Ballard
- [ ] Belltown
- [ ] Beacon Hill
- [ ] Capitol Hill
- [ ] Central District
- [ ] Columbia City
- [ ] Delridge
- [ ] First Hill
- [ ] Georgetown
- [ ] Greenwood / Phinney
- [ ] International District
- [ ] Interbay
- [ ] North
- [ ] Northeast
- [ ] Northwest
- [ ] Madison Park / Madison Valley
- [ ] Magnolia
- [ ] Rainier Beach
- [ ] Ravenna / Laurelhurst
- [ ] South Lake Union / Eastlake
- [ ] Southeast
- [ ] Southwest
- [ ] South Park
- [ ] Wallingford / Fremont
- [ ] West Seattle
- [ ] King county (outside Seattle)
- [ ] Outside King County

Race/Ethnicity

- [ ] American Indian or Alaska Native
- [ ] Asian
- [ ] Black or African American
- [ ] Hispanic or Latino
- [ ] Native Hawaiian or other Pacific Islander
- [x] White
- [ ] Prefer not to Identify

Age

- [ ] Under 18
- [x] 18-44
- [ ] 45-64
- [ ] 65+
- [ ] Prefer not to identify

Gender

- [x] Female
- [ ] Male
- [ ] Transgender
- [ ] Prefer not to identify

Neighborhood

- [ ] Ballard
- [ ] Belltown
- [ ] Beacon Hill
- [ ] Capitol Hill
- [ ] Central District
- [ ] Columbia City
- [ ] Delridge
- [ ] First Hill
- [ ] Georgetown
- [ ] Greenwood / Phinney
- [ ] International District
- [ ] Interbay
- [ ] North
- [ ] Northeast
- [ ] Northwest
- [ ] Madison Park / Madison Valley
- [ ] Magnolia
- [ ] Rainier Beach
- [ ] Ravenna / Laurelhurst
- [ ] South Lake Union / Eastlake
- [ ] Southeast
- [ ] Southwest
- [ ] South Park
- [x] Wallingford / Fremont
- [ ] West Seattle
- [ ] King county (outside Seattle)
- [ ] Outside King County

Race/Ethnicity

- [ ] American Indian or Alaska Native
- [ ] Asian
- [ ] Black or African American
- [ ] Hispanic or Latino
- [ ] Native Hawaiian or other Pacific Islander
- [x] White
- [ ] Prefer not to Identify

Age

- [ ] Under 18
- [x] 18-44
- [ ] 45-64
- [ ] 65+
- [ ] Prefer not to identify

Gender

- [ ] Female
- [x] Male
- [ ] Transgender
- [ ] Prefer not to identify

City of Seattle

Neighborhood
- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☑ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity
- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☑ White
- ☐ Prefer not to Identify

Age
- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender
- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood
- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity
- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age
- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender
- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

X

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☒ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☒ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☒ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☒ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☒ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☒ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☑ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

leighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
] Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☒ 18-44
☐ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☒ Female
☐ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☑ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
] Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☐ 45-64
☑ 65+
☐ Prefer not to identify

Gender

☐ Female
☑ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

☑ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
] Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☑ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☑ Female
☐ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

SE KING COUNTY

☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☑ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
✓ Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☑ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☐ Female
☑ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☒ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☒ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☒ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☒ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☒ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☑ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☑ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☑ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☑ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☑ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☑ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Appendix D: Department of Neighborhood Focus Group Notes

Friends of Little Saigon (FOLS)

Please select which technology you wish to comment on:

☐SCL: Binoculars ☐SCL: Sensorlink Transformer Meter (TMS) ☐SFD: Computer-Aided Dispatch ☐SPD:9-11 Call Recorder

☐SCL: Sensorlink Ampstik ☐SDOT: Acyclica ☐SPD: Computer-Aided Dispatch ☒SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

- Will they keep the data safe on coplogic?
- Can it be hacked?
- What if you report your neighbour and your neighbour hacks the system and find out?
- What is the money amount limit for coplogic / Why is there a limit for coplogic?: (a community member says that she believes that the limit $500 or under, but it's hard to have a limit because a lot of packages cost more than $500 such as electronics get stolen and you won't be able to report it online)
- The departement is having all these technologies being used but not letting the public aware of it
- Coplogic is not clear and is confusing to use (what you can report and what you can't report)
- If coplogic is known by the community would they use it ? (Community members agreed that no one would use coplogic because it's not in Vietnamese. Not even people who speak english fluently even use it.
- Many community members don't trust the system)

What value, if any, do you see in the use of this technology?

- Coplogic has been going on for a few years it's not very effective. The only effective thing is that coplogic is doing saving police hours and time.

What do you want City leadership to consider about the use of this technology?

- Most of the time, our community don't report things because they don't trust the system, they often tell someone that they trust a friend. Is there an option that someone and report a crime for someone else?

Other comments:

- The government should be more transparent with the technology system with the public.
- The translation is much far removed from the actual Vietnamese language.

- The translation is very hard to understand, the language is out of context (The flyer is poorly translate)
- Is there resources to support these technologies? Is there translations so that it is accessible for everyone? Will this accommodate everyone?
- Police should have a software that connects them to translation and interpretation right away instead of having to call a translator
- How will other people know of the technology if they can't come to focus group meetings? Such as flyers? Social media? Etc.
- Besides face to face meetings, are there plans to execute this information of the technology and surveillance to the community?
- Will the City of Seattle go to community events, temple, the church to reach out to the community and explain the technologies?
- These technologies are taking a part of our taxes, so everyone should know. It should be for everyone to know, not only catered to one group or population.

Are there any questions you have, or areas you would like more clarification?

- How effective are the tools/technology?
- How many people know of these technologies? Provide statistics
- What are the statistics of the coplogic?
- What is the data and statistics for coplogic and what are people reporting?
- What is the most common crime that they are reporting?
- And how effective is coplogic based on the statistics and data?

City of Seattle

Friends of Little Saigon (FOLS)

Please select which technology you wish to comment on:

☐SCL: Binoculars	☐SCL: Sensorlink Transformer Meter (TMS)	☐SFD: Computer-Aided Dispatch	☒SPD:9-11 Call Recorder
☐SCL: Sensorlink Ampstik	☐SDOT: Acyclica	☒SPD: Computer-Aided Dispatch	☐SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

- CAD did not work from experience. A community member said that they reported that they needed assistance at 10:00pm and no one showed up, then had to call 911 at 12:00am and someone finally showed up at 4:30am
- Why create more options and technologies if the police department and government can not support it? It's a waste of time and money (taxes). Should have enough personals before they implement technology.
- Government should have enough personals to support translation if they choose to translate.

What do you want City leadership to consider about the use of this technology?

- The city should focus on having the community review the technologies that are yet to be implemented.
- The Vietnamese community is not getting the information we need to report crimes

Other comments:

- Engagement is very important. Engaging the community and engaging different demographics.
- Friday night, Saturdays, and Sunday afternoon work the best for the Vietnamese community.
- If the city wants to involve the vietnamese community and engage the Vietnamese community, it is important to accommodate with our community It is important to proofread the translation, have 3 people proofread. Someone
  pre 1975, post 1975 and current Vietnamese language. The government clearly does not proofread the translation.

Council on American Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington
Thursday, Feb. 21, 2019
Technology Discussed: CopLogic

1. Do you have concerns about this specific technology or how it's used?
    - Having used the system myself the one thing I noted was the type of report you can file, they ask questions like if you knew the suspect, and if you're saying no I don't know who did it. and you check a box that says I understand that no one is going to investigate this
        - What is the point of having a system in place than If no one is going to investigate it
        - It is for common things like my car is broken into and stuff was taken out of my car, you can file it if you need a report for insurance. But if you were to call that and report to the police, they wouldn't come for days
    - So for example if I can be a straight up Islamophobe and I can see a Muslim woman and make a bunch of false reports online, and how long would it take for someone to say I see you making all these reports. Because people can make so many different reports, how do you deal with that
        - There are very limited types of reports that it will accept. So if someone wanted to report graffiti and they were reporting more hate crime related graffiti an officer will review the report
        - So I think the review process would be really important
    - Another barrier is that it's an online system so we need to think about wifi access and there is this assumption that everyone has access to internet and computers. And what I'm hearing is that people can just file a report at a click of their finger. And if these people can do that on their computer what stops them from being able to file all these cases about certain groups and individuals.
    - Additional there have been cases in the past where people are abusing reporting system. This one doesn't allow you to report against known suspect but I could see that happening in the future so I wanted that to be mentioned. The other thing under protection is says all activity can be stored and the data Is monitored by lexis nexus… and this company does a lot of research on crime mapping which brings up some of the concerns on like CVE
        - But what you are saying is that lexis nexus does other mapping that it can use this information for
        - Yes, because I want to clarify what is the technological ambition of SPD because I don't think this would work well in the communities that SPD is supposed to served. And I would want a contract review of what lexis nexus does. Will the info stay on the data and server of lexis nexus, what happens to it
    - Another thing is has SPD given Lexis nexus to use this in any of the research data they do, because they put out a lot of information regarding mapping, and crime control. And what information are they allowed to take
    - We have seen recently people doing interesting things when reporting crimes. I think its important to realize that when reporting crime people have a different perception when reporting crime. People will see you in a certain neighborhood and might think they

stole that car, or are doing something bad here. So when we give people the ability to report online we need to be concerned with accessibility about people being able to report freely… and we saw for a year that if an African American person came to use a swimming pool someone can call and say they don't live here. I think SPD is trying alleviate some of those calls they are getting, but I don't think this is the solution to the problem

- What is the logic behind this overall, because is seems like it presents more cons than pros, and what is analytics database you use to look at these reports. Because when I am using government data base I can see where I need more surveillance etc. so we are getting all these open wholes in the system. Is this a right wing Donald trump agenda to watch neighbors of color and surveillance
- I think im more concerned with where does this information end up and how is it used
- What is the usefulness of the information that is not followed up on. And how does it help the people it's actually serving? So for example someone works for an anti-Muslim white supremacy group and they have people in different areas report issues about different Muslim groups in Seattle how do you prove the validity of these information and make sure they aren't just causing harm

2. What value do you think this brings to our city?
    - I think technology saves time, money, makes filing a report easy, I had to do that once it takes a lot of time.
    - I appreciate that it is easier so something like a hit or run or a car breaking in, that's fine.
3. What worries you about how this is used?
    - The only issues I can think of right now is it seems like it would be very easy to make a fraudulent report or a report that is for a small thing that you can make into a big thing, like the things you see go viral on the internet. So now it seems like the barrier to making a police report is smaller
    - I agree I think the bar is lowered and different people are perceived differently. And we have seen how SPD criminalizes different communities for behaviors that don't need to be criminalizing
    - A lot of different kinds of reports have to do with peoples perceived notion, so my concern comes from how do we make sure that this kind of technology isn't used to map our where Muslims live/are, and there types of religious belief. Or isn't being used to monitor them. How do we ensure that this isn't used to map our communities
    - The only comment I have that in the forms I have filled out is it won't allow you to fill out the form if you are naming a specific individual, you can name a group, but a not a person. The following criteria is there no known suspects, it happens in Seattle, so things like thefts. So you can report, graffiti, identity theft, credit card fraud, simple shop lift. So when I click report it says if you have a suspect it says please call. And when I press report it allows me to report anonymously, so I could report against a community with no follow up
        - Well that doesn't stop them from targeting al-Noor masjid, or Safeway in new holly, or new holly gathering hall, and it can target the people in that community. And people don't feel comfortable with increase police presences, so it targets area if not targeting people

- When I was buying the house in Dallas (participant currently still lives/works/plays in Seattle) one of the first things I did was looking at a crime map and based off of that if someone is making a lot of reports can that be used for crime mapping because than that can lower the property value. And if the police isn't following up then how is it being used
- Its definitely possible for people to report inaccurate information

4. What recommendations would you give policy makers at the City about this technology?
    a. But my concern is reporting someone that can really target people of color. And that happens much more threatening to people. So the concept of an upset black women is more intimidating than an upset women that is another race and how many times will behavior like that be reported. Or how many times will a black man be reported against because it seems scary. So I think it lowers the bar when you don't have to talk to an individual when you don't have to talk to a police
    b. My questions are, how accessible are cop logic to people who don't read or speak English. How is SPD going to do what they can to make sure that this doesn't negatively impact communities they are already having issues with like the Sea Tac community that already feels threaten and criminalized by communities.

5. Can you imagine another way to solve the problem this technology solves?
    - So the SPD is very data driven these days and the one thing we repeat is report report report, call 911 and report online whatever you thinking is happening because all of that goes into their data base and is used for them to use resources and put police based off of where there is more crime. The report report report mentality assumes there are good relationships between the community and police, so even if someone doesn't do something bad, I don't know that they would feel comfortable reporting, even if online
    - From the community I have come from I am almost certain that they haven't even used online reporting so how do we make sure that we are giving everyone access to use online reporting. And there are certain crimes that are so common in areas that they don't even report it because they think the police should already know about it
    - I think the department should solely rely on the technology only as a way of collecting info they should still use in personal resources to actively participant in local community and make connections you can't rely only on this technology alone to do this

6. Other comments
    a. Also in this day in age we need to consider that immigration is a issue, and this administrative has blended the different agencies so people have a hard time knowing where SPD starts and ICE starts and those lines have been blurred and that is a real concern for many families

Council on Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington

Thursday, Feb. 21, 2019

Technology Discussed: Binoculars/Spotting Scope

1. Do you have concerns about this specific technology or how it's used?
    . People in our community don't have the access to say or be apart of these conversation. A lot of these people are literate, and might not have the same cultural values. For Muslim women there are a type of consent that you have when you walk outside and are covered in a certain away versus when you are in the privacy of your own home. And people might not have that cultural and religious awareness
    a. I had one quick concerns, as far as the data that is collected using these binoculars, who has access to it
        - Seattle City Light: Information goes into the billing system, which customers can access if they have the automated reader but do not have access to under the current system
    - I know the focus is on binoculars but my mind is on new technologies and when people who are consumers and feel like I am overcharged how do I follow up and get those issues resolved. For systems that are completed based off of technologies how will I know if that data is being altered.
    b.
2. What value do you think this brings to our city?
    . I would just add this is more my general comments I think its good that Seattle city lights is providing notifications to people when this is happening. Are they wearing something visible that show people they are from Seattle city lights? And is there a way for people to complain?
        - Yes they are wearing vests that are very visible. Yes we have a couple different avenues the easiest is to call the customer service line and to submit a complaint there
3. What worries you about how this is used?
    . My primary concerns on my end is if someone is looking into my home with binoculars its a privacy concern. Most Muslim women wear hijab and I don't feel comfortable if someone is using binoculars looking from the outside when we are not wearing the hijab. My concern is that it is a huge invasion of privacy
    a. I have a question as the women expressed the feeling of people reading the meters with binoculars, if the meter has abnormal behavior or is in a different place of the house. Have there been situations where someone sees the person looking at someone house with binoculars, and they might not have gotten notified. Or the meter might be on the opposite side of where they are looking. Are they getting background checks? Or are complaints being followed up

- Seattle City Light: Yes all city employees have background checks, and if a complaint gets called in they will go through disciplinary actions
- What are the average times for disciplinary actions. How long is the process for a full investigation
- Seattle City Light: It's a multiple step process in terms of different levels. There are warnings, and if there was undo actions. Timeline really depends, I'm not sure
- Cause I think that people who go through the different nuances of how privacy can be breach that is just the end all be all of how privacy can breach so I think there needs to be policy put in place so that people don't have their privacy breach and they are being monitored by a pedophile

4. What recommendations would you give policy makers at the City about this technology?
   . When I look at the Seattle city of light they do a lot of estimated guesses and as a consumer they might give you a $500 fee based off of the estimated guesses so I think it is important to have some sort of device that better clearly shows how much you use

5. Can you imagine another way to solve the problem this technology solves?
   . My other question is if its actually not efficient why do you get the option to opt out (of the new automated system). If there is an old school way of doing it that involves a breach of privacy because these are human beings using the binoculars, so If this other option is better why are people having the ability to opt out.
6. Other comments: (Many comments were discussed over Seattle City Light's upcoming change from binocular use to automated meter readers)
   . Who opted out was it home owners?
   a. When we go to a place with 12 tenements do all 12 of them have the ability to opt out or in, or just the owners of the building?
   b. Each home owner has a schedule provided to them and it is a 3 day period which they can come in and look at the system
   c. Is there a cost to them to have the new meter.
      - Seattle City Light: There is no cost with getting the new meter, but there is still a cost If we have to send someone out there to read it
      - What I don't understand is why the new practice is not to just use the new system since that is more accurate and it is doesn't require binoculars
      - What is the cost of opting out
      - Seattle City Light: There is a flat rate
   - I was gonna reiterate when we talk about equity and equitable practices. You can opt out (of the automated system) but there is a fee. And it makes me think

how much of It is a choose if one of these you have to pay for and the other one is free. So that sounds a little problematic when looking at choices of equity. I think choices are great, but also people need to be well informed. Like people within the community need to have more clear information to make the best decision for themselves

- Going back to people who make the decision. I want the person who are living in the house to know what decision is being made. So not just the person who owns the house, but the person living in the home. And not everyone it literate and not everyone speaks English. And its really important that you are giving them information they can actually consume. Instead of giving them notices they cant read

Council on Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington
Thursday, Feb. 21, 2019
Technology Discussed: Acyclica

1. Do you have concerns about this specific technology or how it's used?
    - Where does this data go? Does it go to SDOT? Google maps?
    - My other question is, it said whatever is being transferred is encrypted. All encrypted means to me is getting data from one device to another will be transferred without it being intercepted. What I don't know is, how much information are people getting
    - My concern is related to data, yeah we like to use gps. But what is the perimeter, what is the breach of access. Where is the data being used, and what can that turn into. we might be okay if the data is only being used for traffic related updates, but they might use it for more
    - I also would like to see how acyclica actually does what they do. They are using a lot of words that normally don't know. So I want to know how exactly they are hashing and salting. So for them to be clear about how they doing it. like when whatsapp encrypted they didn't give us the exact code but told us how they are doing it
    - Asking for a greater transparency for how they are doing this
    - I think the purpose of it is really important but the biggest concern is collecting all of this information without consent of passersby.
    - So the specific identifier that acyclica uses it mac addresses? You could potentially use that number to track that phone for the lifetime of the phone, for as long as that phone is on and being used. And that is very concerning.
    - Also I want to understand more where is this data going, and I want to know if this data is going to be used for future projects.
    - I want to ask is this something people opt into
    - People don't even know this is being used

2. What value do you think this brings to our city?
    - I like getting places and I like getting traffic information.
3. What worries you about how this is used?
    - What I don't like is you using my phone to get that information. I want whatever is in my cellphone to be protected. And I wanna know what you can access
    - I think based on Seattle and Seatac's higher up wanting to monitor and map out Muslims and where they are, and I don't like people being able to use our phone to track our location or actions they might think is violent. So based off of Seattle's track record and law enforcement agencies I don't like it
    - People who live outside of Seattle are also being impacted by it anytime they drive in Seattle
    - Could someone "opt out" by having wifi disabled on their device? I don't know if this covers cell towers. Because if it covers cell towers the only thing you could is having your phone on airplane mode

4. What recommendations would you give policy makers at the City about this technology?
    - I think the big question is why aren't we using other vendors, like I mentioned google maps, or waze, in fact komo 4 uses ways. Where other options we're looked at, and what were the trade off there's. And I want to see some transparency between the decision-making processes
    - I don't think this data should be shared with other private agencies, or other interagency programs
    - If all you're looking at is traffic flow, why are you not using the sensors in the road to give traffic flow updates.
    -
5. Can you imagine another way to solve the problem this technology solves?
    - I don't know if this already exists but something that makes it that data can't be used from one technology and use it for a different purposes
    - I think speaking from an industry perspective that is really important to have a processes for. Because all of this data is being used regardless of if you live in Seattle, or people live in different countries even who are visiting. That data is being collected. My understanding is that SDOT doesn't get the data directly. So my concern is how long can acyclica keep this data, use this data. Why wasn't a different option used, one in which some sort of consent can be used, so something like waze, google maps where people can opt in can get that information.
    - Road sensors or ways to count cars
    - I think its better to count cars than phones, because there is some expectation that your car will be monitored.
    - Using vehicle level granularity

Entre Hermanos

Please select which technology you wish to comment on:

☐SCL: Binoculars	☐SCL: Sensorlink Transformer Meter (TMS)	☐SFD: Computer-Aided Dispatch	☐SPD:9-11 Call Recorder
☐SCL: Sensorlink Ampstik	☒SDOT: Acyclica	☐SPD: Computer-Aided Dispatch	☐SPD: CopLogic

1) What concerns, if any, do you have about the use of this technology?

El uso de wifi en Acyclica porque pueden obtener toda la información de los teléfonos.

Si vale la pena la inversión

Enfocando al grupo: La tecnología ya está instalada. que les preocupa de su uso?

El tráfico sigue igual.

Quien usa o almacena la información.

La preocupación es la colección de data.

Colección y almacenamiento de información es la mayor preocupación.

No es la colección de data lo alarmante sino los recursos (dinero utilizado) ya que o la tecnología no están funcionando porque el tráfico sigue igual. No hay cambio con la nueva tecnología, esos gastos no son válidos ya que no hay resultados. Esos gastos pudieran ser utilizados para la comunidad.

También tienen que ver si la tecnología emite radiación o alguna otra cosa dañina; perjudicial a la salud.

El gobierno tiene todos los datos.

No necesitan esta tecnología para tener los datos porque ya existen métodos para eso, incluso aplicaciones o alguna otra cosa.

La otra preocupación del grupo es que no haya un cambio al problema que se quiere resolver. En el caso de Acrylica sería el mejorar el tráfico.

- Tecnologías como esta necesitan recolectar más opiniones de expertos.
- Sería bueno que la información sea compartida con la comunidad. (Transparencia en fines y objetivos de la tecnología y datos guardados, tácticas implementadas.)

2) What do you want City leadership to consider about the use of this technology?

Hay lugares donde no se necesitan. En algunas partes de Magnolia, Queen Anne, Northgate, no se ocupan.

Seguimiento de pregunta: En las comunidades donde viven los latinos que tanto se ocupa Acyclica?

Participante no cree que allí se ocupan.

Hablaron sobre la necesitad de puntos estratégicos y calles con más necesidad de ayuda por causa del tráfico.

What do you think about this technology in particular ?

Bien, la tecnología ayuda con la velocidad o el movimiento de los coches.

La información se guarda y analizan por donde viajas o cuantas veces cruzas este rastreo.

Si es solo para ver el tráfico está bien.

Está bien en algunas partes. Puede que sea algo bueno. Pero puede que esta tecnología pueda compartir información personal que puede ser utilizada de otra forma en especial si hay Hacking (forma negativa, uso de datos).

La tecnología en sí no es tan grande (de tamaño) para ser algo visualmente desagradable. La información captada a través de estos medios puede que ayude a conducir el tráfico de mejor manera pero también puede que tome información personal.

Are there any questions you have, or areas you would like more clarification? ●

La tecnología no es un router, sino colección de data para planeaciones urbanas.

Participante: “quiero creer” “convencerme” que los sensores están allí para ayudar con el tráfico.

No se sabe cuándo las instalaron, los resultados deberían de ser públicos. Si la tecnología es para aliviar el flujo de tráfico entonces por qué no extienden el programa? O por qué no hay mejoramiento del tráfico?

Alternatives to this technology

- Alguna pantalla que indique cuáles vías son alternativas puede reemplazar esto.

- Cambios al límite de velocidad puede que alivie el flujo del tráfico.
- Dejar de construir tanto.
- Rediseño de calles ayudaría flujo de tráfico.
- El rediseñar las vías servirá para las futuras generaciones.

City of Seattle

Entre Hermanos

Please select which technology you wish to comment on:

☒SCL: Binoculars ☒SCL: Sensorlink Transformer Meter (TMS) ☐SFD: Computer-Aided Dispatch ☐SPD:9-11 Call Recorder

☐SCL: Sensorlink Ampstik ☐SDOT: Acyclica ☐SPD: Computer-Aided Dispatch ☐SPD: CopLogic

1) What concerns, if any, do you have about the use of this technology?

Los binoculares son preocupantes si la persona no tiene ética. Es preocupante que una persona vea a través de binoculares a que una tecnología mida el uso de la electricidad

Al grupo le incomoda el uso de binoculares

Sensorlynk específicamente la preocupación sería que le quita el trabajo a una persona.

Si es para detectar robo el grupo cree que hay otras maneras de saber quien roba

que no tan solo será para leer la electricidad sino para obtener otros tipos de información si cámaras fueran usadas

2) What value, if any, do you see in the use of this technology?

Ahorro de energía

Record y datos mas precisos

Oportunidad de trabajo a quien utiliza los binoculares

Estabiliza los precios de la electricidad

3) What do you want City leadership to consider about the use of this technology?

: Usar background check, uso de uniforme por trabajadores, cámara en binoculares.

What do you think about this technology in particular ?

Sensorlink Si

Binoculares son invasivos

Are there any questions you have, or areas you would like more clarification? ●

La confianza en estos medidores serán confiables? Serán efectivos?

El uso de binoculares se puede acompañar de una cámara añadida

Alternatives to this technology

Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad

Entre Hermanos

Please select which technology you wish to comment on:

☐SCL: Binoculars ☐SCL: Sensorlink Transformer Meter (TMS) ☐SFD: Computer-Aided Dispatch ☐SPD:9-11 Call Recorder

☐SCL: Sensorlink Ampstik ☐SDOT: Acyclica ☐SPD: Computer-Aided Dispatch ☒SPD: CopLogic

1) What concerns, if any, do you have about the use of this technology?

Las fallas electrónicas son preocupantes especialmente en reportes policiacos.

Las preocupaciones es que el reporte no salió, no llegó por cualquier razón.

No todos podrán o saben usar las computadoras.

Fallas de los algoritmos de cada demanda es alarmante.

Que y cuando determina la urgencia de respuesta

Las personas le temen a los policías. Y este medio puede ayudar a que el miedo disminuya.

La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

2) What value, if any, do you see in the use of this technology?

La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

El uso de computadora está bien para las denuncias.

Si personas usan esta tecnología y es analizada en tiempo real por otras personas no hay problema.

Es otro método para denunciar

Está de acuerdo con el uso de computadoras para denunciar solo que no todos son capaz de usar este método/tecnología.

3) What do you want City leadership to consider about the use of this technology?
Que sea multi-idioma, implementar audio, implementar sistemas que ayuden a múltiples personas con diversas capacidades/necesidades

Si es usada de manera adecuada y como han dicho está bien.

El uso de la tecnología es bueno para dar respuesta para todas las cosas y personas

What do you think about this technology in particular ?

Grupo están de acuerdo con su uso.

Puede salvar una vida.

Los riesgos y acciones determinan la urgencia de la intermisión policiaca.

Alguna gente se siente más capaz de presentar una queja a través de este sistema, la tecnología en uso tiene validez.

Bueno para la violencia doméstica.

Are there any questions you have, or areas you would like more clarification?

La computadora decidirá la importancia/urgencia del reporte/emergencia dando a llevar acciones de emergencia.

Gravedad de emergencia es determina por tecnología.

La definición de emergencia es diferente con cada persona.

Cada uno tiene la definición de vigilancia, pero ¿que tal la definición de emergencia?

SITUATIONS TO APPLY ITS USE

Una pelea en la calle, un malestar corporal, cuestiones de vida, abuso doméstico

Si nos basamos en la definición de emergencia sólo en cuanto estemos en peligro inmediato o en tiempos mínimos/ de transcurrencia alarmante/peligrosa el uso de será implementado o limitado solo a instantes inmediatos de peligro.

Para reportar algo que ya sucedió o que son recurrentes.

Basado en el concepto de emergencia, las personas pueden tomar el método adecuado para reportar su caso y a través del medio necesario.

Los reportes no son anónimos.

Los datos son recolectados aun, a pesar de la opción escogida.

Alternatives to this technology

Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad

Entre Hermanos

City of Seattle
Surveillance

Inicio

Resumen: El departamento de vecindarios quiere saber la opinión de este grupo. Ellos verán videos de un minuto y medio y encontrarán folletos en sus mesas donde encontraran más información sobre lo visto.

Demográficos:

Ocho personas participaron, una de West Seattle, una de First Hill, dos de Ravenna/Laurelhurst y cuatro de King County (outside Seattle).

Cuatro personas se consideraron hispano o latino, una como india americana o nativa de Alaska, y tres no opinaron.

Cinco personas marcaron 18-44 como su rango de edad, dos marcaron 45-64 como el suyo y una no opinó.

Cinco personas marcaron masculino como género, una como transgénero, una como femenino, y otra no opinó.

Otra Información Importante:

- Preguntas serán hechas.
- Habrá una hoja para poder conversar sobre videos de interés
- Se les agradeció por venir.
- El concepto de vigilancia será manejado como la ciudad de Seattle lo maneja.
- Tom: Agradeció a los invitados por venir

Surveillance. In 2017 city council passed an ordinance to see what technology fit the definition of surveillance. The information gathered by these surveillance technologies are as follows: to “observe or analyze the movements, behaviors, or actions of identifiable individuals in a manner” which "is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice.”

Presentador: Preguntó si la conversación en inglés fue entendida.

Grupo: Concordó.

Tom: Do not let information on videos stop you from making comments or raising questions.

Presentador: Dio a entender el concepto de vigilancia como ha sido interpretada por la ciudad de Seattle. Fue analizada de esta manera: “La vigilancia es definida como tecnologías que observan o analizan los movimientos, comportamientos, o acciones de individuales identificables de una manera que razonablemente levanta inquietudes sobre libertades civiles, la libertad de expresión o asociación, igualdad racial o justicia social.”

- Los movimientos de la gente son observados a través de esta tecnología y puede que para algunas personas esto sea incómodo.
- Las cámaras de policía no califican como tecnologías de vigilancia en este tema.
- La presentación mostrada en la pantalla a través de los videos será transmitida en inglés.
- Se pidió que todos se traten con respeto y que opinen y que su nombre sea mencionado e incluso la vecindad donde viven.

El Grupo

Participante vino porque quiere obtener más información y dar su opinión. Es de Seattle.

Participante viene de Shoreline/Seattle para ver cuánto la tecnología entra afecta

Participante vino porque quiere saber qué información es colectada por el gobierno y para qué usan esa información. Puede que la información obtenida a través de la tecnología sea usada para perseguir a personas de color/minorías/personas marginadas.

Participante vino de First Hill, porque quiere ver el punto de vista de la ciudad y ver que opiniones surgirán.

Participante viene de Seatac porque tiene interés en el tema y porque la seguridad es importante y quiere saber a dónde llega la información.

Participante vine en Ravenna/Northgate, quiere ver que tan confiable es la tecnología y para qué es utilizada. Perjudicial o beneficial?

Participante vine en Seatac y vino porque es un tema muy interesante ya que se tiene que saber/mantener informado de lo que hacen los gobernantes.

Participante vino de Burien por la importancia del tema y la privacidad.

Presentador: La tecnología no es nueva. Ya está siendo usada. Y quieren saber el formato para que las futuras tecnologías tengan.

El video de Seattle Department of Transportation de Acyclica fue mostrado

Esta tecnología es un sensor que detecta el wifi. Es un sensor que detecta la tecnología wifi.

Seattle Metering Tool fue mostrada

Nadie del grupo sabe del tema más el presentador no hablará a fondo de esto para no influenciar opiniones.

Video de Fire Department's Computer Aided Dispatch fue mostrado

El 9-1-1 logging recorder video fue mostrado

Aclaración: Información impresa fue entregada explicando cada una de las tecnologías.

Video de Coplogic fue mostrado

El grupo no conocía que se puede reportar a la policía a través de su página/en línea.

El video de Seattle Police Computer Aided Dispatch fue mostrado

Esta tecnología es similar a la de los bomberos.

Se preguntó cuál video era de interés para analizar

Se acordó el análisis de Acyclica, Binoculares/Sensorlink, y Coplogic

Las Preguntas que sea harán serán las siguientes:

¿Qué piensan de este sistema de tecnología en específico y el motivo de usarla?
¿Cuál creen que sea el aporte de esta tecnología a la cuidad?
¿Qué preocupación les causa el uso que se le dará a este sistema?
¿Qué recomendarían a el grupo de políticos de la cuidad responsables de tomar las decisiones de implementar estas tecnologías?
¿Qué otra manera habría de resolver el problema que esta tecnología esta designada a resolver?

La Acyclica

Pregunta: ¿Qué piensan de este sistema de tecnología en específico y el motivo de usarla? (Como se usa y cuál es el uso)

- Bien, la tecnología ayuda con la velocidad o el movimiento de los coches.
- La información se guarda y analizan por donde viajas o cuantas veces cruzas este rastreo.
- Si es solo para ver el tráfico está bien.

- Está bien en algunas partes. Puede que sea algo bueno. Pero puede que esta tecnología pueda compartir información personal que puede ser utilizada de otra forma en especial si hay Hacking (forma negativa, uso de datos).

- La tecnología en sí no es tan grande (de tamaño) para ser algo visualmente desagradable. La información captada a través de estos medios puede que ayude a conducir el tráfico de mejor manera pero también puede que tome información personal.

Pregunta: Qué es lo que aporta esta tecnología a la ciudad?

- Seria algo bueno el aporte por la agilidad del tráfico solo si la tecnología está sincronizada con los semáforos, de otra manera no es útil si no aporta para el mejoramiento del tráfico.

- Participante dice que hay alternativas para esquivar el tráfico.

- Participante opina que la tecnología es interesante ya que usa google maps y está de acuerdo con el mejoramiento del tráfico.

- Si el objetivo es de mejorar el tráfico está de acuerdo. Pero también quiere saber en qué lugar(es) estarán los aparatos, si algunas personas serán beneficiadas más que otras.

Pregunta: Qué preocupaciones tienen con posible uso/uso potencial de esta tecnología?

- Le preocupa el uso de wifi en Acyclica porque pueden obtener toda la información de los teléfonos.

- Si el potencial puede ser aplicada a la inversión.

Enfocando al grupo: La tecnología ya está instalada, que les preocupa de su uso?

- El tráfico sigue igual.

- Quien usa o almacena la información.

- La preocupación es la colección de data.

Más de la mitad de grupo opina que esa (el almacén y colección de información) es la preocupación.

- Participante no está de acuerdo. No es la colección de data lo alarmante sino los recursos (dinero utilizado) ya que o la tecnología no están funcionando porque el tráfico sigue igual. No hay cambio con la nueva tecnología, esos gastos no son válidos ya que no hay resultados. Esos gastos pudieran ser utilizados para la comunidad.

- También tienen que ver si la tecnología emite radiación o alguna otra cosa dañina; perjudicial a la salud.

- El gobierno tiene todos los datos.

- Opinión de otro participante: No necesitan esta tecnología para tener los datos porque ya existen métodos para eso, incluso aplicaciones o alguna otra cosa.

La otra preocupación del grupo es que no haya un cambio al problema que se quiere resolver. En el caso de Acrylica sería el mejorar el tráfico.

- Tecnologías como esta necesitan recolectar más opiniones de expertos.

- Sería bueno que la información sea compartida con la comunidad. (Transparencia en fines y objetivos de la tecnología y datos guardados, tácticas implementadas.)

Pregunta: Le dirían algo a los políticos algo del lugar donde se encuentran estos aparatos?

- Hay lugares donde no se necesitan. En algunas partes de Magnolia, Queen Anne, Northgate, no se ocupan.

Seguimiento de pregunta: En las comunidades donde viven los latinos que tanto se ocupa Acyclica?

- Participante no cree que allí se ocupan.

Hablaron sobre la necesitad de puntos estratégicos y calles con más necesidad de ayuda por causa del tráfico.

Presentrador: Crees que Acylica es como el router de google?

- La tecnología no es un router, sino colección de data para planeaciones urbanas.

- Participante: “quiero creer” “convencerme” que los sensores están allí para ayudar con el tráfico.

- No se sabe cuándo las instalaron, los resultados deberían de ser públicos. Si la tecnología es para aliviar el flujo de tráfico entonces por qué no extienden el programa? O por qué no hay mejoramiento del tráfico?

Otra pregunta: Alguna otra tecnología que pueda ser utilizada en vez de Acyclica?

Alternativas:

- Alguna pantalla que indique cuáles vías son alternativas puede reemplazar esto.
- Cambios al límite de velocidad puede que alivie el flujo del tráfico.
- Dejar de construir tanto.
- Rediseño de calles ayudaría flujo de tráfico.
- El rediseñar las vías servirá para las futuras generaciones.

Tecnologia #2

Sensorlink/Binoculares

Pregunta: Que opina el grupo de la tecnología?

- Los binoculares son preocupantes si la persona no tiene ética. Es preocupante que una persona vea a través de binoculares a que una tecnología mida el uso de la electricidad.

- Un sensor que detecta la electricidad sería mejor.

- Al grupo le incomoda el uso de binoculares.

Pregunta: Qué opinas sobre la tecnología medidora de electricidad (sensorlink) y que sea usada en tu casa?

- No le incomoda o afecta a dos participantes.

- La preocupación sería que le quita el trabajo a una persona.

- Los binoculares son invasivos.

- Para que usar binoculares si es que se puede llegar a el hogar y ver el medidor en persona, pidiendo permiso? Si la tecnología es usa para ver que las personas se roban la electricidad, creen que no saben quiénes roban?

- El grupo cree que si saben.

Pregunta: Cual creen que sea el aporte que esta tecnología?

- El video dice que 3 millones de dólares son ahorrados.

Pregunta: De qué manera beneficia esto a la cuidad/ciudadanos/comunidad?

- El robo de la luz es preocupante.

- Si ya llevan el record y datos y le hacen saber a la comunidad puede que ahorren dinero.

- Uso de binoculares puede dar trabajo a una persona y dinero puede ser ahorrado con esta tecnología.

- La tecnología trae gasto de electricidad para poder ver gastos de luz? Si pretende evitar el robo entonces los gastos de la factura eléctrica deberían de seguir estables.

Pregunta: La confianza en estos medidores serán confiables? Serán efectivos?

- Ayuda a la precisión, a bajar precios.

- Que quiten los binoculares sería una sugerencia, o usar binoculares que graban con video.

- Si ya tienen récord sobre la energía (consumo, gastos, etc.), el robo de energía no es suficiente para establecer este tipo de tecnología ya que puede ser identificado el robo o alguna otra anomalía dependiendo en el nivel alto o bajo o repentino analizado/visto/detectado por métodos convencionales ya establecidos.

- Otra recomendación: Usar background check, uso de uniforme por trabajadores, cámara en binoculares.

- Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad

- .La preocupación es que no tan solo será para leer la electricidad sino para obtener otros tipos de información si cámaras fueran usadas.

Tecnologia #3 Coplogic

- Esta tecnología no solo el ahorro de tiempo, sino el ahorro de tiempo policial ya que ellos trabajarían en otras cosas

- El uso de computadora está bien para las denuncias.

- Si personas usan esta tecnología y es analizada en tiempo real por otras personas no hay problema.

Enfoque: Lo que estamos queriendo dialogar es el uso del internet y las denuncias.

- Es otro método para denunciar

- Está de acuerdo con el uso de computadoras para denunciar solo que no todos son capaz de usar este método/tecnología.

Pregunta: En que ayuda a la comunidad?

- Por qué usar estos métodos?
- Grupo están de acuerdo con su uso.
- Puede salvar una vida.
- Los riesgos y acciones determinan la urgencia de la intermisión policiaca.
- Alguna gente se siente más capaz de acudir a través de este sistema la tecnología en uso tiene validez.
- Bueno para la violencia doméstica.
- Las fallas electrónicas son preocupantes especialmente en reportes policiacos.
- Las preocupaciones es que el reporte no salió, no llegó por cualquier razón.
- No todos podrán o saben usar las computadoras.
- Fallas de los algoritmos o cuando o que promueve urgencia de cada demanda es alarmante.
- Criterio de demandas y que clase de preocupación de parámetros son confiables tienen que ser cuestionados/analizados, y que/quien es digno de prioridad o importancia o de ayuda.

Pregunta: De qué manera este uso beneficiaria a la comunidad?

- Personas pueden ser discriminadas
- Las personas le temen a los policías. Y este medio puede ayudar a que el miedo disminuya.
- La computadora decidirá la importancia/urgencia del reporte/emergencia dando a llevar acciones de emergencia.
- Gravedad de emergencia determina uso de tecnología.

Pregunta: Alguna inquietud sobre el uso de esta tecnología?

- La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

Pregunta: En qué situación usarán esta tecnología?

- Una pelea en la calle, un malestar corporal, cuestiones de vida, abuso doméstico
- Cada uno tiene la definición de vigilancia, pero que tal la definición de emergencia?
- La definición de emergencia es diferente con cada persona.
- Si nos basamos en la definición de emergencia sólo en cuanto estemos en peligro inmediato o en tiempos mínimos/ de transcurrencia alarmante/peligrosa el uso de será implementado o limitado solo a instantes inmediatos de peligro

Pregunta: Para qué sirve el reporte de la computadora?

- Para reportar algo que ya sucedió o que son recurrentes.
- Basado en el concepto de emergencia, las personas pueden tomar el método adecuado para reportar su caso y a través del medio necesario.
- Los reportes no son anónimos.
- Los datos son recolectados aun, a pesar de la opción escogida.

Pregunta: Qué les recomendarían a los políticos?

- Que sea multi-idioma, implementar audio, implementar sistemas que ayuden a múltiples personas con diversas capacidades/necesidades

Pregunta: Algún otro comentario en general sobre la tecnología de vigilancia?

- Si es usada de manera adecuada y como han dicho está bien.

- El uso de la tecnología es bueno para dar respuesta para todas las cosas y personas.

Consejo:

- Den información más información sobre lo que están haciendo. (transparencia/divulgación de información)

- Que haya más transparencia.

Ser transparentes sobre la colección de datos, para que haya discusiones y decisiones Informadas, en todas las tecnologías implementadas/por implementar.

Byrd Barr Place

2/28/2019 Surveillance Technology Focus Group

Thursday, February 28, 2019
1:42 PM

Disclaimer: some of these notes are written in first-person. These should not be considered direct quotes

Videos:

- Acyclica: sensors recognize when a wifi enabled device is in range of it. Attached to street lights
- 911 recorder: records the conversation with the person calling 911, and conversation with the dispatched officers
- CopLogic: Online police report, treated as a regular policy report
- Computer Aided Dispatch
- Seattle City Light: Binoculars for meter readers; sensor to see if someone is stealing electricity

Tom: Read definition of surveillance

Craig: invasion of privacy?

- Electric one: I never even know they had the sensor one.

Community Member: used to be in the tech industry for thirty years. Writing a book about surveillance and technology
Wanda: I like the online police report. If someone is experiencing a crisis or trauma, you can go ahead and report it.

- Surveillance, I understand the concern, but overall I think it's a good thing. There is good and bad in any location, you'll find people who are taking advantage of it, but hopefully there are systems in place.
- Used to work nights, and catching the bus at night is scary. Having the cameras and police out when catching the bus helps, I appreciate that. No one likes to be watched, but if it's gonna keep people safe, that's a good thing.

Mercy: security is a great safety issue
Craig: there are some parts of the neighborhood/city that need to be watched, and some that need to be left alone
Wanda: as long as it's even
Craig: Sometimes it's not even
Both: There are hot spots though

Which of the surveillance technologies do you think could be abused to pinpoint specific communities?

IG: The Computer Aided Dispatch

Talking about the International District:

- Lots of businesses and residential crammed together in a larger space
- Talking about a great community member who died; if they had surveillance technology them, maybe they would have found his killer

"Some neighborhoods need to be watched"

- Gangs; drug use

Tom: getting back to CAD, how do we feel about the information that is stored

- Craig: there are concerns, but who is allowed to see it, how is it stored? That's a concern
    - Is it used for BOLOs? Is it everyone who is in the area, all of the police officers? Or is there some discretion as to which police officers would be given the information?
- Wanda: plenty of people are arrested who "fit a description"
    - Discussion about the racial discrimination: how people who think that "all [insert race here] look alike".
    - Individuals may think like that, but police officers have the capability to ruin someone's life.
- Marjorie: just recently got a smart phone, and it's new to me that someone could know where I'm going and I wouldn't be aware of it
    - Without my consent.
- Mercy: grew up with the idea that big brother is watching you
    - Tracking how many times I go to the library seems like a waste of money
    - People who are not law abiding citizens, they are the ones to be worried
- Craig: What about selling weed, coke, etc. Should they be worried?
    - Mercy: well at least in Seattle, it's ok to sell
- Mercy: big brother is watching. We already know that, it's just more obvious now
- There is a lot of technology that we are not made aware of

Tom: So acyclica, is it worth it? Some people worried it's tracking, is it something that we can live without?

- Should we put up signs that this road is tracked?
    - Viron: Maybe
    - Mercy: let people out there know that you're on camera.
    - Viron: does it work if your device is not turned on?

Tom: what do you want to tell the city council about tech that is collecting personal information?

- Wanda: they should get our individual consent
- Martha: putting it on the ballot doesn't mean that you are getting individual consent, because if you vote no but it still passes, you didn't give your consent
- Deana: there are some places around Capitol Hill that I don't feel safe at at night
    - Talking about fire department responding to a fire in her building: when one building alarm system goes off, it goes directly to the fire department - affects multiple buildings.
        - Response time is very good.
    - I choose to turn off the GPS tracking, because I don't need people to know where I'm at
        - If others are watching where I'm at, that's an invasion of privacy. I should be able to walk out my front door and go wherever I want without anyone knowing.
- Location privacy: you can tell a lot about a person based on where they go, and tracking that can build a pretty extensive profile of who you are
- IG: now that I know they are tracking, I will turn it off.

Mr. Surveillance: Surveillance is always secret, and it's an aggressive act. It's meant to exert power over others.

Do you think any individual could raise enough concern that it would change anything?

- Resounding no
- Maybe with a larger group
    - Maybe with the whole city

SCL binoculars:

- Craig: they should warn their customers and let them know they are coming into their yard/looking through binoculars.
- Wanda: as long as they aren't looking in people's windows.
    - When we're walking down the street, it's a little different. Certain neighborhoods do need more surveillance than others

Regarding being watched in public:

- Eydie: in public, it depends on how long. If it's a short period of time, that's one thing, but if you're tracked the whole time you're out, it's unreasonable.
    - I don't know what the solutions would be.
    - Even when the meter read just walks into your yard, it's unnerving.
    - What's the purpose of tracking it this way?
- Mercy: (referring to the acyclica) Why are they doing it all the time? Have they not gotten the information yet?
    - They should already know what the traffic flow would be.
    - We lost a lane to the bicyclist
- Craig: facial recognition used on the street is bad.
- Vyron: sometimes you can't walk down the street and shake someone's hand without getting in trouble
- Mr. Surveillance: The technology has gotten ahead of the law, and it means they have to pay less people

Tom: Are we willing to accept more technology to have less police?

- Craig: how about just making it even? Police have an image to people of color; they are afraid of why they are going to be there. We can police ourselves
- Wanda: I disagree. There are some who think there should be less, but there are also a lot of people who worry about walking down the street
    - As a woman and DV survivor, I appreciate the police and appreciate living in a country where I can call a number for help.
    - I have a big problem with the shooting of unarmed black men, but as an individual I still appreciate the police.
    - But I have a problem being tracked, and I have a problem being watched in my home.
- General comment: The number of police being on the corner is a touchy situation

- Knowing the police that are on your corner makes a difference. They can police the community better if there is more of a relationship between the two.
- Craig: it has to be both, even. You can't trade off the technology for the police.
- Mr. Surveillance: The trend is they want to go to more technology and less police.

Tom: If right now we have lots of technology, and we want a balance, then how do we do that?

- Craig: keep it the way it is but clean up the police department. Make sure the people who are working there are good at their jobs, not biased or discriminating

CopLogic: making police reports online

- Craig: I think it's stupid.
  - Would use that technology for stupid crimes
- Mercy: you could report your neighbor for silly things
  - Anonymous reporting of crimes that could target people for things they might not call 911 for
- Wanda: there were some lines of traffic where I saw cars lined up with their windows smashed in; nothing taken, but glass all over the place.
  - Police response when called: maybe you should get a cheaper type of car
  - Would he have said that to us if we were a different skin color, or lived in a different neighborhood?
- IG: I think it's a bad thing: someone could make up a story and the officer didn't have to check it.
- Marjorie: I think the online reporting could be abused

City of Seattle

Appendix E: All Comments Received from Members of the Public

ID: 10617592348
Submitted Through: Survey Monkey
Date: 3/25/2019 12:51:06 PM
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Sensorlink Check Meter Device
What concerns, if any, do you have about the use of this technology?
Medium Concern: The draft SIR says that the data is retrieved from the device "via secure radio protocol", but the SIR never explains that in more detail. Radio frequencies are not inherently secure, so the SIR should specify how this communication channel is supposedly secured so as to prevent other (knowledgeable) passerby from retrieving the data. Other Concerns: Originally, one of my other concerns was that the Check Meter Device (aka SensorLink Transformer Meter System (TMS)) would collect more types of data and at a finer granularity of occurrence than what the normal functioning household meter would collect. However, the SCL staff at the SIR tech fair said it collects the same kinds of data as a normal meter, just that it's located upstream, thus addressing my concerns on that. With that in mind, most of my concerns are alleviated (aside from the radio protocol details) by the fact that the CDT crew is small ("five journey-level engineers"), the "CDT owns six SensorLink TMS units", that the "CDT only investigates specific, metered locations previously identified and properly documented as sites of suspected current diversion", and that mis-use/abuse of this technology would likely not be compliant with IBEW Local 77 & Energy Northwest's "Code of Excellence Program" (http://www.ibew77.com/Letter%20of%20Agreement%20IBEW%20Code%20of%20Excellence%20Energy%20NW.pdf). Additionally, even with those items in mind, SCL might be using the TMS devices and enforcement mechanisms at location/for households disproportionately based on race or other minority characteristics. To that end, I was happy to see in the SIR that "City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible." Hopefully, there are sufficient other programs/discounts for low-income individuals such that people never feel the need to resort to manipulating their electrical system (but I'm not familiar enough with SCL's offerings for low-income individuals, nor have I been low-income while living in Seattle, so I can't make that claim with 100% certainty).
What value, if any, do you see in the use of this technology?
There is a direct monetary cost to current diversion, thus identifying it and recouping the costs helps the city save money.
What do you want City leadership to consider about the use of this technology?
City leadership should ask to review SCL's "equity analysis of past enforcement locations". Additionally, (if not included in said analysis) City leadership should specifically inquire as to what percentage of people/households that were enforcement locations would also be considered low-income. If that percentage is high, then that likely means SCL may cause people to be jailed for effectively being poor (and resourceful); and SCL may have inadequate support offerings for people who are low-income.
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

ID: 10617585382
Submitted Through: Survey Monkey
Date: 3/25/2019 12:48:12 PM
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars / Spotting Scope
What concerns, if any, do you have about the use of this technology?
My concerns are largely alleviated by the fact that the "binoculars are standard, commercial-grade, unpowered binoculars...[without] any special enhancements requiring power (e.g., night-vision or video-recording capabilities)", the CDT crew is small ("five journey-level engineers"), the binoculars are used "for approximately one minute at a time in those cases where an initial investigation has been authorized by the Current Diversion Coordinator", they're only used " to read a meter from a distance when the CDT is otherwise unable to access physically the meter for the purpose of inspection upon suspected current diversion", and that mis-use/abuse of this technology would likely not be compliant with IBEW Local 77 & Energy Northwest's "Code of Excellence Program" (http://www.ibew77.com/Letter%20of%20Agreement%20IBEW%20Code%20of%20Excellence%20Energy%20NW.pdf). Additionally, even with those items in mind, SCL might be using the binoculars and enforcement mechanisms at location/for households disproportionately based on race or other minority characteristics. To that end, I was happy to see in the SIR that "City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible." All things considered then, I'm hopeful that SCL is on the right track. Hopefully, there are sufficient other programs/discounts for low-income individuals such that people never feel the need to resort to manipulating their electrical system (but I'm not familiar enough with SCL's offerings for low-income individuals, nor have I been low-income while living in Seattle, so I can't make that claim with 100% certainty).
What value, if any, do you see in the use of this technology?
There is a direct monetary cost to current diversion, thus identifying it and recouping the costs helps the city save money.
What do you want City leadership to consider about the use of this technology?
City leadership should ask to review SCL's "equity analysis of past enforcement locations". Additionally, (if not included in said analysis) City leadership should specifically inquire as to what percentage of people/households that were enforcement locations would also be considered low-income. If that percentage is high, then that likely means SCL may cause people to be jailed for effectively being poor (and resourceful); and SCL may have inadequate support offerings for people who are low-income.
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

City of Seattle

ID: 10617574681
Submitted Through: Survey Monkey
Date: 3/25/2019 12:45:12 PM
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Ampstick
What concerns, if any, do you have about the use of this technology?
My concerns are largely alleviated by the fact that there's only 4 Ampstick devices, "they are deployed by hand for approximately ten minutes at a time, only when suspected diversion cases occur", and can only measure one 'line' at a time. Additionally, even with those items in mind, SCL might be using the Ampsticks and enforcement mechanisms at location/for households disproportionately based on race or other minority characteristics. To that end, I was happy to see in the SIR that "City Light is undertaking an equity analysis of past enforcement locations and will be reviewing these to ensure that our existing policies and procedures are as equitable as possible." All things considered then, I'm hopeful that SCL is on the right track. Hopefully, there are sufficient other programs/discounts for low-income individuals such that people never feel the need to resort to manipulating their electrical system (but I'm not familiar enough with SCL's offerings for low-income individuals, nor have I been low-income while living in Seattle, so I can't make that claim with 100% certainty).
What value, if any, do you see in the use of this technology?
There is a direct monetary cost to current diversion, thus identifying it and recouping the costs helps the city save money.
What do you want City leadership to consider about the use of this technology?
City leadership should ask to review SCL's "equity analysis of past enforcement locations". Additionally, (if not included in said analysis) City leadership should specifically inquire as to what percentage of people/households that were enforcement locations would also be considered low-income. If that percentage is high, then that likely means SCL may cause people to be jailed for effectively being poor (and resourceful); and SCL may have inadequate support offerings for people who are low-income.
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

ID: 10617441686
Submitted Through: Survey Monkey
Date: 3/25/2019 11:51:11 AM
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars / Spotting Scope
What concerns, if any, do you have about the use of this technology?
none
What value, if any, do you see in the use of this technology?
It's a good way to spot problems and get readings.
What do you want City leadership to consider about the use of this technology?
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

ID: 10600927069
Submitted Through: Survey Monkey
Date: 3/18/2019
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars
What concerns, if any, do you have about the use of this technology?
What a joke. The city has spent millions of dollars converting to digital meters that automatically report usage. Nobody needs binoculars to read them!
What value, if any, do you see in the use of this technology?
Zero
What do you want City leadership to consider about the use of this technology?
Forget it.
Do you have any other comments?
No
Are there any questions you have, or areas you would like clarification?

ID: 10
Submitted Through: Focus Group
Date: 2/28/2019
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars
What concerns, if any, do you have about the use of this technology?
the use of the binoculars can be an invasion of privacy. Period of three days is too vast a window to give note. The lack of knowledge in different standards of privacy by different tenants
What value, if any, do you see in the use of this technology?
What do you want City leadership to consider about the use of this technology?
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

ID: 9
Submitted Through: Focus Group
Date: 2/28/2019
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars
What concerns, if any, do you have about the use of this technology?
ensure that all tenants are aware of the use of binoculars
What value, if any, do you see in the use of this technology?
none. It honestly appears outdated especially with automatic meters being available
What do you want City leadership to consider about the use of this technology?
I would recommend phasing it out completely. If not, ensure that all tenants know that this decision is being made for them.
Do you have any other comments?
I would not assume that all consumers are literate. Have other ways to communicate with individuals such as phone call, news outlets
Are there any questions you have, or areas you would like clarification?

ID: 3
Submitted Through: Focus Group
Date: 2/27/2019
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars, SCL: CheckMeter, SCL: AmpFork, SFD: CAD, SPD: CAD, SPD: 911 Logging Recorder
What concerns, if any, do you have about the use of this technology?
That would be good with advanced technology
What value, if any, do you see in the use of this technology?
Yes, around the city.
What do you want City leadership to consider about the use of this technology?
Need good train to people who use new technologies
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

ID: 10550713652
Submitted Through: Survey Monkey
Date: 2/23/2019 12:12:23 PM
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars
What concerns, if any, do you have about the use of this technology?
This is playing outrageous. Well we are telling the public is that it is okay for a city worker to come and use binoculars to look into your private property.
What value, if any, do you see in the use of this technology?
This really is barbaric there are certain technologies that their intermediate benefit might be greater than the risk that provide a much more simple solution then this solution. This solution a binocular use can possibly be interpreted for many things ho
What do you want City leadership to consider about the use of this technology?
It's just not right.
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

Appendix F: Department Responses to Public Inquiries

City Light received the following questions for Group 2 surveillance technologies during the public comment period of Feb. 5, 2019 to March 26, 2019. City Light's answers to the questions, which solely related to City Light's use of binoculars for current diversion detection, are presented below.

Do Seattle City Light Current Diversion employees wear something visible that shows customers they are from Seattle City Light?

Seattle City Light employees who are working in the field can be identified by their Seattle City Light ID badge and a hard hat.

If a City Light customer wants to file a complaint about a City Light employee, how do they do that?

A customer can file a complaint about a City Light employee by contacting Customer Care at (206) 684-3000, via email, mail, or in person at the Customer Service Center in the Seattle Municipal Tower located at 700 Fifth Ave., 4th floor lobby, Seattle, WA 98104.

Has there been a situation where a customer sees a City Light employee looking at someone's house with binoculars and the customer may not have been notified?

No advance notification is provided to the public, as doing so may compromise the detection of current diversion on a single, previously suspected service-drop location. Current Diversion staff view locations that are in public view, so it is possible other customers have observed this work. However, staff use binoculars for approximately one-minute at a time and only for City Light business purposes.

Has there been a situation where the meter was located on the opposite side of where the City Light employee was looking?

The Current Diversion team only investigates specific meters and other implicated electrical equipment at locations previously identified and documented as sites of suspected current diversion. Binoculars are used only to make determinations about whether current diversion is likely taking place, and, in certain instances, to view implicated and potentially dangerous electrical equipment.

Do City Light employees get background checks?

City Light conducts job-related background checks prior to hire in order to ensure a safe and secure work environment in which employees, the public, resources, and assets are protected, while protecting the integrity and confidentiality of information gathered during the evaluation. In most cases, a background check will be conducted for the finalist following a contingent offer of employment. Offer letters issued prior to completion of the background check will notify the finalist that the offer is contingent upon successful completion of any and all required background checks. In addition, City Light personnel whose work duties require having critical

access to City Light physical and logical assets must have a background check prior to being granted such access, which is renewed at least once every four years.

If a City Light customer files a complaint against an employee, are complaints being followed up? What is the average time for disciplinary action for a City Light employee? How long is the process for a full investigation?

Yes. City Light customer complaints about employee conduct are generally escalated to the People & Culture team at City Light for further action in order to ensure that City Light employees are serving customers reliably and with integrity. Appropriate next steps to address employee conduct are determined on a case-by-case basis. The complaining customer may not be informed of the specific action taken by City Light, due to the confidential nature of personnel matters. However, City Light is committed to employee accountability and providing excellent customer service.

When a full fact-finding investigation is necessary, it is City Light's objective to complete it as promptly as possible while ensuring that the investigation is fair, complete, and impartial. In the event of harassment, discrimination, or retaliation allegations, it is City Light's objective to complete investigations within 90 days unless compelling circumstances require more time. The duration of investigations is often dependent upon the availability and cooperation of witnesses, the volume of relevant documents, as well as the complexity of the subject-matter at issue. Resulting disciplinary and follow-up actions after an investigation are completed as promptly as possible while respecting the due process rights of City Light employees.

What is the purpose of tracking current diversion by using binoculars?

Binoculars may be used to address meter access issues, such as locked gates, unsafe premises, or threatening dogs. The binoculars enable Current Diversion staff to evaluate if a meter has been tampered with to substantiate suspicions of current diversion.

Appendix G: Letters from Organizations or Commissions

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

March 12th, 2019

Seattle City Council
600 4th Ave
Seattle, WA 98104

Re: Surveillance Ordinance Group 2 Public Comment

We would like to first thank City Council for passing one of the strongest surveillance technology policies in the country, and thank Seattle IT for facilitating this public review process.

These public comments were prepared by volunteers from the Community Technology Advisory Board (CTAB) Privacy & Cybersecurity Committee, as part of the surveillance technology review defined in Ordinance 125376. These volunteers range from published authors, to members of the Seattle Privacy Coalition, to industry experts with decades of experience in the information security and privacy sectors.

We reviewed and discussed the Group 2 Surveillance Impact Reports (SIRs) with a specific emphasis on privacy policy, access control, and data retention. Some recurring themes emerged, however, that we believe will benefit the City as a whole, independent of any specific technology:

- **Interdepartmental sharing of privacy best practices**: When we share what we've learned with each other, the overall health of the privacy ecosystem goes up.
- **Regular external security audits**: Coordinated by ITD (Seattle IT), routine third-party security audits are invaluable for both hosted-service vendors and on-premises systems.
- **Mergers and acquisitions**: These large, sometimes billion-dollar ownership changes introduce uncertainty. Any time a vendor, especially one with a hosted service, changes ownership, a thorough review of any privacy policy or contractual changes should be reviewed.
- **Remaining a Welcoming City**: As part of the Welcoming Cities Resolution, no department should comply with a request for information from Immigration and Customs Enforcement (ICE) without a criminal warrant. In addition, the privacy of all citizens should be protected equally and without consideration of their immigration status.

Sincerely,

Privacy & Cybersecurity Committee volunteers
Torgie Madison, Co-Chair
Smriti Chandashekar, Co-Chair
Camille Malonzo
Sean McLellan
Kevin Orme
Chris Prosser
Rabecca Rocha
Adam Shostack
T.J. Telan

Community Technology Advisory Board
Steven Maheshwary, CTAB Chair
Charlotte Lunday, CTAB Co-Vice Chair
Torgie Madison, CTAB Co-Vice Chair
Smriti Chandashekar, CTAB Member
Mark DeLoura, CTAB Member
John Krull, CTAB Member
Karia Wong, CTAB Member

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SFD: Computer-Aided Dispatch (CAD)

Comments

The use of a centralized Computer-Aided Dispatch (CAD) system is essential to protecting the health and safety for all Seattle citizens. The National Fire Protection Association (NFPA) standards outline specific alarm answering, turnout, and arrival times[1] that could only be accomplished in a city of this size with a CAD system.

In addition, with over 96,000 SFD responses per year (2017)[2], only a computerized system could meet the state's response reporting guidelines established in RCW 35A.92.030[3].

CentralSquare provides the dispatch service used by SFD. CentralSquare is a new entity resulting from the merger of Superion, TriTech, Zuercher, and Aptean[4] in September 2018.

Recommendations

- Tritech, the underlying technology supplying SFD with CAD services, has been in use since 2003 [SIR 4.3], making it 16 years old. As with any technology, advancements in security, speed, usefulness, and reliability come swiftly. Due to the age of the technology, we recommend conducting a survey into the plausibility of replacing Tritech as SFD's CAD solution.

- Tritech was merged very recently into CentralSquare in one of the largest-ever government technology mergers to date. Due diligence should be exercised to ensure that this vendor is keeping up to date with industry best practices for security and data protection, and that their privacy policies are still satisfactory after the CentralSquare merger. We recommend ensuring that the original contracts and privacy policies have remained unchanged as a result of this merger.

---

[1] "NFPA Standard 1710." https://services.prod.iaff.org/ContentFile/Get/30541
[2] "2017 annual report - Seattle.gov." https://www.seattle.gov/Documents/Departments/Fire/FINAL%20Annual%20Report_2017.pdf
[3] "RCW 35A.92.030: Policy statement—Service ... - Access WA.gov." https://app.leg.wa.gov/rcw/default.aspx?cite=35A.92.030
[4] "Superion, TriTech, Zuercher, and Aptean's Public Sector Business to " 5 Sep. 2018, https://www.tritech.com/news/superion-tritech-zuercher-and-apteans-public-sector-business-to-form-centra

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SDOT: Acyclica

Comments

Traffic congestion is an increasingly major issue for our city. Seattle is the fastest-growing major city in the US this decade, at 18.7% growth, or 114,00 new residents[5]. Seattle ranks sixth in the nation for traffic congestion[6]. The need for intelligent traffic shaping and development has never been greater. Acyclica, a service provided by Western Systems and now owned by FLIR[7], is an implementation of surveillance technology specifically designed to address this problem.

We were happy to see the 2015 independent audit of Acyclica's systems [SIR 8.2]. This is an excellent industry best practice, and one that we'll be recommending to other departments throughout this document.

In addition, we are pleased to see the hashing function's salt value rotated every 24-hours [SIR 4.10]. This ensures that even the 10-year retention policy [SIR 5.2] cannot be abused to correlate multiple commute sessions and individually identify a person.

Recommendations

- FLIR Systems' acquisition of Acyclica is a recent development (September 2018). We recommend verifying that the Western Systems terms [SIR 3.1] still apply. If they have been superseded by new terms from FLIR Systems, those should be subject to an audit by SDOT and Seattle IT. Specifically, section 2.5.1 of Western Systems' terms must still apply:

  > 2.5.1. It is the understanding of the City that the data gathered are encrypted to fully eliminate the possibility of identifying individuals or vehicles. In no event shall City or Western Systems and its subcontractors make any use of the data gathered by the devices for any purpose that would identify the individuals or vehicles included in the data.

- FLIR Systems is known primarily as an infrared technology vendor. Special care should be taken if FLIR/Acyclica attempt to couple IR scanning with WiFi/MAC sniffing. Implementation of an IR system would necessitate a new public surveillance review.

---

[5] "114,000 more people: Seattle now decade's fastest-growing big city in ...." 24 May. 2018, https://www.seattletimes.com/seattle-news/data/114000-more-people-seattle-now-this-decades-fastest-growing-big-city-in-all-of-united-states/
[6] "INRIX Global Traffic Scorecard." http://inrix.com/scorecard/
[7] "FLIR Systems Acquires Acyclica | FLIR Systems, Inc.." 11 Sep. 2018, http://investors.flir.com/news-releases/news-release-details/flir-systems-acquires-acyclica

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SCL: Binoculars, Check Meter, SensorLink

Comments

As these three technologies are serving the same team and mission objectives, we will review them here in a combined section.

The mission of the Current Diversion Team (CDT) is to investigate and gather evidence of illegal activity related to the redirection and consumption of electricity without paying for its use. As such, none of these technologies surveil the public at large. They instead target specific locations and equipment, albeit without the associated customer's knowledge.

It appears as though all data collected through the Check Meter Device and SensorLink Amp Fork are done without relying on a third-party service, so the usual scrutiny of a vendor's privacy policies does not apply.

Recommendations

- **Binoculars**: We have no recommendations for the use of binoculars.
- **Check Meter Device & SensorLink Amp Fork**: As noted in the comments above, we have no further recommendations for the use of the Check Meter Device and SensorLink Amp Fork technologies.
- **Racial Equity**: As with any city-wide monitoring practice, it can be easy to more closely scrutinize one neighborhood over another. Current diversion may be equally illegal (and equally prevalent) across the city, but the enforcement of this law may be unevenly applied. This could introduce racial bias by disproportionately burdening specific neighborhoods with a higher level of surveillance.

  As described, DPP 500 P III-416 section 5.2[8] asserts that all customers shall receive uniform consideration [SIR RET 1.7]. To ensure this policy is respected, we encourage City Light to track and routinely review the neighborhoods where CDT performs investigations, with a specific emphasis on racial equity. This information should be made publicly available.

  When asked at the February 27th Surveillance Technology public meeting, SDOT indicated that no tracking is currently being done on where current diversion is enforced.

[8] "SCL DPP 500 P III-416 Current Diversion - Seattle.gov." 11 Jan. 2012, http://www.seattle.gov/light/policies/docs/III-416%20Current%20Diversion.pdf

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: 911 Logging Recorder

Comments

This is a technology that the general public would likely already assume is in place. Some of the more sensational 911 call logs have been, for example, played routinely on the news around the country. Since it would not alarm the public to know that 911 call recording is taking place, our recommendations will focus primarily on data use, retention, and access control.

Call logging services are provided by NICE Ltd., an Israeli company founded in 1986. This vendor has had a troubling history with data breaches. For example, a severe vulnerability discovered in 2014 allowed unauthorized users full access to a NICE customer's databases and audio recordings[9]. Again, in 2017, a NICE-owned server was set up with public permissions, exposing phone numbers, names, and PINs of 6 million Verizon customers[10].

Recommendations

- SIR Appendix K includes a CJIS audit performed in 2017. SIR section 4.10 also mentions that ITD (Seattle IT) periodically performs routine monitoring of the SPD systems.

  However, given the problematic history with the quality of the technology vendor, if any of the NICE servers, networks, or applications were installed by the vendor (or installation was overseen/advised by the vendor), we recommend an external audit of the implementation of the call logging technology.

- SIR sections 3.3 and 4.2 outline the SPD-mandated access control and data retention policies, however it is not apparent if there is a policy that strictly locks down the use of this technology to a well-defined list of allowed cases. We recommend formally documenting the allowed 911 Logging use cases, and creating a new SIR for any new desired applications of this technology.

  With a 90-day retention policy [SIR 4.2], and with SPD receiving 900,000 calls per year[11], there are about 220,000 audio recordings existing at any given time. This is enough for a data mining, machine learning, or voice recognition project.

---

[9] "Backdoor in Call Monitoring, Surveillance Gear — Krebs on Security." 28 May. 2014, https://krebsonsecurity.com/2014/05/backdoor-in-call-monitoring-surveillance-gear/
[10] "Nice Systems exposes 14 million Verizon customers on open AWS ...." 12 Jul. 2017, https://www.techspot.com/news/70106-nice-systems-exposes-14-million-verizon-customers-open.html
[11] "9-1-1 Center - Police | seattle.gov." https://www.seattle.gov/police/about-us/about-policing/9-1-1-center

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: Computer-Aided Dispatch (CAD)

Comments

As mentioned in the section "SFD: Computer-Aided Dispatch (CAD)" and the section "SPD: 911 Logging Recorder", these dispatch technologies are mandatory for functional emergency services of a city this size. No other system would be able to meet the federal- and state-mandated response times and reporting requirements.

SIR section 4.10 mentions that ITD (Seattle IT) performs routine inspections of the Versaterm implementation.

Versaterm, founded in 1977, provides the technology used by SPD's CAD system. SPD purchased this technology in 2004. In September of 2016, there was a legal dispute between Versaterm and the City of Seattle over a Public Records Act (PRA) disclosure of certain training and operating manuals[12]. The court ruled in favor of Versaterm.

Recommendations

- It is not immediately clear what use cases are described in SIR 2.5 describing data access by "other civilian staff whose business needs require access to this data". All partnerships and data flows between SPD and businesses should be explicitly disclosed.

- This system has been in place for 15 years. As with any technology, advancements in security, speed, usefulness, and reliability come swiftly. Due to the age of the technology, and the potential damaged relationship between Seattle and Versaterm due to the aforementioned legal dispute, we recommend conducting a survey into the plausibility of replacing Versaterm as SPD's CAD solution.

- As mentioned in the introduction to this document, Seattle has adopted the Welcoming Cities Resolution[13]. In honoring this resolution, we recommend that SPD never disclose identifying information, from CAD or any system, to Immigrations and Customs Enforcement (ICE) without a criminal warrant.

---

[12] "Versaterm Inc. v. City of Seattle, CASE NO. C16-1217JLR | Casetext." 13 Sep. 2016, https://casetext.com/case/versaterm-inc-v-city-of-seattle-2
[13] "Welcoming Cities Resolution - Council | seattle.gov." http://www.seattle.gov/council/issues/past-issues/welcoming-cities-resolution

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: CopLogic

Comments

Track 1 - Public reporting of no-suspect, no-evidence, non-emergency crimes

CTAB understands that in cases where no evidence or suspect is available, a crime should be reported (for statistical or insurance purposes) but does not require the physical appearance of an SPD officer.

Track 2 - Retail Loss Prevention

This track is more problematic, as it could be used by retailers as a method to unreasonably detain, intimidate, or invade the privacy of a member of the public accused of, but not proven guilty of, shoplifting.

Recommendations

- **Track 2**: If not already done, retailers should be trained and informed that having a CopLogic login does not allow them to act as if they are law enforcement officers. Members of the public suspected of shoplifting need to have an accurate description of their rights in order to make informed decisions before providing identifying information. Retailers are also held to a lower standard than SPD regarding racial bias. It is virtually guaranteed that people of color are disproportionately apprehended and entered into the retail track of CopLogic.

  We recommend discontinuing Track 2 entirely.

- **Track 1 & 2**: If not already done, SPD, in coordination with Seattle IT, should perform or hire a company to perform an audit of the vendor's systems. If this audit has not been performed in the 8 years since purchasing this system, it should absolutely be done before the 10-year mark in 2020.
- **Track 1 & 2**: It is not immediately clear in the SIR or LexisNexis's Privacy Policy what CopLogic does with these records long-term, after SPD has imported them into their on-premises system. A written statement from LexisNexis on how this data is used, mined, or sold to affiliates/partners should be acquired by SPD.
- **Track 1 & 2**: We recommend migrating CopLogic to an on-premises solution. We found the LexisNexis privacy policy to be obfuscated and vague[14]. Such sensitive information should not be protected by trust alone.

[14] "Privacy Policy | LexisNexis." 7 May. 2018, https://www.lexisnexis.com/en-us/terms/privacy-policy.page

City of Seattle

March 20, 2019

RE: ACLU-WA Comments Regarding Group 2 Surveillance Technologies

Dear Seattle IT:

On behalf of the ACLU of Washington, I write to offer our comments on the surveillance technologies included in Group 2 of the Seattle Surveillance Ordinance process. We are submitting these comments by mail and electronically because they do not conform to the specific format of the online comment form provided on the CTO's website, and because the technologies form groups in which some comments apply to multiple technologies.

These comments should be considered preliminary, given that the Surveillance Impact Reports (SIR) for each technology leave a number of significant questions unanswered. Specific unanswered questions for each technology are noted in the comments relating to that technology, and it is our hope that those questions will be answered in the updated SIR provided to the Community Surveillance Working Group and to the City Council prior to their review of that technology. In addition to the SIR, our comments are also based on independent research relating to the technology at hand.

The 8 technologies in Group 2 are covered in the following order.

I. Acyclica (SDOT)

II. CopLogic (SPD)

III. Computer-Aided Dispatch & 911 Logging Recorder Group

1. Computer-Aided Dispatch (SPD)
2. Computer-Aided Dispatch (SFD)
3. 911 Logging Recorder (SPD)

IV. Current Diversion Technology Group

1. Check Meter Device (Seattle City Light)
2. SensorLink Amp Fork (Seattle City Light)
3. Binoculars/Spotting Scope (Seattle City Light)

ACLU
AMERICAN CIVIL LIBERTIES UNION
Washington

901 Fifth Ave, Suite #630
Seattle, WA 98164
(206) 624-2184
aclu-wa.org

Tana Lin
Board President

Michele Storms
Executive Director

Shankar Narayan
Technology & Liberty Project Director

City of Seattle

I. Acyclica - SDOT

Background

Acyclica technology is a powerful location-tracking technology that raises a number of civil liberties concerns because of its ability to uniquely identify individuals and their daily movements. Acyclica (via its hardware vendor, Western Systems), manufactures Intelligent Transportation System (ITS) sensors called RoadTrend that are used by the Seattle Department of Transportation for the stated purpose of traffic management. These RoadTrend sensors collect encrypted media access control (MAC) addresses, which are transmitted by any Wi-Fi enabled device including phones, cameras, laptops, and vehicles. Collection of MAC addresses, even when hashed (a method of de-identifying data irreversibly),[1] can present locational privacy challenges.

Experts analyzing a dataset of 1.5 million individuals found that just knowing four points of approximate spaces and times that individuals were near cell antennas or made a call were enough to uniquely identify 95% of individuals.[2] In the case of Acyclica's operation in Seattle, the dataset is comprised of MAC addresses recorded on at least 301 intersections,[3] which allows Acyclica to generate even more precise location information about individuals. Not only do the RoadTrend sensors pick up the MAC addresses of vehicle drivers and riders, but these sensors can also pick up the MAC addresses of all nearby individuals, including pedestrians, bicyclists, and people in close structures (e.g., apartments, offices, and hospitals). Acyclica technology's location tracking capabilities means that SDOT's use of Acyclica can not only uniquely identify individuals with ease, but can also create a detailed map of their movements. This raises privacy concerns for Seattle residents, who may be tracked without their consent by this technology while going about their daily lives.

These location-tracking concerns are exacerbated by the lack of clarity around whether SDOT has a contract with Acyclica (see below). Without a contract, data ownership and scope of data sharing and repurposing by Acyclica is unclear. For example, without contractual restrictions, Acyclica

[1] Hashing is a one-way function that scrambles plain text to produce a unique message digest. Unlike encryption—which is a two-way function, allowing for decryption—what is hashed cannot be un-hashed. However, hashed location data can still be used to uniquely identify individuals. While it is infeasible to compute an input given only its hash output, pre-computing a table of hashes is possible. These types of tables consisting of pre-computed hashes and their inputs are called rainbow tables. With a rainbow table, if an entity has a hash, then they only need to look up that hash in their table to then know what the original MAC address was.
[2] Montjoye, Y., Hidalgo, C., Verleysen, M., and Blondel, V. 2013. Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports.* 3:1375.
[3] The SIR states that SDOT has 301 Acyclica units installed throughout the City. However, an attached location excel sheet in Section 2.1 lists 389 Acyclica units, but only specifies 300 locations.

would be able to share the raw data (i.e., the non-aggregated, hashed data before it is summarized and sent to SDOT) with any third parties, and these third parties would be able to use the data in any way they see fit, including combining the data with additional data such as license plate reader or facial recognition data. Acyclica could also share the data with law enforcement agencies that may repurpose the data, as has happened with other City data. For example, in 2018, U.S. Immigration and Customs Enforcement (ICE) approached Seattle City Light with an administrative subpoena demanding information on a particular customer location, including phone numbers and information on related accounts.[4] ICE also now has agency-wide access to a nationwide network of license plate readers controlled by Vigilant Solutions,[5] indicating the agency may seek additional location data for immigration enforcement purposes in the future. Data collected via Acyclica should never be used for law enforcement purposes.

The uncertainty around the presence or absence of a contract contributes to two key issues: (1) lack of a clearly defined purpose of use of Acyclica technology; and (2) lack of clear restrictions on the use of Acyclica technology that track that purpose. With no contract, SDOT cannot enforce policies restricting the use of Acyclica technology to the intended purpose.

There are also a number of contradictory statements in the SIR concerning the operation of Acyclica technology,[6] as well as discrepancies between the SIR, the information shared at the technology fair (the first public meeting to discuss the Group 2 technologies),[7] and ACLU-WA's conversation with the President of Acyclica, Daniel Benhammou. All these leave us with concerns over whether SDOT fully understands (and the SIR reflects) the capabilities of the technology. In addition, there remain a number of critical unanswered questions that the final SIR must address (set forth below).

Of additional concern is the recent acquisition of Acyclica by FLIR Systems, an infrared and thermal imaging company funded by the U.S. Department of Defense.[8] As of March 2019, FLIR has discontinued Acyclica RoadTrend sensors.[9] Neither the implications of the FLIR acquisition nor the discontinuation of the RoadTrend sensors are mentioned in the SIR—but if the sensors used will change, the SIR should make clear how that will impact the technology.

a. Specific Concerns

- *Inadequate Policies Defining Purpose of Use.* Policies cited in the SIR are vague,

[4] https://crosscut.com/2018/02/immigration-officials-subpoena-city-light-customer-info
[5] https://www.theverge.com/2018/3/1/17067188/ice-license-plate-data-california-vigilant-solutions-alpr-sanctuary
[6] Explained in further detail in 1. Acyclica – SDOT *Major Concerns* below.
[7] http://www.seattle.gov/tech/initiatives/privacy/events-calendar#/pi=3
[8] https://www.crunchbase.com/acquisition/flir-systems-acquires-acyclica--e6043a1a#section-overview
[9] https://www.flir.com/support/products/roadtrend#Specifications

short, and impose no meaningful restrictions on the purposes for which Acyclica devices may be used.[10] Section 1.1 of the abstract set forth in the SIR states that Acyclica is used by over 50 agencies to "to help to monitor and improve traffic congestion." Section 2.1 is similarly vague, providing what appear to be examples of some types of information the technology produces (e.g., calculated average speeds) in order to facilitate outcomes (correcting traffic signal timing, providing information to travelers about expected delays, and allowing SDOT to meet traffic records and reporting requirements)—but it's not clear this list is exhaustive. Section 2.1 fails to describe the purpose of use, all the types of information Acyclica provides, and all the types of work that Acyclica technology facilitates. All these must be clarified.

- *Lack of Clarity on Whether Acyclica and SDOT have a Written Contract.* The SIR does not state that any contract exists, and in the 2018 conversation ACLU-WA had with Benhammou, he stated that there was no contract between the two parties. However, at the 2019 technology fair, the SDOT representative affirmatively stated that SDOT has a contract with Acyclica. As previously mentioned, the lack of a contract limits SDOT's ability to restrict the scope of data sharing and repurposing. The only contractual document provided appears to be a terms sheet in Section 3.0 detailing SDOT's terms of service with Western Systems (the hardware vendor that manufactures the Acyclica RoadTrend sensors), which states that Western Systems only deals with the maintenance and replacement of the hardware used to gather the data, and not the data itself.

- *Lack of Clarity on Data Ownership.* At the technology fair, the SDOT representative stated that SDOT owns all the data collected (including the raw data), but the SIR only states that the aggregated traffic data is owned by SDOT. In the 2018 conversation, Benhammou stated that Acyclica owns all the raw data. There is an apparent lack of clarity between SDOT and Acyclica concerning ownership of data that must be addressed.

- *Data Retention Periods are Unclear.* Section 5.2 of the SIR states that there is a 10-year internal deletion requirement for the aggregated traffic data owned by SDOT, but pg. 37 of the SIR states that "the data is deleted within 24 hours to prevent tracking devices over time." In the 2018 interview, Benhammou stated that Acyclica retains all non-aggregated data indefinitely. It is unclear whether the different retention periods stated in the SIR are referring to different types of data. The lack of clarity on data retention periods also relates to the lack of clarity on data ownership given that data retention periods may depend on data ownership.

[10] As noted in 1. Acyclica – SDOT *Background* above.

- *Inaccurate Descriptions of Anonymization/Data Security Practices.* The SIR appears to use the terms "encryption" and "hashing" interchangeably in some parts of the SIR, making it difficult to clearly understand Acyclica's practices in this area. For example, Section 7.2 states: "Contractually, Acyclica guarantees that the data gathered is encrypted to fully eliminate the possibility of identifying individuals or vehicles." But by design, encryption allows for decryption with a key, meaning anyone with that key and access to the data can identify individuals. (Also, if there is no contract between SDOT and Acyclica, the use of 'contractually' is misleading). This language is also used in the terms sheet detailing SDOT's contract with Western Systems (in Section 2.5.1 in the embedded contract). The SIR compounds this confusion with additional contradictory statements. For example, the SIR states in multiple sections that the data collected by the RoadTrend sensors are encrypted and hashed on the actual sensor. However, according to a letter from Benhammou provided by SDOT representatives at the technology fair,[11] the data is never hashed on the sensor—the data is only hashed after being transmitted to Acyclica's cloud server. These contradictory descriptions cause concern.

- *No Restrictions on Non-City Data Use.* Section 6.3 of the SIR states that there are no restrictions on non-City data use. However, there are no policies cited making clear the criteria for such use, any inter-agency agreements governing sharing of Acyclica data with non-City parties, or why the data must be shared in the first place.

- *Not All Locations of Acyclica Devices are Specified.* Section 2.1 of the SIR states that there are 301 Acyclica locations in Seattle. However, in the embedded excel sheet detailing the serial numbers and specific intersections in which Acyclica devices are installed, there are 389 serial numbers, but only 300 addresses/locations specified. The total number and the locations of Acyclica devices collecting data in Seattle is unclear. This gives rise to the concern that there are unspecified locations in which Acyclica devices are collecting MAC addresses.

- *No Mention of RoadTrend Sensor Discontinuation.* As noted in the background,[12] Acyclica has been acquired by FLIR, an infrared and thermal imaging company. As of March 2019, FLIR's product webpage states that the Acyclica RoadTrend sensors (those currently used by SDOT) have been discontinued.[13] From the information we have, it is unclear if SDOT will be able to continue using the RoadTrend sensors described in the 2019 SIR. Given that FLIR sensors, such as the TrafiOne, have capabilities that go much farther than those of the

[11] Included in Appendix 1.
[12] As noted in 1. Acyclica – SDOT *Background* above.
[13] https://www.flir.com/support/products/roadtrend#Specifications

RoadTrend sensors (e.g., camera technology and thermal imaging)[14] as well as potentially different technical implementations, their use would give rise to even more serious privacy and misuse concerns. Neither the implications of the FLIR acquisition nor the discontinuation of the RoadTrend sensors are mentioned in the SIR.

- *No Mention of Protecting MAC Addresses of Non-Drivers/Riders (e.g., people in nearby buildings).* The Acyclica sensors will pick up the MAC addresses of all nearby individuals, regardless of whether they are or are not driving or riding in a vehicle. The SIR does not mention any steps taken to reduce the privacy infringements on non-drivers/riders.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- For what specific purpose or purposes will Acyclica be used, and what policies state this?
- Does SDOT have a contract with Acyclica, and if so, why is the contract not included in the SIR?
- Who owns the raw, non-aggregated data collected by Acyclica devices?
- What is the retention period for the different types of collected data (aggregated and non-aggregated)—for both SDOT and Acyclica?
- Provide accurate descriptions of Acyclica's data security practices, including encryption and hashing, consistent with the letter from Daniel Benhammou, including any additional practices that prevent reidentification.
- What third parties will access Acyclica's data, for what purpose, and under what conditions?
- Why are 89 locations not specified in the embedded Acyclica locations sheet in Section 2.1 of the SIR?
- Will SDOT continue to use Acyclica RoadTrend Sensors, and for how long? If SDOT plans to switch to other sensors, which ones, and how do their capabilities differ from the RoadTrend Sensors?
- Did SDOT consider any other alternatives when deciding to acquire Acyclica? Did SDOT consider other, more privacy protective traffic management tools in use (for example, inductive-loop detectors currently used by the Washington State Department of Transportation and the US

[14] https://www.flir.com/support/products/trafione#Resources

Department of Transportation)?[15]

- How does SDOT plan to reduce the privacy infringements on non-drivers/riders?

c. Recommendations for Regulation:

At this stage, pending answers to the questions set forth above, we can make only preliminary recommendations for regulation of Acyclica. We recommend that the Council adopt, via ordinance, clear and enforceable rules that ensure, at a minimum, the following:

- There must be a binding contract between SDOT and Acyclica.
- The contract between SDOT and Acyclica must include the following minimum provisions:
  - A data retention period of 12 hours or less for any data Acyclica collects, within which time Acyclica must aggregate the data, submit it to SDOT, and delete both non-aggregated and aggregated data.
  - SDOT receives only aggregated data.
  - SDOT owns all data, not Acyclica.
  - Acyclica cannot share the data collected with any other entity besides SDOT for any purpose.
- The ordinance must define a specific purpose of use for Acyclica technology, and all use of the tool and its data must be restricted to that purpose. For example: Acyclica may only be used for traffic management purposes, defined as activities concerning calculating average travel times, regulating traffic signals, controlling traffic disruptions, determining the placement of barricades or signals for the duration of road incidents impeding normal traffic flow, providing information to travelers about traffic flow and expected delays, and allowing SDOT to meet traffic records and reporting requirements.
- SDOT must produce an annual report detailing its use of Acyclica, including details how SDOT used the data collected, the amount of data collected, and for how long it was retained and in what form.

II. CopLogic – SPD

[15] https://www.fhwa.dot.gov/publications/research/operations/its/06108/03.cfm

Background

CopLogic (LexisNexis's Desk Officer Reporting System-DORS)[16] is a technology owned by LexisNexis and used by the Seattle Police Department to allow members of the public and retailers to submit online police reports regarding non-emergency crimes. Members of the public and retailers can submit these reports through an online portal they can access via their phone, tablet, or computer. Community members can report non-emergency crimes that have occurred within the Seattle city limits, and retail businesses that participate in SPD's Retail Theft Program may report low-level thefts that occur in their businesses when they have identified a suspect. This technology is used by SPD for the stated purpose of freeing up resources in the 9-1-1 Center, reducing the need for a police officer to be dispatched for the sole purpose of taking a police report.

This technology gives rise to potential civil liberties concerns because it allows for the collection of information about community members, unrelated to a specific incident, and without any systematic method to verify accuracy or correct inaccurate information. In addition, there is lack of clarity surrounding data retention and data sharing by LexisNexis, and around how CopLogic data will be integrated into SPD's Records Management System.

a. Concerns

- *Lack of Clarity on CopLogic/LexisNexis Data Collection and Retention.* There is no information in the SIR or in the contract between SPD and LexisNexis detailing the data retention period by LexisNexis (Section 5.2 of the SIR). This lack of clarity stems in part from an unclear description of what's provided by LexisNexis—it's described as an online portal, but the SIR and the contract provided appears to contemplate in Section 4.8 that LexisNexis will indeed access and store collected data. If true, the nature of that access should be clarified, and data restrictions including clear access limitations and retention periods should accordingly be put in place. Once reports are transferred over to SPD's Records Management System (RMS), the reports should be deleted by CopLogic/LexisNexis.

- *Lack of Clarity on LexisNexis Data Sharing with Other Agencies or Third Parties.* If LexisNexis does access and store data, it should do so only for purposes of fulfilling the contract, and should not share that data with third parties. But the contract between SPD and LexisNexis does not make clear whether LexisNexis is prohibited entirely from sharing data with other entities (it does contain a restriction on "transmit[ting]" the data, but without reference to third parties.

[16] https://risk.lexisnexis.com/products/desk-officer-reporting-system

- *No Way to Correct Inaccurate Information Collected About Community Members.* Community members or retailers may enter personally-identifying information about third parties without providing notice to those individuals, and there is no immediate, systematic method to verify the accuracy of information that individuals provide about third parties. There are also no stated measures in the SIR to destroy improperly collected data.

- *Lack of clarity on how the CopLogic data will be integrated with and analyzed within SPD's RMS.* At the technology fair, SPD stated that completed complaints will go into Mark43[17] when it is implemented. ACLU-WA has previously raised concerns about the Mark43 system, and it should be made clear how CopLogic data will enter that system, including to what third parties it will be made available.[18]

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What data does LexisNexis collect and store via CopLogic? What are LexisNexis's data retention policies for CopLogic data?

- Are there specific policies restricting LexisNexis from sharing CopLogic data with third parties? If so, what are they?

- Is there any way to verify or correct inaccurate information collected about community members?

- How will CopLogic data be integrated with Mark43?

c. Recommendations for Regulation:

Pending answers to the questions set forth above, we can make only preliminary recommendations for regulation of CopLogic. SPD should adopt clear and enforceable policies that ensure, at a minimum, the following:

- After CopLogic data is transferred to SPD's RMS, LexisNexis must delete all CopLogic data.

- LexisNexis is prohibited from using CopLogic data for any purpose other than those set forth in the contract, and from sharing CopLogic data with third parties.

[17] https://www.aclu-wa.org/docs/aclu-letter-king-county-council-regarding-mark-43
[18] A Records Management System (RMS) is the management of records for an organization throughout the records-life cycle. New RMSs (e.g., Mark43) may have capabilities that allow for law enforcement agencies to track and analyze the behavior of specific groups of people, leading to concerns of bias in big data policing, particularly for communities of color.

- Methods are available to the public to correct inaccurate information entered in the CopLogic portal.
- Measures are implemented to delete improperly collected data.

III. Computer-Aided Dispatch & 911 Logging Recorder Group

Overall, concerns around the Computer-Aided Dispatch (CAD) and 911 Logging Recorder technologies focus on use of the technologies and/or collected data them for purposes other than those intended, over-retention of data, and sharing of that data with third parties (such as federal law enforcement agencies). Therefore, for all of these technologies as appropriate, we recommend that the responsible agency should adopt clear and enforceable rules that ensure, at a minimum, the following:

- The purpose of use must be clearly defined, and its operation and data collected must be explicitly restricted to that purpose only.
- Data retention must be limited to the time needed to effectuate the purpose defined.
- Data sharing with third parties, if any, must be limited to those held to the same restrictions.
- Clear policies must govern operation, and all operators should be trained in those policies.

Specific comments follow:

1. Computer-Aided Dispatch – SPD

Background

CAD is a software package (made by Versaterm) utilized by the Seattle Police Department's 9-1-1 Center that consists of a set of servers and software deployed on dedicated terminals in the 9-1-1 center, in SPD computers, and as an application on patrol vehicles' mobile data computers and on some officers' smart phones. The stated purpose of CAD is to assist 9-1-1 Center call takers and dispatchers with receiving requests for police services, collecting information from callers, and providing dispatchers with real-time patrol unit availability. Concerns include lack of clarity surrounding data retention and data sharing with third parties.

a. Concerns:

- *Lack of clarity on data retention within CAD v. RMS.* While the SIR makes clear that at some point, CAD data is transferred to SPD's RMS, it is unclear what data, if any, the CAD system itself retains and for how long. If the CAD system does retain some data (for example, call logs)

independent of the RMS, and that data is accessible to the vendor, appropriate data protections should be put in place. But because the SIR usually references "data collected by CAD," it is unclear where that data resides.

- *Lack of a policy defining purpose of the technology and limiting its use to that purpose*: Unlike SFD's similar system, SPD appears to have no specific policy defining the purpose of use for CAD and limiting its use to that purpose.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- Does the CAD system itself store data? If so, what data and for how long? Who can access that data?

c. Recommendations for Regulation:

Depending on the answer to the question above, appropriate data protections may be needed as described above. In addition, SPD should adopt a policy similar to SFD's, clearly defining purpose and limiting use of the tool to that purpose.

2. Computer-Aided Dispatch – SFD

Background

Computer Aided Dispatch (CAD) is a suite of software packages used by SFD and made by Tritech that provide unit recommendations for 911 emergency calls based on the reported problem and location of a caller. The stated purpose of CAD is to allow SFD to manage emergency and non-emergency call taking and dispatching operations. The technology allows SFD to quickly enable personnel to execute rapid aid deployment.

Generally and positively, SFD clearly defines the purpose of use, restricts CAD operation and data collection to that purpose only, limits sharing with third parties, and specifies policies on operation and training. However, SFD must clarify what data is retained within CAD, data retention policies, and provide information about its data sharing partners.

d. Concerns

- *Lack of clarity on data retention within CAD*. It is unclear what data, if any, the CAD system itself retains and for how long. If the CAD system does retain some data (for example, call logs) and that data is accessible to the vendor, appropriate data protections should be put in place.
- *Lack of clarity on data retention policies*. At the technology fair, we learned that CAD data is retained indefinitely. It is not clear what justifies indefinite retention of this data.

- *Lack of clarity on data sharing partners.* In Section 6.3 of the SIR, SFD states that in rare case where CAD data is shared with partners other than those specifically named in the SIR, a third-party nondisclosure agreement is signed. However, there are no examples or details of who those partners are and the purposes for which CAD data would be shared.

e. Outstanding Questions That Must be Addressed in the Final SIR:

- Does the CAD system itself store data? If so, what data and for how long? Who can access that data?
- Who are SFD's data sharing partners? For what purpose is data shared with them?

f. Recommendations for Regulation:

Depending on the answer to the question regarding if the CAD system itself stores data, appropriate data protections may be needed as described above. SFD should adopt a clear policy requiring deletion of CAD data no longer needed. In addition, depending on how data is shared, SFD should adopt a policy that clearly limits what for what purposes CAD data would be shared, and with what entities.

3. 911 Logging Recorder – SPD

Background

The NICE 911 logging recorder is a technology used by SPD to audio-record all telephone calls to SPD's 9-1-1 communications center and all radio traffic between dispatchers and patrol officers. The stated purpose of the 9-1-1 Logging Recorder is to allow SPD to provide evidence to officers and detectives who investigate crimes and the prosecutors who prosecute offenders. These recordings also provide transparency and accountability for SPD, as they record in real time the interactions between 9-1-1 call takers and callers, and the radio traffic between 9-1-1 dispatchers and police officers. The NICE system also supports the 9-1-1 center's mission of quickly determining the nature of the call and getting the caller the assistance they need as quickly as possible with high quality, consistent and professional services.

Concerns include lack of clarity surrounding data retention schedules and data sharing with third parties.

a. Concerns

- *Lack of clarity on data retention.* Section 4.2 of the SIR states: "Recordings

requested for law enforcement and public disclosure are downloaded and maintained for the retention period related to the incident type." Similar to other technologies noted above, it is unclear whether the 9-1-1 system itself stores these recordings, or if they are stored on SPD's RMS. If the former, it should be made clear how the technology vendor accesses these recordings and for what purpose, if at all.

- *More clarity needed on data sharing with third parties.* There are no details or examples of the "discrete pieces of data" that are shared outside entities and individuals as referenced in Section 6.0 of the SIR.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What is SPD's data retention schedule for data stored in the NICE system, if any?
- What "discrete pieces of data" does SPD share with third parties?

c. Recommendations for Regulation:

SPD should adopt a clear policy requiring deletion of data no longer needed. In addition, depending on how data is shared, SPD should adopt a policy that clearly limits what for what purposes data would be shared, and with what entities.

IV. Current Diversion Technology Group – Seattle City Light

The technologies in this group—the Check Meter device (SensorLink TMS), the SensorLink Amp Fork, and the Binoculars/Spotting Scope raise civil liberties concerns primarily due to lack of explicit, written policies imposing meaningful restrictions on use of the technologies. While the purpose of the current diversion technologies appears clear—to assess whether suspected diversions of current have occurred and/or are continuing to occur—there are no explicit policies in the SIR detailing restrictions on what can and cannot be recorded by these technologies.

Below are short descriptions of the technologies, followed by concerns and recommendations.

Background

1. Check Meter Device (SensorLink TMS)

The SensorLink TMS device measures the amount of City Light-provided electrical energy flowing through the service-drop wire over time, digitally capturing the instantaneous information on the device for later retrieval by the Current Diversion Team via the use of a secure wireless protocol.

The stated purpose of use is to allow Seattle City Light to maintain the integrity of its electricity distribution system, to determine whether suspected current diversions have taken place, and to provide the valuation of the diverted energy to proper authorities for cost recovery.

2. SensorLink Amp Fork

The SensorLink Amp Fork is an electrical device mounted on an extensible pole allowing a circular clamp to be placed around the service-drop wire that provides electrical service to a customer location via its City Light-provided meter. The device then displays instantaneous readings of the amount of electrical energy (measured in amperage, or "amps") that the Current Diversion Team may compare against the readings displayed on the meter, allowing them to determine if current is presently being diverted.

The stated purpose of use of the Amp Fork is to allow Seattle City Light to assess whether suspected diversions of current have occurred and/or are continuing to occur. The Amp Fork allows the Utility to determine the valuation of the energy illegally diverted, which supports City Light's mission of recovering this value for ratepayers via a process called "back-billing."

3. Binoculars/Spotting Scope

The binoculars are standard, commercial-grade, unpowered binoculars. They do not contain any special enhancements requiring power (e.g., night-vision or video-recording capabilities). They are used to read a meter from a distance when the Current Diversion Team is otherwise unable to access physically the meter for the purpose of inspection upon suspected current diversion.

The stated purpose of the binoculars is to allow Seattle City Light to inspect meters and other implicated electrical infrastructure at a distance. If a determination of diversion is sustained, data may be used to respond to lawful requests from the proper law enforcement authorities for evidence for recovering the value of the diverted energy.

a. Concerns Regarding all Three Current Diversion Technologies

- *Absence of explicit, written policies imposing meaningful restrictions on use.* At the technology fair, a Seattle City Light representative stated that these technologies are used only for the purpose of checking current diversions, but could not confirm that Seattle City Light had clear, written policies for what data could and could not be recorded (e.g., an employee using the binoculars to view non-meter related information). The absence of written, specific policies increases the risk of unwarranted surveillance of individuals. There is also no mention in the SIRs of

specific data protection policies in place to safeguard the data (e.g., encryption, hashing, etc.).

- *Seattle City Light's records retention schedule is mentioned in the SIRs, but details about it are omitted.* It is unclear how long Seattle City Light retains data collected, and for what reason.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What enforceable policies, if any, apply to use of these three technologies?
- What is Seattle City Light's data retention schedule?

c. Recommendations for Regulation:

Seattle City Light must create clear, enforceable policies that, at a minimum:

- Define purpose of use for each technology and restrict its use to that purpose.
- Clearly state what clear data protection policies exist to safeguard stored data, if any, and ensure the deletion of data collected by the technology immediately after the relevant current diversion investigation has closed.

Thank you for your consideration, and please don't hesitate to contact me with questions.

Best,

Shankar Narayan
Technology and Liberty Project Director

Jennifer Lee
Technology and Liberty Project Advocate

Appendix 1: Benhammou Letter

16

City of Seattle

Acyclica

February 6th, 2015

RE: Acyclica data privacy standards

To whom it may concern:

The purpose of this letter is to provide information regarding the data privacy standards maintained by Acyclica. Acyclica is a traffic information company specializing in traffic congestion information management and analysis. Among the various types of data sources which make of Acyclica's traffic data portfolio including GPS probe data, video detection and inductive loops, Acyclica also utilizes our own patent-pending technology for the collection of Bluetooth and Wifi MAC addresses. MAC or Media Access Control addresses are unique 48-bit numbers which are associated with devices with Bluetooth and/or Wifi capable devices.

While MAC addresses themselves are inherently anonymous, Acyclica goes to great lengths to further obfuscate the original source of data through a combination of hashing and encryption to all but guarantee that information derived from the initial data bears no trace of any individual.

Acyclica's technology for collecting MAC addresses for congestion measurement operates by detecting nearby MAC addresses. The MAC addresses are then encrypted using GPG encryption before being transmitted to the cloud for processing. Encrypting the data prior to transmission means that no MAC addresses are ever written where they can be retrieved from the hardware. Once the data is received by our servers, the data is further anonymized using a SHA-256 algorithm which makes the raw MAC address nearly impossible to decipher from the hashed output. Furthermore, any customer seeking to download data for further investigation or integration through our API can only ever view the hashed MAC address.

Acyclica occasionally provides data to partners to help enhance the quality of congestion information. The information which is provided to such partners is received through API calls which only return aggregated information about traffic data over a given period such as the average travel-time over a 5-minute period. Aggregating the data provides a final layer of anonymization by reporting on the collective trend of all vehicles rather than the specific behavior of a single vehicle.

As always questions, comments and concerns are welcome. Please do let me know if we can provide further clarity and transparency on our internal operations with regards to data processing and privacy standards. We take the privacy of the public very seriously and always treat our customers and the data with the utmost respect.

Regards,

Daniel Benhammou
President
Acyclica Inc.

Appendix H: Comment Analysis Methodology

Overview

The approach to comment analysis includes combination of qualitative and quantitative methods. A basic qualitative text analysis of the comments received, and a subsequent comparative analysis of results, were validated against quantitative results. Each comment was analyzed in the following ways, to observe trends and confirm conclusions:

1. Analyzed collectively, as a whole, with all other comments received
2. Analyzed by technology
3. Analyzed by technology and question

A summary of findings are included in Appendix B: Public Comment Demographics and Analysis. All comments received are included in Appendix E: All Individual Comments Received.

Background on Methodological Framework

A modified Framework Methodology was used for qualitative analysis of the comments received, which "*…approaches [that] identify commonalities and differences in qualitative data, before focusing on relationships between different parts of the data, thereby seeking to draw descriptive and/or explanatory conclusions clustered around themes" (Gale, N.K., et.al, 2013).* Framework Methodology is a coding process which includes both inductive and deductive approaches to qualitative analysis.

The goal is to classify the subject data so that it can be meaningfully compared with other elements of the data and help inform decision-making. Framework Methodology is "not designed to be representative of a wider population, but purposive to capture diversity around a phenomenon" (*Gale, N.K., et.al, 2013).*

Methodology

Step One: Prepare Data

1. Compile data received.
    a. Daily collection and maintenance of 2 primary datasets.
        i. Master dataset: a record of all raw comments received, questions generated at public meetings, and demographic information collected from all methods of submission.
        ii. Comment analysis dataset: the dataset used for comment analysis that contains coded data and the qualitative codebook. The codebook contains the qualitative codes used for analysis and their definitions.
2. Clean the compiled data.
    a. Ensure data is as consistent and complete as possible. Remove special characters for machine readability and analysis.
    b. Comments submitted through SurveyMonkey for "General Surveillance"

remained in the "General Surveillance" category for the analysis, regardless of content of the comment. Comments on surveillance generally, generated at public meetings, were categorized as such.

c. Filter data by technology for inclusion in individual SIRs.

Step Two: Conduct Qualitative Analysis Using Framework Methodology

1. Become familiar with the structure and content of the data. This occurred daily compilation and cleaning of the data in step one.
2. Individually and collaboratively code the comments received, and identify emergent themes.
   I. Begin with deductive coding by developing pre-defined codes derived from the prescribed survey and small group facilitator questions and responses.
   II. Use clean data, as outlined in Data Cleaning section above, to inductively code comments.
      A. Each coder individually reviews the comments and independently codes them.
      B. Coders compare and discuss codes, subcodes, and broad themes that emerge.
      C. Qualitative codes are added as a new field (or series of fields) into the Comments dataset to derive greater insight into themes, and provide increased opportunity for visualizing findings.
   III. Develop the analytical framework.
      A. Coders discuss codes, sub-codes, and broad themes that emerge, until codes are agreed upon by all parties.
      B. Codes are grouped into larger categories or themes.
      C. The codes are be documented and defined in the codebook.
   IV. Apply the framework to code the remainder of the comments received.
   V. Interpret the data by identifying differences and map relationships between codes and themes, using R and Tableau.

Step Three: Conduct Quantitative Analysis

1. Identify frequency of qualitative codes for each technology overall, by questions, or by themes:
   I. Analyze results for single word codes.
   II. Analyze results for word pair codes (for context).
2. Identify the most commonly used words and word pairs (most common and least common) for all comments received.
   I. Compare results with qualitative code frequencies and use to validate codes.
   II. Create network graph to identify relationships and frequencies between

words used in comments submitted. Use this graph to validate analysis and themes.

3. Extract CSVs of single word codes, word pair codes, and word pairs in text of the comments, as well as the corresponding frequencies for generating visualizations in Tableau.

Step Four: Summarization

1. Visualize themes and codes in Tableau. Use call out quotes to provide context and tone.
2. Included summary information and analysis in the appendices of each SIR.

Appendix I: Supporting Policy Documentation

Appendix J: CTO Notification of Surveillance Technology

Thank you for your department's efforts to comply with the new Surveillance Ordinance, including a review of your existing technologies to determine which may be subject to the Ordinance. I recognize this was a significant investment of time by your staff; their efforts are helping to build Council and public trust in how the City collects and uses data.

As required by the Ordinance (SMC 14.18.020.D), this is formal notice that the technologies listed below will require review and approval by City Council to remain in use. This list was determined through a process outlined in the Ordinance and was submitted at the end of last year for review to the Mayor's Office and City Council.

The first technology on the list below must be submitted for review by March 31, 2018, with one additional technology submitted for review at the end of each month after that. The City's Privacy Team has been tasked with assisting you and your staff with the completion of this process and has already begun working with your designated department team members to provide direction about the Surveillance Impact Report completion process.

Please let me know if you have any questions.

Thank you,
Michael Mattmiller

Technology	Description	Proposed Review Order
Binoculars/Spotting Scope	The spotting scope is used to read meters from a distance when direct access to the meter is obstructed. Scopes are used by SCL's Current Diversion team to conduct investigations. Use of this technology may occur without informing a domicile's resident(s).	1
SensorLink Amp Fork	The SensorLink Amp Fork is used by SCL's Current Diversion team to measure the load on line-side entrance conductors, allowing SCL to determine the total amount of power being consumed at a service location. This tool provides an instantaneous reading to the group conducting the investigation. Use of this technology may occur without informing a domicile's resident(s).	2
Check Meter Device	This device measures the total amount of power being consumed at a service location where current diversion is confirmed or suspected. The device is set at the transformer and is used when a prolonged reading is desired by the Current Diversion team. Use of this technology may occur without informing a domicile's resident(s).	3

City of Seattle

2020 Surveillance Impact Report Executive Overview

Current Diversion Technologies

Seattle City Light

DRAFT

Overview

The Operational Policy statements in this document represent the only allowable uses of the equipment and data collected by this technology.

This Executive Overview documents information about the collection, use, sharing, security and access controls for data that is gathered through Seattle City Light's Current Diversion Technologies (CDT), specifically the **SensorLink TMS (Check Meter Device), SensorLink Amp Fork, and Binoculars / Spotting Scope**. All information provided here is contained in the body of the full Surveillance Impact Review (SIR) documents but are provided in a condensed format for easier access and consideration.

Note: **All use of CDT as described in this document and the accompanying SIRs is governed by SCL Department Policy & Procedure DPP 500 P III-416 which contain details on policy and training related to deployment and use of the Current Diversion Technologies.**

1.0 Technology Description

Binoculars: The binoculars are standard, commercial-grade, unpowered binoculars. They do not contain any special enhancements requiring power (e.g., night-vision or video-recording capabilities). They are used to read a meter from a distance when the CDT is otherwise unable to access physically the meter for the purpose of inspection upon suspected current diversion. CDT crews may also, in the event they have a report of an aggravated case – where there is an electrical system alteration posing a present danger to the public or the electrical system's integrity – observe such alterations.

SensorLink Amp Fork: Ampstik is an electrical device mounted on an extensible pole (up to 40' to 50') which allows a circular clamp to be placed around the service-drop wire that provides electrical service to a customer location via its City Light-provided meter. The device then displays instantaneous readings of the amount of electrical energy (measured in amperage, or "amps") that the CDT may compare against the readings displayed on the meter, allowing them to determine if current is presently being diverted.

SensorLink TMS (Check Meter Device): The SensorLink TMS (Check Meter Device) measures the amount of City Light-provided electrical energy flowing through the service-drop wire over time, digitally capturing the instantaneous information on the device for later retrieval by the CDT via the use of a secure wireless protocol. The TMS device is housed in a black, weatherproofed box of approximately four-square inches, with a City Light inventory control number on the outside for identification by City Light line crews. These are typically deployed on the electric pole, adjacent to the transformer, from one week to one month, depending on the specific case need and crew availability.

2.0 Purpose

Operational Policy:

> **Per Department Policy & Procedure DPP 500 P III-416 section 1.1, in support of SMC 21.49.100: To establish procedures for preventing, detecting, reporting, investigating, and correcting illegal, unauthorized, or inadvertent diversions of electric current and recovering lost revenue and costs from such diversions.**

The Current Diversion Team (CDT) crew uses the described technologies to inspect meters and other implicated electrical infrastructure at a distance. If a determination of diversion is sustained, data may be used to respond to lawful requests from the proper law enforcement authorities for evidence for recovering the value of the diverted energy.

3.0 Data Collection and Use

Operational Policies:

> **Per Department Policy & Procedure DPP 500 P III-416: The Current Diversion Coordinator or a designated current diversion investigator investigates suspected current diversion as soon as it is practical to do so after receiving a report of suspected current diversion.**
>
> **Per Department Policy & Procedure DPP 500 P III-416: The Current Diversion Coordinator or a designated current diversion investigator determines how many kilowatt hours or kilowatts of demand have been diverted and who shall be billed for them.**
>
> **Per Department Policy & Procedure DPP 500 P III-416: The CDT work unit investigating the diversion forwards its Investigation/Correction Cost Form to the Current Diversion Coordinator, who determines the total amount to be billed for investigation and correction costs. SMC 21.49.130(E) designates allowable billing provisions.**

The CDT only investigates specific meters, with the approval of the Current Diversion Coordinator, and other implicated electrical equipment at locations previously identified and properly documented as sites of suspected current diversion.

4.0 Data Minimization & Retention

Operational Policy:

> **Data will be retained per City Light records retention schedules.**

The CDT only investigates specific meters and other implicated electrical equipment at locations previously identified and properly documented as sites of suspected current diversion.

DRAFT

5.0 Access & Security

Operational Policy:

> **Records of inspections facilitated by use of current diversion technologies are stored in a private folder on City Light's digital file locations, accessible only by CDT members and management.**

Access

CDT members, who are journey-level electrical workers trained in the proper use this equipment, may collect these data. These consist of meter reads and, in certain instances, other implicated electrical equipment that poses a present danger to the public or the electrical system integrity.

The limited number of this equipment and of CDT members makes the routine tracking of the straight-forward. Equipment is issued to CDT members, and stored in their official vehicles. These vehicles are operated, locked, and stored in accordance with Utility security procedures. Equipment serial numbers are recorded and the CDT member to whom they are assigned, as well as their deployment status, are logged.

Security

CDT members are trained in how to store information in private folders on City Light's digital storage locations, in addition to the general privacy and security training required by Seattle IT.

6.0 Data Sharing and Accuracy

Operational Policy:

> **Data is collected and maintained for Seattle City Light use and may only be shared with outside entities for the purposes of law enforcement or legal action by the relevant jurisdictional authority. This policy is formally laid out in Seattle City Light Department Policy & Procedure DPP 500 P III-416.**

Reports from observations facilitated by the use of current diversion technology may be shared with other parties in two instances, both of which are public entities. These are (1) when a determination is made that current diversion has taken place, in which case a valuation of the stolen energy is sent to the customer billing division of City Light for "back-billing" to the customer for cost recovery, and (2) when police investigators and/or prosecutors require evidence for further proceedings in complex or aggravated cases, as when large sums of energy have been diverted/stolen, or where there is a safety risk to the public.

When a report is sent to law enforcement, it does not include power consumption information. Law enforcement then relies upon the Public Disclosure Law to request power records, if they decide to do so, and City Light would provide that information pursuant to that request. This may be effectuated either by a subpoena or by a request from law enforcement based upon probable cause and pursuant to the Washington Public Disclosure Law (see RCW 42.56.335).

DRAFT

Per City of Seattle's Privacy Statement, outlining commitments to the public about how we collect and manage their data: *We do not sell personal information to third parties for marketing purposes or for their own commercial use.* The full Privacy Statement may be found **here.**

7.0 Equity Concerns

Operational Policy:

> **All customers shall receive uniform consideration and courtesy in all matters involving actual or suspected current diversion.**

Seattle City Light Department Policy & Procedure DPP 500 P III-416 provides that "all customers shall receive uniform consideration and courtesy in all matters involving actual or suspected current diversion." City Light aims to ensure that the enforcement mechanisms are equitable, in that they should be not only unbiased but also equitably enforced.

DRAFT

SUMMARY and FISCAL NOTE*

Department:	Dept. Contact/Phone:	CBO Contact/Phone:
SCL / ITD	Ivonne Golbourne / 206-684-3680 Jonathan Porat / 206-256-5520	Jennifer Breeze/206-256-5972

** Note that the Summary and Fiscal Note describes the version of the bill or resolution as introduced; final legislation including amendments may not be fully described.*

1. BILL SUMMARY

Legislation Title: AN ORDINANCE relating to surveillance technology implementation; authorizing approval of uses and accepting the 2019 surveillance impact reports for the Seattle City Light's use of Current Diversion Technologies.

Summary and background of the Legislation: Per SMC Chapter 14.18 (also known as the Surveillance Ordinance), authorizing the approval of the surveillance impact reports for Seattle City Light's use of existing Current Diversion Technologies (Binoculars / Spotting Scope, Check Meter Device, SensorLink AmpFork).

2. CAPITAL IMPROVEMENT PROGRAM

Does this legislation create, fund, or amend a CIP Project? ___ Yes _X_ No

3. SUMMARY OF FINANCIAL IMPLICATIONS

Does this legislation amend the Adopted Budget? ___ Yes _X_ No

Does the legislation have other financial impacts to the City of Seattle that are not reflected in the above, including direct or indirect, short-term or long-term costs?
This technology is currently in use by Seattle City Light and no additional costs, either direct or indirect, will be incurred based on the continued use of the technology. However, should it be determined that SCL should cease use of the technology, there would be costs associated with decommissioning the technologies. Additionally, there may be potential financial penalty related to breach of contract with the technology vendors.

Is there financial cost or other impacts of *not* implementing the legislation?
Per the Surveillance Ordinance, the City department may continue use of the technology until legislation is implemented. As such, there are no financial costs or other impacts that would result from not implementing the legislation.

4. OTHER IMPLICATIONS

a. Does this legislation affect any departments besides the originating department?
This legislation does not affect other departments. The technology under review is used exclusively by Seattle City Light.

b. Is a public hearing required for this legislation?
A public hearing is not required for this legislation.

c. Is publication of notice with *The Daily Journal of Commerce* and/or *The Seattle Times* required for this legislation?
No publication of notice is required for this legislation.

d. Does this legislation affect a piece of property?
This legislation does not affect a piece of property.

e. Please describe any perceived implication for the principles of the Race and Social Justice Initiative. Does this legislation impact vulnerable or historically disadvantaged communities? What is the Language Access plan for any communications to the public?
The Surveillance Ordinance in general is designed to address civil liberties and disparate community impacts of surveillance technologies. Each Surveillance Impact Review included in the attachments, as required by the Surveillance Ordinance, include a Racial Equity Toolkit review adapted for this purpose.

f. Climate Change Implications

1. **Emissions: Is this legislation likely to increase or decrease carbon emissions in a material way?**
   No.

2. **Resiliency: Will the action(s) proposed by this legislation increase or decrease Seattle's resiliency (or ability to adapt) to climate change in a material way? If so, explain. If it is likely to decrease resiliency in a material way, describe what will or could be done to mitigate the effects.**
   No.

g. If this legislation includes a new initiative or a major programmatic expansion: What are the specific long-term and measurable goal(s) of the program? How will this legislation help achieve the program's desired goal(s).
There is no new initiative or programmatic expansion associated with this legislation. It approves the continuation of use for the specific technologies under review.

List attachments/exhibits below:

February 25, 2021

MEMORANDUM

To: Transportation and Utilities Committee
From: Lise Kaye, Analyst
Subject: Council Bill 120002: Seattle City Light Current Diversion Technologies

On Wednesday, March 3, 2021 the Transportation and Utilities Committee will discuss Council Bill (CB) 120002. The proposed bill is intended to meet the requirements of Seattle Municipal Code Chapter 14.18, Acquisition and Use of Surveillance Technologies.[1] (Attachment 1 to this memo summarizes these requirements and process by which the Executive develops the required Surveillance Impact Reports.) The proposed bill would approve Seattle City Light's (SCL's) continued use of three existing Current Diversion tools and accept the Surveillance Impact Reports (SIR) for each technology. As required by SMC 14.18.020(3), the Executive conducted a public engagement process to receive public comments and/or concerns about this technology. In addition, the Community Surveillance Working Group ("Working Group") has completed a Privacy and Civil Liberties Impact Assessment ("Impact Assessment") of the technology, and the City's Chief Technology Officer (CTO) has provided his response ("Response") to the Impact Assessment.

This memo describes each technology and summarizes both the potential civil liberties and potential disparate impacts and the public engagement processes for each, as reported in the SIRs. It also summarizes key concerns and recommendations from the Working Group's Impact Assessment and the CTO's Response. Finally, the memo identifies several policy considerations for possible Council action.

Seattle City Light Current Diversion Technologies

CB 120002 would approve SCL's use of and accept SIRs for three technologies employed when the utility's Current Diversion Team investigates electricity that is being used but is unaccounted for by SCL's billing system (i.e., is not being paid for). Data collected by the technologies may be used by law enforcement authorities as evidence for recovering the value of the diverted energy. The SIR reports that, in 2017, SCL recovered $1.6 million in stolen energy costs using these technologies. Council passage of CB 120002 would approve SCL's use of the following three Current Diversion tools and accept the Surveillance Impact Reports (SIR) for each technology.

- Binoculars/Spotting Scope. The Current Diversion Team uses standard, commercial grade binoculars to examine meters where current diversion is suspected. The binoculars do not have any special enhancements requiring power (e.g. night vision, video-recording capabilities) and do not collect data. Staff take notes on data collected by means of

[1] (Ord. 125679 , § 1, 2018; Ord. 125376 , § 2, 2017.)

binoculars which are stored in a secure folder on SCL's digital network drive. The data is only accessible by Current Diversion Team members and the Current Diversion Coordinator. SCL has clarified that, while the title of the SIR includes "Spotting Scope," SCL only uses the term as an "informal term" for binoculars.

- Check Meter Device. Officially called the "SensorLink Transformer Meter System," this device is housed in a small box temporarily attached to an electric pole. The Device measures electrical energy flowing through an electrical service wire over time. Members of the Current Diversion Team access the data remotely using a secure radio protocol and a specific, password-protected software program. The downloaded data are stored in a secure folder on SCL's digital network drive, accessible only by Current Diversion Team members and SCL management. Data stored in the Check Meter Device are deleted after its retrieval by the Current Diversion staff and/or upon its removal from the electrical pole. SCL retains the downloaded information in accordance with Washington State's Retention Schedule for Utility Service Providers, which calls for electricity diversion investigation records to be retained for six years after an investigation is closed and then destroyed.[2]
- SensorLink AmpFork, also referred to in the SIRs as the SensorLink Ampstik, is a handheld tool that provides an instantaneous reading of electrical energy flow through an electrical service wire. A member of the Current Diversion Team may then compare the information against the readings displayed on the electric meter, allowing staff to determine if current is presently being diverted. Only members of the Current Diversion Team and the Current Diversion Coordinator may access the data, which is stored on a private folder on SCL's digital file locations. The data may be shared with SCL's customer billing division or with police investigators or prosecutors who require evidence for further proceedings in complex or aggravated cases, as when large sums of energy have been diverted/stolen, or where there is a safety risk to the public.

Civil Liberties and Potential Disparate Impacts on Historically Marginalized Communities

Departments submitting SIRs are required to complete an adapted version of the Racial Equity Toolkit (RET) to inform the SIR public engagement process and to highlight and mitigate impacts on racial equity from the use of the technology. The RET for the Current Diversion Technologies states that SCL does not anticipate impacts on civil liberties from the technologies. However, the RET states that SCL is conducting an equity analysis of past enforcement locations to ensure that its policies and procedures are as equitable as possible. The equity analysis has not been completed as of the date of the drafting of this memo. The RET also reports that SCL had not yet finalized the metrics to be used as part of the CTO's annual equity assessments.[3]

[2] Per UT55-05G-07

[3] SMC 14.18.050B requires that the Chief Technology Officer produce and submit to the City Council a Surveillance Technology Community Equity Impact Assessment and Policy Guidance Report that addresses whether Chapter 14.18 of the SMC is effectively meeting the goals of the Race and Social Justice Initiative, any recommended adjustments to laws and policies to achieve a more equitable outcome, and any new approaches and considerations for the SIRs.

Public Engagement

The Executive accepted public comments on this technology from February 5 – March 5, 2019 and conducted one public meeting for multiple SIRs on February 27, 2019.[4] In addition, the Department of Neighborhoods conducted four focus group meetings in partnership with four organizations serving communities of color and other marginalized communities.[5] The SIR includes all notes from the focus groups (Appendix D); comments pertaining solely to these technologies received from members of the public (Appendix E), and letters from organizations or commissions (Appendix G). Nine of the 46 public comments (in Appendix E) relate to SCL's Current Diversion technologies; seven of those convey a range of opinions pertaining to binoculars including some support, questions about using outdated technology and concerns about invasion of privacy.

Privacy and Civil Liberties Impact Assessment

The Impact Assessment identifies three "Key Concerns" concerns about the use of data and data retention associated with SCL's Current Diversion technologies and recommends that Council adopt three specific policies. The Impact Assessment also requests that SCL's equity analysis of past enforcement locations be provided for public review. As noted above, SCL has not yet completed the equity analysis; Executive staff report that, when finalized, the analysis will be available for public viewing. Tables 1 and 2 (on the next page) summarize the CTO's Response to the "Key Concerns" and describe whether and how the SIRs as drafted would address the Working Group's recommended policies.

Key Concerns and the CTO's Response. Table 1 summarizes the CTO's response to each of the Working Group's "Key Concerns." The Response concludes that SCL's policy, training and limitations from the technologies themselves provide adequate mitigation for the potential privacy and civil liberty concerns raised by the Working Group.

[4] The February 27, 2019 City Surveillance Technology Fair solicited comments on SCL's Current Diversion Technologies, SFD's Computer-Aided Dispatch technology, Seattle Department of Transportation's Acyclica travel time measurement technology, and three Seattle Police Department Technologies: 911 Call Logging Recorder, Computer-Aided Dispatch, and CopLogic.

[5] Appendix D contains notes from these focus group meetings, which were conducted as part of a "World Café" pilot project in collaboration with the Council on American-Islamic Relations, Entre Hermanos, Byrd Barr Place, and Friends of Little Saigon. Notes from Entre Hermanos are in Spanish; Executive staff are reviewing options to translate these notes into English.

Table 1. CTO Response to Privacy and Civil Liberties Impact Assessment of SCL Current Diversion Technologies

Working Group Key Concern	CTO Response
1. No explicit, written restrictions on use	The policy and operational documentation provide detail about how the technology is used and how any data collected is managed, and it is our assessment that the documentation provides adequate protections.
2. No specific data protection provisions	The data storage location and access controls are adequate for protecting information collected by these technologies during current diversion investigations.
3. Unjustifiably long data retention period	SCL follows legally required retention periods that ensure that only data that is necessary to complete an investigation is preserved after the investigation in case of any dispute.

Recommended Policies. The Impact Assessment recommends that Council ensure that SCL adopt "clear and enforceable policies that ensure, at a minimum, the following:

1. Define purpose of use for each technology and restrict its use to that purpose.
2. Ensure there are clear data protection policies to safeguard stored data.
3. Ensure the deletion of data collected by the technology immediately after the relevant current diversion investigation has closed."

Table 2 below describes how the SIRs as drafted would address these three recommendations. Areas not fully addressed are included in the "Policy Considerations" section below.

Table 2. Working Group Recommendations Addressed in the SIR

Working Group Recommendation	Whether/How Addressed in SIR
1. Define the purpose of and use of each technology and restrict its use to that purpose.	**Executive Overview.** Operational Policies represent the only allowable uses of the equipment and data collected by this technology. Note: the Executive Overview is not adopted by CB 120003. *See "Policy Considerations" below.*
2. Ensure clear data protection policies to safeguard stored data.	**4.10.** Data for each device is stored in a private folder on City Light's digital file locations, accessible only by Current Diversion Team members and the Current Diversion Coordinator.
3. Ensure that data is deleted after the relevant current diversion investigation has closed.	**4.10.** SCL complies with Washington State's required retention period, which requires retention for six years after an investigation is closed.[6]

[6] See UT55-05G-07 Rev 0 of Washington State's Utility Services Records Retention Schedule

Policy Considerations

Central Staff has identified the following potential policy considerations relative to the Working Group's key concerns and recommendations:

1. Restrictions on use. SCL's policies do not concisely specify the allowable uses of the three Current Diversion technologies. . Council may wish to amend the proposed Council Bill to also adopt the Executive Overview of the SIRs which identify specific language as constituting the enforceable policies and procedures applicable to the Current Diversion technology.
2. Annual equity assessment metrics. SCL has not yet finalized metrics to be used in evaluating the Current Diversions technology as part of the CTO's annual equity assessments. These assessments are intended to play a key role in determining whether the City's surveillance legislation is meeting the goals of the Race and Social Justice Initiative. Council may wish to request a report on the proposed metrics by a date certain and/or defer approval of this SIR, pending completion of these metrics.
3. Correct title for Binoculars/Spotting Scope SIR. SCL has clarified that, while the title of the SIR includes "Spotting Scope," SCL only uses the term as an "informal term" for a binocular. However, in other contexts, a Spotting Scope is a significantly different piece of equipment than Binoculars.[7] Council may wish to amend the title of the SIR to refer only to "Binoculars."

Committee Action

Options for Council action are as follows:

1. Pass CB 120002 as transmitted;
2. Request Central Staff to prepare amendments to the Council Bill and/or to one or more of the SIRs to address additional concerns or issues; or
3. Take no action.

Attachment:

1. Background Summary and Surveillance Impact Report Process

cc: Dan Eder, Interim Director
Aly Pennucci, Budget and Policy Manager

[7] For example, this article published by the Audubon Society describes when a Spotting Scope can provide greater detail than Binoculars.

Attachment 1 - Background Summary and Surveillance Impact Report Process

Recent Legislative History

Ordinance 125376, passed by Council on July 31, 2017, required City of Seattle departments intending to acquire surveillance technology to obtain advance Council approval, by ordinance, of the acquisition and of a surveillance impact report (SIR).[1] Departments must also submit a SIR for surveillance technology in use when Ordinance 125376 was adopted (referred to in the ordinance as "retroactive technologies"). The Executive originally included 28 "retroactive technologies," on its November 30, 2017 Master List but revised that list to 26 in December 2019. The Council has approved two SIRs and twice extended the initial March 3, 2020 deadline for completion of SIRs for all 26 technologies: first by six months to accommodate extended deliberation of the first two SIRS; and then by a second six months due to COVID-related delays. Either the Chief Technology Officer or the Council may determine whether a specific technology is "surveillance technology" and thus subject to the requirements of SMC 14.18. Each SIR must describe protocols for a "use and data management policy" as follows:

- How and when the surveillance technology will be deployed or used and by whom, including specific rules of use
- How surveillance data will be securely stored
- How surveillance data will be retained and deleted
- How surveillance data will be accessed
- Whether a department intends to share access to the technology or data with any other entity
- How the department will ensure that personnel who operate the technology and/or access its data can ensure compliance with the use and data management policy
- Any community engagement events and plans
- How the potential impact of the surveillance on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities have been taken into account; and a mitigation plan
- The fiscal impact of the surveillance technology

Community Surveillance Working Group

On October 5, 2018, Council passed Ordinance 125679, amending SMC 14.18, creating a "community surveillance working group" charged with creating a Privacy and Civil Liberties Impact Assessment for each SIR.[2] At least five of the seven members of the Working Group

[1] As codified in SMC 14.18.030, Ordinance 125376 identified a number of exemptions and exceptions to the required Council approval, including information voluntarily provided, body-worn cameras and cameras installed in or on a police vehicle, cameras that record traffic violations, security cameras and technology that monitors City employees at work.

[2] Ordinance 125679 also established a March 31, 2020 deadline for submitting SIRs on technologies already in use (referred to as "retroactive technologies") when Ordinance 125376 was passed, with provision to request a six-month extension.

must represent groups that have historically been subject to disproportionate surveillance, including Seattle's diverse communities of color, immigrant communities, religious minorities, and groups concerned with privacy and protest.[3] Each Privacy and Civil Liberties Impact Assessment must describe the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities and will be included in the SIR. Prior to submittal of a SIR to Council, the Chief Technology Officer may provide a written statement that addresses privacy rights, civil liberty or other concerns in the Working Group's impact assessment.

Executive Overviews

In May 2019, members of the Governance, Equity, and Technology Committee requested that IT staff prepare a summary section for each of the two lengthy SIR documents under review at that time. The Committee then accepted the resultant "Condensed Surveillance Impact Reports (CSIRs) together with the complete SIRs. The Executive has continued this practice with subsequent SIRs but has renamed the documents "Executive Overviews." The Operational Policy Statements in the Executive Overview represent the only allowable uses of the subject technology.

SIR Process

Chart 1 is a visual of the SIR process from inception to Council Review:

Chart 1. Surveillance Impact Report (SIR) Process

Department drafts SIR about technology use, privacy, and data security.	Draft SIR made public. One or more public meetings scheduled to solicit feedback.	Working Group reviews SIR; creates Impact Assessment, documenting privacy and civil liberty concerns.	City's Chief Technology Officer addresses any Working Group concerns.	Council reviews Executive's proposed ordinance reflecting the SIR, authorizing the use of existing or new technology.

[3] The Mayor appoints four members and Council appoints three members.

Group 2 Surveillance Impact Report (SIR) Legislation

Transportation & Utilities Committee

March 3, 2021

Presentation by Seattle IT Privacy Office

City of Seattle

Surveillance Impact Report (SIR) Overview

- 2017: Ordinance 125376 took effect Sept 4th, revising the law to address the intended use of technologies with potential to impact civil liberties
- 2017: City identifies 29 technologies in use by 4 departments, later reduced to 26 technologies
- 2018: Ordinance amended to add an external Surveillance Advisory Working group
- 9/23/2019: Group 1 SIR legislation approved by Council (Ordinance 125936)
- 2020: Deadline extension from 9/1/2020 to 3/1/2021 due to COVID-19 delays
- **1/20/2021: Presented Overview of Surveillance Ordinance at the Transportation and Utilities Committee**
- **1/26/2021: Group 2 SIR legislation transmitted to Council**
- **2/22/2021: Group 3 SIR legislation transmitted to City Clerk**

Surveillance Criteria

Definition: *Technology whose primary purpose is to observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice. Identifiable individuals also include individuals whose identity can be revealed by license plate data when combined with any other record.*

Exclusions

- Consents to provide the data
- Opt-out notice
- Body-worn cameras
- Police vehicle cameras
- Cameras installed pursuant to state law…or to record traffic violations
- Security cameras
- City infrastructure protection cameras
- Technology that monitors only City employees

Inclusions

- Disparately impacts disadvantaged groups
- PII shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service
- Collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection
- Raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice

Surveillance Impact Report (SIR) Process

- Submitted for all retroactive and newly proposed technologies that meet the definition and have no exclusion criteria
- Created by the Departments with project management from IT

1. Privacy Impact Assessment
2. Financial Information
3. Racial Equity Toolkit
4. Public Engagement Comments and Analysis
5. Privacy and Civil Liberties Impact Assessment
6. CTO Response
7. Appendices & Supporting Documentation

General SIR Creation Timeline

1) Draft & Review SIRs	2) Public Comment Period	3) Public Comment Analysis	4) Working Group Review	5) CTO Response	6) Executive Overview	7) Council Review
Staff from the department requesting the technology completes SIR content	The initial draft released for public review and comment. One or more public meetings will take place to solicit feedback.	City staff compiles public comments and finalizes the SIR content.	The Surveillance Advisory Working Group reviews each SIR, complete an Assessment included in SIR submission	The CTO responds to the Privacy and Civil Liberties Assessment.	City Staff creates condensed version of the SIR for submission to Council (formerly called the Condensed SIR – CSIR)	City Council will decide on the use of the surveillance technology, by full Council vote.

8-9 months

Group 2 Surveillance Impact Reports (CB 120002, CB 120003, CB 120004)

1	**Binoculars / Spotting Scope (SCL)**	The spotting scope is used to read meters from a distance when direct access to the meter is obstructed.
2	**Check Meter Device (SCL)**	This device measures the total amount of power being consumed at a service location where current diversion is confirmed or suspected. The device is set at the transformer and is used when a prolonged reading is desired by the Current Diversion team.
3	**SensorLink Amp Fork (SCL)**	The SensorLink Amp Fork is used by SCL's Current Diversion team to measure the load online-side entrance conductors, allowing SCL to determine the total amount of power being consumed at a service location. This tool provides an instantaneous reading to the group conducting the investigation.
4	**Computer Aided Dispatch (SFD)**	Computer-aided dispatch (CAD) is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.
5	**Computer Aided Dispatch (SPD)**	CAD is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field.
6 / 7	**Automated License Plate Reader (ALPR) for Patrol and Parking Enforcement (SPD)**	ALPRs are computer-controlled, high-speed camera systems mounted on parking enforcement or police vehicles that automatically capture an image of license plates that come into view and converts the image of the license plate into alphanumeric data that can be used to locate vehicles reported stolen or otherwise sought for public safety purposes and to enforce parking restrictions.
8	**CopLogic (SPD)**	System allowing individuals to submit police reports on-line for certain low-level crimes in non-emergency situations where there are no known suspects or information about the crime that can be followed up on. Use is opt-in, but individuals may enter personally identifying information about third-parties without providing notice to those individuals.
9	**911 Logging Recorder (SPD)**	System providing networked access to the logged telephony and radio voice recordings of the 911 center.

Group 2 SIR Public Engagement

Short 1-2 minute video overview of each technology provided on SIR website.

Binoculars / Spotting Scope (City Light)

The spotting scope is used to read meters from a distance when direct access to the meter is obstructed. Scopes are used by SCL's Current Diversion team to conduct investigations. Use of this technology may occur without informing a domicile's resident(s).

View Summary Watch Review View Full Report

Check Meter Device (City Light)

This device measures the total amount of power being consumed at a service location where current diversion is confirmed or suspected. The device is set at the transformer and is used when a prolonged reading is desired by the Current Diversion team. Use of this technology may occur without informing a domicile's resident(s).

View Summary Watch Review View Full Report

SensorLink AmpFork (City Light)

The SensorLink Amp Fork is used by SCL's Current Diversion team to measure the load on line-side entrance conductors, allowing SCL to determine the total amount of power being consumed at a service location. This too provides an instantaneous reading to the group conducting the investigation. Use of this technology may occur without informing a domicile's resident(s).

View Summary Watch Review View Full Report

Computer Aided Dispatch (CAD) (Fire)

Computer-aided dispatch (CAD) is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.

View Summary Watch Review View Full Report

Computer Aided Dispatch (CAD) (Police)

CAD is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field.

View Summary Watch Review View Full Report

Automated License Plate Readers (Police)

ALPRs are computer-controlled, high-speed camera systems mounted on parking enforcement or police vehicles tha automatically capture an image of license plates that come into view and converts the image of the license plate into alphanumeric data that can be used to locate vehicles reported stolen or otherwise sought for public safety purpose and to enforce parking restrictions.

View Summary Watch Review View Full Report View Policy Appendix

CopLogic (Police)

System allowing individuals to submit police reports on-line for certain low-level crimes in non-emergency situatio where there are no known suspects or information about the crime that can be followed up on. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.

View Summary Watch Review View Full Report

911 Logging Recorder (Police)

System providing networked access to the logged telephony and radio voice recordings of the 911 cente

View Summary Watch Review View Full Report

Group 2 SIR Public Engagement

- February 5th – March 26th, 2019
- Technology Fair Style Event
- Recorded presentations and posted online
- Produced 2-minute video overviews of technologies

Engagement Method	(Approximate) Number of Individuals Participating	Number of Comments Received	Number of Questions Received
Focus Groups	18	12	13
Public Meeting	19	1	0
Online Comments	16	16	29
Letter	4	4	0
Email	2	2	0
Total	59	35	42

SEATTLE CITY COUNCIL
CENTRAL STAFF

Group 2 Surveillance Impact Reports

LISE KAYE, COUNCIL CENTRAL STAFF

TRANSPORTATION AND UTILITIES COMMITTEE| MARCH 3, 2021

Proposed Council Bills

I. Bills would approve the continuing use of specific surveillance technologies and accept Surveillance Impact Reports (SIRs) on those technologies

   a. CB 120002: Seattle City Light Current Diversion (3 SIRs)

   b. CB 120003: Seattle Fire Dept Computer-Aided Dispatch (1 SIR)

   c. CB 120004: Seattle Police Department (5 SIRs)

II. Committee Options

   a. Pass CB 120002, 120003 and/or 120004 as transmitted;

   b. Request Central Staff to prepare amendments to the Council Bill and/or to one or more of the SIRs to address additional concerns or issues; or

   c. Take no action

Proposed Council Bills – Today's Agenda

I. Introduction

II. Executive Overview

III. CB 120002: Seattle City Light Current Diversion (3 SIRs)

   a. Central Staff Summary
   b. Council Q&A

IV. CB 120003: Seattle Fire Dept Computer-Aided Dispatch (1 SIR)

   a. Central Staff Summary
   b. Council Q&A

V. CB 120004: Seattle Police Department (5 SIRs)

   a. Central Staff Summary
   b. Council Q&A

Elements to Consider

1. Purpose and Use of Each Technology
2. Civil Liberties and Potential Disparate Impacts on Historically Marginalized Communities (Racial Equity Toolkit)
3. Public Engagement
4. Privacy and Civil Liberties Impact Assessment
5. Chief Technology Officer's Response

Elements to Consider

- Policy Considerations
  - Primarily areas where Working Group's recommendations go beyond the mitigations described in the SIRs – not intended as staff recommendations
  - Incomplete information in a SIR
  - Legal and logistical parameters around addressing Working Group concerns (e.g. holding third-parties to City privacy standards; state mandated data retention schedules)

CB 120002: Seattle City Light Current Diversion technologies – 3 SIRs

Used to investigate potential electricity theft

- Binoculars/Spotting Scope
- Check Meter Device
- SensorLink AmpFork

SCL Current Diversion Technologies

- Civil Liberties and Potential Disparate Impacts
  - None anticipated
  - Equity analysis of past enforcement locations – not yet complete
  - Metrics for CTO's annual equity assessments – not identified
- Public comments: some support; concerns about outdated technology and invasion of privacy

SCL Current Diversion Technologies

- Impact Assessment issues:
  - Allowable uses
  - Data protection
  - Data retention
- CTO's Response: SCL's policy and training and limitations of the technologies provide adequate mitigation for Working Group concerns

SCL Current Diversion Technologies

- Policy Considerations
  - Restrictions on use
  - Annual equity assessment metrics
  - Title of Binoculars/Spotting Scope SIR

CB 120003: Seattle Fire Department Computer-Aided Dispatch – 1 SIR

Supports personnel who dispatch Fire and Emergency Medical Services units in emergency situations.

SFD Computer-Aided Dispatch

- Civil Liberties and Potential Disparate Impacts
  - Potential disclosure of personally identifiable information
  - Sensitive information could be used by law enforcement to target of members of historically marginalized communities or track locations and history of service requests
  - Metrics for CTO's annual equity assessments – not identified
- Public comments: some support; concerns about outdated technology and invasion of privacy

SFD Computer-Aided Dispatch

- Impact Assessment issues:
  - Allowable uses
  - Data accessibility, retention and sharing
  - Operators trained to policies
  - Continuity of contractual terms and privacy policies through merger
- CTO's Response: SFD's policy and training and limitations of the technologies provide adequate mitigation for Working Group concerns

SFD Computer-Aided Dispatch

- Policy Considerations
  - Restrictions on use
  - Data retention
  - Third-party data sharing
  - Annual equity assessment metrics

CB 120004: Seattle Police Department surveillance technologies – 5 SIRs

- Automated License Plate Readers
- Parking Enforcement System
- Computer-Aided Dispatch
- CopLogic
- 911 Logging Recorder

CB 120004: Automated License Plate Readers

Assist in identification of stolen vehicles, and vehicles wanted in conjunction with felonies or associated with wanted persons or Amber and Silver Alerts (abducted children and missing people).

* SIR updated in January 2019, with new policies effective February 1, 2019

SPD Automated License Plate Readers

- Civil Liberties and Potential Disparate Impacts
  - Could be used to identify individuals without reasonable suspicion of having committed a crime
  - Could be used to search for information that is not incidental to any active investigation
  - Could over-surveil vulnerable or historically targeted communities
- Public comments: support, concerns about data retention, security, privacy, potential for error or misuse, surveillance in general

SPD Automated License Plate Readers

- Impact Assessment issues:
  - Allowable use of data
  - Data access, collection, retention and sharing,
  - System audits,
  - Role/effectiveness of this technology in solving crimes
- CTO's Response: SPD's updated policies and training and limitations of the technologies provide adequate mitigation for Working Group concerns

SPD Automated License Plate Readers

- Policy Considerations
  - Restrictions on use

CB 120004: Parking Enforcement Systems

Enforce parking laws, such as vehicle impoundment for unpaid fines, time-restricted parking areas, and restricted parking zones. Identify stolen vehicles or those sought in connection with a criminal investigation using specialized license plate reader software.

* SIR updated in January 2019, with new policies effective February 1, 2019

SPD Parking Enforcement Systems

- Civil Liberties and Potential Disparate Impacts
  - Could be used to identify individuals without reasonable suspicion of having committed a crime
  - Could be used to search for information that is not incidental to any active investigation
  - Could over-surveil vulnerable or historically targeted communities
- Public comments: some support, concerns included data retention, equitable enforcement and surveillance in general

SPD Parking Enforcement Systems

- Impact Assessment issues:
  - Allowable use of data
  - Data access, collection, retention and third-party sharing,
  - Data sharing between Patrol and Parking Enforcement
  - System audits; financial and operational records, including use by neighborhood and demographic
  - Role/effectiveness of this technology in solving crimes
- CTO's Response: SPD's updated policies and training and limitations of the technologies provide adequate mitigation for Working Group concerns

SPD Parking Enforcement Systems

- Policy Considerations
  - Restrictions on use
  - Data Sharing between Patrol and Parking Enforcement
  - Equitable Enforcement
  - Genetec Patroller Software as “non-surveillance” technology

CB 120004: Computer-Aided Dispatch

Supports personnel who dispatch SPD Patrol units in emergency situations.

SPD Computer-Aided Dispatch

- Civil Liberties and Potential Disparate Impacts
  - Potential disclosure of personally identifiable information
  - Potential to contribute to structural racism through data sharing, storage and retention, thereby creating a disparate impact on historically targeted communities
  - Metrics for CTO's annual equity assessments – not identified
- Public comments: some support; concerns included data security

SPD Computer-Aided Dispatch

- Impact Assessment issues:
  - Allowable use of data
  - Data access
  - Data retention
  - Operators trained to policies
- CTO's Response: SIR provided information specific to each concern

SPD Computer-Aided Dispatch

- Policy Considerations
  - Restrictions on use
  - Annual equity assessment metrics

CB 120004: CopLogic

Crime-reporting software with two applications:

1) Individual reporting of low-level crimes
2) Retail theft reporting

SPD CopLogic

- Civil Liberties and Potential Disparate Impacts
  - Information could be disseminated in ways that could negatively impact peoples' civil liberties
  - Racial or ethnicity-based information may be entered into the system
  - Potential to contribute to structural racism through data sharing, storage and retention, thereby creating a disparate impact on historically targeted communities
  - Metrics for CTO's annual equity assessments – not identified

SPD CopLogic

- Public comments:
  - Some support
  - Request for technology to be available in languages other than English
  - Concerns about: uneven access to the programs, potential for racial bias in reports and for inaccurate reports, unfair treatment of suspects, data collection, retention and sharing

SPD CopLogic

- Impact Assessment issues:
  - Allowable use of data
  - Data retention
  - Civil liberty impacts of the retail theft program; recommend discontinuing the program
  - Third-party data sharing
- CTO's Response: SPD's policies and training and limitations of the technologies provide adequate mitigation for Working Group concerns

SPD CopLogic

- Policy Considerations
  - Retail theft reporting component of CopLogic
  - Lexis-Nexis contract provisions: purpose and use restrictions, data retention, data sharing
  - Annual equity assessment metrics

CB 120004: 911 Logging Recorder

Automatically records all telephone calls received by the Seattle Police Department's 9-1-1 Center as well as all radio traffic between dispatchers and SPD patrol officers.

SPD 911 Logging Recorder

- Civil Liberties and Potential Disparate Impacts
  - Potential disclosure of personally identifiable information
  - Potential to contribute to structural racism through data sharing, storage and retention, thereby creating a disparate impact on historically targeted communities
  - Metrics for CTO's annual equity assessments – not identified
- Public comments: some support; concerns included data use, retention and sharing

SPD 911 Logging Recorder

- Impact Assessment issues:
  - Allowable use of data
  - Data retention and sharing
  - Data retention
  - Vendor and third-party contract provisions
- CTO's Response: SIR provided information specific to each concern

SPD 911 Logging Recorder

- Policy Considerations
  - Restrictions on use (internal to City)
  - Third-party restrictions on use
  - Annual equity assessment metrics – not included

File #: CB 120003, **Version:** 1

CITY OF SEATTLE

ORDINANCE _____

COUNCIL BILL _____

AN ORDINANCE relating to surveillance technology implementation; authorizing approval of uses and accepting the surveillance impact report for the Seattle Fire Department's use of Computer Aided Dispatch.

WHEREAS, Ordinance 125376 requires Council approval of surveillance impact reports (SIRs) related to approval of uses for certain technology, with existing/retroactive technology to be placed on a Master Technology List; and

WHEREAS, the ordinance provisions apply to the Computer Aided Dispatch (CAD) system in use by Seattle Fire Department (SFD); and

WHEREAS, SFD conducted policy rule review and community review as part of the development of the SIRs; and

WHEREAS, Seattle Municipal Code Section 14.18.080, enacted by Ordinance 125679, also requires review of the SIRs by a Community Surveillance Working Group composed of relevant stakeholders and a statement from the Chief Technology Officer in response to the Working Group's recommendations; and

WHEREAS, development of the SIRs and review by the Working Group has been completed; NOW, THEREFORE,

BE IT ORDAINED BY THE CITY OF SEATTLE AS FOLLOWS:

Section 1. Pursuant to Ordinances 125376 and 125679, the City Council approves use of the Seattle Fire Department's Computer Aided Dispatch and accepts the Surveillance Impact Report (SIR), for this technology, attached to this ordinance as Attachment 1, and the Executive Overview, for the same technology, attached to

this ordinance as Attachment 2.

Section 2. This ordinance shall take effect and be in force 30 days after its approval by the Mayor, but if not approved and returned by the Mayor within ten days after presentation, it shall take effect as provided by Seattle Municipal Code Section 1.04.020.

Passed by the City Council the _____ day of _____, 2021, and signed by me in open session in authentication of its passage this _____ day of _____, 2021.

_____

President _____ of the City Council

Approved / returned unsigned / vetoed this _____ day of _____, 2021.

_____

Jenny A. Durkan, Mayor

Filed by me this _____ day of _____, 2021.

_____

Monica Martinez Simmons, City Clerk

(Seal)

Attachments:
Attachment 1 - Computer-Aided Dispatch (CAD) SIR

Attachment 2 - Computer-Aided Dispatch (CAD) Executive Overview

City of Seattle

2019 Surveillance Impact Report

Computer-Aided Dispatch (CAD)

Seattle Fire Department

City of Seattle

Table of Contents

Submitting Department Memo 3
Surveillance Impact Report ("SIR") overview 5
Privacy Impact Assessment 7
Financial Information 22
Expertise and References 23
Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet 25
Privacy and Civil Liberties Assessment 36
CTO Response 41
Appendix A: Glossary 46
Appendix B: Meeting Notice(s) 48
Appendix C: Meeting Sign-in Sheet(s) 57
Appendix D: Department of Neighborhood Focus Group Notes 83
Appendix E: All Comments Received from Members of the Public 116
Appendix F: Department Responses to Public Inquiries 121
Appendix G: Letters from Organizations or Commissions 122
Appendix H: Comment Analysis Methodology 147
Appendix I: Supporting Policy Documentation 150
Appendix J: CTO Notification of Surveillance Technology 353

City of Seattle

Submitting Department Memo

Memo

Date: 04/15/2019
To: City Council
From: Seattle Fire Department
Subject: Cover Memo – Computer Aided Dispatch

Description

Computer Aided Dispatch (CAD) is a suite of software packages that provide unit recommendations for 911 emergency calls based on the reported problem and location of a caller. The Seattle Fire Department uses CAD to manage dispatches for over 100,000 individual responses each year.

Purpose

The mission of the Seattle Fire Department is to save lives and protect property through emergency medical service, fire and rescue response and fire prevention. During an emergency, quick and effective decision-making by dispatchers and first responders can be the difference between life and death. CAD is a tool that allows dispatchers and first responders to work more efficiently and effectively assessing emergency situations and events to determine the appropriate response and resources.

Benefits to the Public

The City of Seattle has the highest cardiac arrest survival rate of any major city in the United States. A large part of that success is due to the CAD software allowing dispatchers to make quicker decisions and immediately assign accurate resources. The CAD system can be described as the "tip of the spear" when it comes to emergency responses. All subsequent actions taken by SFD personnel in responding to emergency calls and events are predicated on the information obtained by CAD after a call has been received.
TriTech's Respond CAD, Computer Aided Dispatch (CAD) solution was developed exclusively for EMS agencies to manage emergency and non-emergency call taking and dispatching operations. This solution captures all major data points throughout each call to provide comprehensive data collection to immediately enable personnel to execute rapid aid deployment in emergency situations.

A study by the Illinois Department of Transportation on the impact of CAD systems finds that:
"The introduction of CASD systems allows for dramatic increases in the quality and quantity of performance related data."

The Seattle Fire Department simply could not provide the same level of quality service to the public without CAD.

Privacy and Civil Liberties Considerations

CAD receives information from callers in order to properly respond to emergency situations, often including their name, phone number, address from which they are calling, medical conditions, and potentially other personally identifiable information. While most of this information is consciously volunteered by callers, some of the information may be stored for future reference in emergency situations or for quality assurance purposes. Additionally, information may be provided to CAD about a location with identifiable information without their knowledge as part of the premise notes. This information can be invaluable to first responders in order to have a complete picture of the environment and potential hazards they will encounter before arriving at the scene.

Policy Update

This SIR was drafted and finalized in 2018 prior to the merger of TriTech / CentralSquare, the vendors mentioned in this document. As such, the SIR may contain references to the vendor TriTech, which is now CentralSquare. Reviewing the contractual agreements post-merger, the privacy and contractual provisions remain unchanged. SFD's CAD data is not shared with the vendor or any of the other customers they have acquired.

City of Seattle

Surveillance Impact Report ("SIR") overview

About the Surveillance Ordinance

The Seattle City Council passed Ordinance 125376, also referred to as the "Surveillance Ordinance," on September 1, 2017. SMC 14.18.020.b.1 charges the City's executive with developing a process to identify surveillance technologies subject to the ordinance. Seattle IT, on behalf of the executive, developed and implemented a process through which a privacy and surveillance review is completed prior to the acquisition of new technologies. This requirement, and the criteria used in the review process, are documented in Seattle it policy pr-02, the "surveillance policy".

How this Document is Completed

This document is completed by the requesting department staff, support and coordinated by the Seattle information technology department ("Seattle it"). As Seattle it and department staff complete the document, they should keep the following in mind.

1. Responses to questions should be in the text or check boxes only; all other information (questions, descriptions, etc.) Should **not** be edited by the department staff completing this document.
2. All content in this report will be available externally to the public. With this in mind, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.

Surveillance Ordinance Review Process

The following is a high-level outline of the complete SIR review process.

Upcoming for Review	Initial Draft	Open Comment Period	Final Draft	Working Group	Council Review
The technology is upcoming for review, but the department has not begun drafting the surveillance impact report (SIR).	Work on the initial draft of the SIR is currently underway.	The initial draft of the SIR and supporting materials have been released for public review and comment. During this time, one or more public meetings will take place to solicit feedback.	During this stage the SIR, including collection of all public comments related to the specific technology, is being compiled and finalized.	The surveillance advisory working group will review each SIR's final draft and complete a civil liberties and privacy assessment, which will then be included with the SIR and submitted to Council.	City Council will decide on the use of the surveillance technology, by full Council vote.

Privacy Impact Assessment

Purpose

A Privacy Impact Assessment ("PIA") is a method for collecting and documenting detailed information collected in order to conduct an in-depth privacy review of a program or project. A PIA asks questions about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. It also requests information about policies, training and documentation that govern use of the technology. The PIA responses are used to determine privacy risks associated with a project and mitigations that may reduce some or all of those risks. In the interests of transparency about data collection and management, the City of Seattle has committed to publishing all PIAs on an outward facing website for public access.

When is a Privacy Impact Assessment Required?

A PIA may be required in two circumstances.

1. When a project, technology, or other review has been flagged as having a high privacy risk.
2. When a technology is required to complete the surveillance impact report process. This is one deliverable that comprises the report.

1.0 Abstract

1.1 Please provide a brief description (one paragraph) of the purpose and proposed use of the project/technology.

Computer Aided Dispatch (CAD) is a suite of software packages that provide unit recommendations for 911 emergency calls based on the reported problem and location of a caller. The Seattle Fire Department uses CAD to manage dispatches for thousands of responses each year.

1.2 Explain the reason the project/technology is being created or updated and why the PIA is required.

According to the Surveillance Ordinance, a technology has surveillance capability if it can be used "to collect, capture, transmit, or record data that could be used to surveil, regardless of whether the data is obscured, de-identified, or anonymized before or after collection and regardless of whether technology might be used to obscure or prevent the capturing of certain views or types of information."

CAD receives information from callers in order to properly respond to emergency situations, often including their name, phone number, address from which they are calling, medical conditions, and potentially other personally identifiable information. While most of this information is consciously volunteered by callers, some of the information may be stored for future reference in emergency situations or for quality assurance purposes. Additionally, information may be provided to CAD about someone or a situation with identifiable information without their knowledge.

2.0 Project / Technology Overview

Provide an overview of the project or technology. The overview gives the context and background necessary to understand the purpose, mission and justification for the project / technology proposed

2.1 Describe the benefits of the project/technology.

The City of Seattle has the highest cardiac arrest survival rate of any major city in the United States. A large part of that success is due to the CAD software allowing dispatchers to make quicker decisions and immediately assign accurate resources. The CAD system can be described as the "tip of the spear" when it comes to emergency responses. All subsequent actions taken by SFD personnel in responding to emergency calls and events are predicated on the information obtained by CAD after a call has been received.

For more details about Seattle Fire's performance please see the SFD Annual Report: http://www.seattle.gov/Documents/Departments/Fire/FINAL%20Annual%20Report_2017.pdf

2.2 Provide any data or research demonstrating anticipated benefits.

TriTech's Respond CAD, Computer Aided Dispatch (CAD) solution was developed exclusively for EMS agencies to manage emergency and non-emergency call taking and dispatching operations. This solution captures all major data points throughout each call to provide comprehensive data collection to immediately enable personnel to execute rapid aid deployment in emergency situations.

The Computer Aided Dispatch system offers an array of features and functions that aid in the rapid deployment of aid. A list of CAD system abilities from Tritech may be found here: https://www.tritech.com/downloads/Z_18_IMCCAD_DS.pdf

A study by the Illinois Department of Transportation on the impact of CAD systems finds that:

"The introduction of CASD systems allows for dramatic increases in the quality and quantity of performance related data." For a detailed examination of system benefits, this study is available here: https://utc.uic.edu/wp-content/uploads/Strategic-Project-Plan-Computer-Assisted-Scheduleing-and-Dispatch1.pdf

2.3 Describe the technology involved.

CAD is a distributed server environment utilizing multiple workstations to centrally manage 911 emergency calls. The software is made by Tritech Software Systems. According to Tritech:

"CAD dispatch software helps communications center personnel manage a large amount of information—unit locations, unit statuses, pending and active calls, and other critical data—while serving as a voice of reassurance to callers and providing vital information that links police officers, firefighters, and paramedics." (Source: https://www.tritech.com/solutions/inform/inform-cad)

The Seattle Fire Department has integrated CAD into many facets of our operations, from dispatching and resource delivery to staffing and reporting to federal authorities on departmental performance.

2.4 Describe how the project or use of technology relates to the department's mission.

The mission of the Seattle Fire Department is to save lives and protect property through emergency medical service, fire and rescue response and fire prevention. During an emergency, quick and effective decision-making by dispatchers and first responders can be the difference between life and death. CAD is a tool that allows dispatchers and first responders to work more efficiently and effectively assessing emergency situations and events to determine the appropriate response and resources.

2.5 Who will be involved with the deployment and use of the project / technology?

Uniformed Seattle Fire Department personnel assigned to emergency response are involved with the use of the CAD system. This includes but is not limited to call dispatch operators, departmental operations, and mobile apparatus operators. The following divisions within the organization use the CAD system:

- Fire Alarm Center (FAC)
- SFD Operations Staff (SFD HQ).

Additionally, Seattle IT provides an SFD Client Services Director to facilitate strategic IT project management and client services for SFD IT technologies and applications, including the CAD system. Details about the IT department roles and responsibilities may be found in Appendix I of this SIR.

3.0 Use Governance

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities contracting with the City are bound by restrictions specified in the surveillance ordinance and privacy principles and must provide written procedures for how the entity will comply with any restrictions identified.

3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

Seattle Fire Department employees have access to CAD view, which is restricted via Active Directory controls and firewall rules. There is also a software firewall built into the system server to limit access and provide an additional level of system security.

Only specially trained members of the Fire Alarm Center can input information into CAD. The training process required for these months of hands-on training on location.

3.2 List the legal standards or conditions, if any, that must be met before the project / technology is used.

There are local, state and federal regulatory requirements that apply to fire department operations and use of CAD systems to assist in meeting these stringent service level expectations. These include the following:

- RCW 35.22.280, which enumerates the powers afforded to first class cities, including Seattle: http://app.leg.wa.gov/rcw/default.aspx?cite=35.22.280.
- The authority of the Seattle Fire Department to provide emergency services can be found in Article X of the City of Seattle Charter: http://clerk.ci.seattle.wa.us/~public/charter/charter.htm
- National Fire Protection Standards (NFPA) mandate requirements response times and other service level standards for municipal fire departments. Details of these standards may be found here: https://www.nfpa.org/codes-and-standards
- RCW 35A.92.010 sets state level reporting standards for city fire departments, the requirements of which rely on CAD to meet: http://app.leg.wa.gov/RCW/default.aspx?cite=35.103.010

3.3 Describe the policies and training required of all personnel operating the project / technology, and who has access to ensure compliance with use and management policies.

SFD commanding officers, such as the acting Lieutenant and/or Captain, are responsible for ensuring compliance of uniformed personnel in their unit.

SFD's Policy and Operating Guidelines (POG), contain details on policy and training related to deployment and use of SFD's CAD system. Applicable details from the POG can be found in Appendix I of this SIR.

4.0 Data Collection and Use

4.1 Provide details about what information is being collected from sources other than an individual, including other IT systems, systems of record, commercial data aggregators, publicly available data and/or other City departments.

CAD information includes both manually collected and automated data. Details about both of these are as follows:

Manually collected information includes the call information that CAD operators input into the system in the course of an emergency call. In addition to this information, there is an Emergency Medical Dispatch CAD plug in application which includes a decision tree protocol that facilitates interactions with callers.

Automated information include data from phone companies that they are required to collect and use to route emergency communications. The automated information includes but is not limited to automatically collected phone numbers with address links. These are described below:

- ANI is Automatic Number Identification. The ANI is a 10-digit Telephone Number (TN) associated with a device originating a 9-1-1 call. The ANI may be the actual number of a device, such as at a home; it may be a number that represents a Billing Telephone Number (BTN). This representation is often the case when calling from a business MLTS / PBX; it also may be called an Emergency Location Identification Number (ELIN), often used to indicate a more granular location within a business, especially in large campus or building environments.
- ALI is Automatic Location Identification. The ALI information is the '911 call location data' that is displayed to the 9-1-1 call taker on their computer display when answering 9-1-1 calls.

4.2 What measures are in place to minimize inadvertent or improper collection of data?

Information intake occurs during the initial call, during evaluation and response triage. When trying to validate location information to determine response resources, the operator may attempt to clarify this information from the caller and/or use computerized look up or confirmation of location. Once on scene at an emergency, there may be a need to update the initial intake information based on the existing situation.

4.3 How and when will the project / technology be deployed or used? By whom? Who will determine when the project / technology is deployed and used?

Tritech has been use by the Seattle Fire Department since 2003 and was deployed at the Fire Alarm Center (FAC) and in the mobile fleet (apparatus).

Uniformed Seattle Fire Department personnel assigned to emergency response are involved with the use of the CAD system. This includes but is not limited to call dispatch operators, departmental operations, and mobile apparatus operators.

Additionally, Seattle IT provides an SFD Client Services Director to facilitate strategic IT project management and client services for SFD IT technologies and applications, including the CAD system. Details about the IT department roles and responsibilities may be found in Appendix I of this SIR.

4.4 How often will the technology be in operation?

The technology is in operation daily. It runs 24 hours a day, seven days a week, 365 days a year.

4.5 What is the permanence of the installation? Is it installed permanently, or temporarily?

The installation and use of CAD is permanent.

4.6 Is a physical object collecting data or images visible to the public? What are the markings to indicate that it is in use? What signage is used to determine department ownership and contact information?

The CAD software has no physical or visual indicator that it is in use. The software itself runs 24 hours a day, 7 days a week, 365 days a year.

4.7 How will data that is collected be accessed and by whom?

Access to CAD systems and data are as following:

- Caller information is collected by SFD dispatchers. The data is then accessible by all Fire Department personnel and is role-based depending on need to access the information and system.
- CAD data is also shared with American Medical Response (AMR) in real-time in order to coordinate resources needed for basic life support (BLS) EMS calls. AMR has their own access into the CAD system via Mobile Data Computer (MDC) in real time to aid in determining dynamic resource allocation and immediate response dispatch if warranted by the emergency.
- Some basic information including emergency response time, location, whether the incident is active or closed, and the date and time is also available online to the public via Realtime 911: http://www2.seattle.gov/fire/realtime911/ with a one-minute delay.
- Pulse Point, a phone app that coordinates CPR volunteers and the location of AEDs with emergency cardiac victims. The app receives CAD info on cardiac emergencies at the same rate as the SFD personnel do for specific cardiac event response and public assistance for CPR. This has saved lives over the use of the system.

Additionally, incidental data access may occur through delivery of technology client services. All ITD employees are required to comply with appropriate regulatory requirements regarding security and background review. Information on the ITD roles associated with client services for City Departments can be found in Appendix I.

4.8 If operated or used by another entity on behalf of the City, provide details about access, and applicable protocols.

The following are entities that use the CAD system:

- AMR accesses a limited view of CAD data for staging ambulances close to an incident. The data access and protocols for use are outlines in the memorandum of agreement (MOA) between the company of SFD, in Appendix I.
- King County gets a nightly extract of the data via an electronic health records (eHR) data export of CAD to a data secure FTP server.
- NFPA(FEMA/DHS) receives a quarterly update on performance measure, per regulatory requirement.

4.9 What are acceptable reasons for access to the equipment and/or data collected?

The following are acceptable reasons for access to the CAD system and data:

- Emergency Services and Dispatch
- Communication for first responders
- Public Records (some exemptions may apply)
- Discovery for litigation purposes
- Sharing of information with law enforcement in accordance with the Uniform Healthcare Information Act (UHCIA)
- Quality Assurance
- Client services for SFD IT technologies and applications, including the CAD system. Details about the IT department roles and responsibilities may be found in the appendix of this SIR.
- Quality Assurance

4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

The following safeguards are in place to protect CAD data:

- Physical security of servers at FAC and back-up location at Seattle Police West Precinct includes key-card access
- Active directory rules control system access. AD access controls are role-based and based on a dedicated domain separating it from the City standard domain.
- Additions and deletion to AD is conducted by the services captain who gets daily reports on personnel. The services captain adjusts key card access daily to meet 24-hour threshold access control for personnel changes such as termination or reassignment.
- With each call, an activity log is created which allows the Quality Assurance (QA) specialist to review the timeline of decisions and system interaction during an incident response.

ITD support functions may require limited system access as detailed above. Supporting documentation on ITDs responsibilities in maintaining and supporting the CAD system can be found in Appendix I of this document.

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

Seattle Fire Department CAD data is stored on a secure server located at the Fire Alarm Center. A back-up physical server in case of catastrophic failure is also maintained at the Seattle Police Department's West Precinct. SFD personnel arrive at the backup location when that is activated. Access controls and physical security are described in section 4.10.

5.2 How will the owner allow for departmental and other entities, to audit for compliance with legal deletion requirements?

All records are kept in accordance with state retention requirements.

5.3 What measures will be used to destroy improperly collected data?

Any improperly collected data is manually destroyed by SFD personnel, specifically members of the FAC.

Per the TriTech Software Support Agreement: "If Client determines a Software Error exists, Client shall immediately notify TriTech by telephone, followed by an error report in writing, setting forth the defects noted with specificity requested by TriTech."

5.4 which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

Data is retained for the life of the system. The following roles are responsible for ensuring compliance with data retention requirements:

- Assistant Chief of Risk Prevention
- Communications Deputy Chief

6.0 Data Sharing and Accuracy

6.1 Which entity or entities inside and external to the City will be data sharing partners?

Data sharing partners include:

- American Medical Response (AMR)
- The University of Washington, Harborview Medical Center (UWHMC)
- ESO Solutions, current vendor for electronic healthcare records (eHR)
- King County – King County Emergency Medical Services (KC EMS) contracts through KC for hosted her records access
- In case of suspected criminal activity resulting in or from an emergency response, applicable event data is provided to SPD for investigative purposes.

6.2 Why is data sharing necessary?

Data sharing is necessary for coordinated, rapid responses to 911 incidents, particularly reducing the amount of time needed to make contact with patients and thereby improve outcomes.

Specifically, sharing with the University of Washington is for quality assurance and research purposes, including cardiac arrest data. Aggregated CAD data is also shared with King County for quality assurance and comparison with other local Fire and EMS agencies. Sharing with AMR is necessary for coordinating EMS responses in real-time. The eHR software uses CAD data to fill out incident details in electronic healthcare records, which are subsequently provided to emergency room staff for continuity of patient care.

6.3 Are there any restrictions on non-City data use?

Yes ☒ No ☐

6.3.1 If you answered yes, provide a copy of the department's procedures and policies for ensuring compliance with these restrictions.

Subsets of CAD data is restricted for exclusive use by several partner agencies, including the University of Washington's Harborview Medical Center, American Medical Response and King County.

In rare cases where CAD data is shared with other partners, a third-party nondisclosure agreement is signed.

6.4 How does the project/technology review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?

Department leadership and the Seattle City Attorney's Office review and approve data-sharing with external agencies like King County EMS and partners such as ESO and AMR.

6.5 Explain how the project/technology checks the accuracy of the information collected. If accuracy is not checked, please explain why.

There is a dedicated quality assurance manager at the Fire Alarm Center who is responsible for reviewing all 911 calls and CAD data. King County EMS also provides some oversight relating to aggregated data.

6.6 Describe any procedures that allow individuals to access their information and correct inaccurate or erroneous information.

All patients can request reports from CAD via the Public Disclosure Officer (PDO). However, the PDO and other SFD staff will never alter a record once it has been created.

If a data error is discovered, the quality assurance manager at the FAC will make note of the error and any subsequent corrections made to a record.

7.0 Legal Obligations, Risks and Compliance

7.1 What specific legal authorities and/or agreements permit and define the collection of information by the project/technology?

CAD is an integral part of the Seattle Fire Department's ability to adequately deliver the services required by law:

- RCW 35.22.280 enumerates the powers afforded to first class cities, including Seattle: http://app.leg.wa.gov/rcw/default.aspx?cite=35.22.280. The subsequent authority of the Seattle
- The Fire Department charter to provide emergency services can be found in Article X: http://clerk.seattle.gov/~public/charter/charter.htm#articleV
- RCW 35A.92.010 sets reporting standards for city fire departments, the requirements of which rely on CAD to meet: http://app.leg.wa.gov/RCW/default.aspx?cite=35.103.010

7.2 Describe what privacy training is provided to users either generally or specifically relevant to the project/technology.

Fire Alarm Center dispatchers undergo extensive training on the use of the CAD system. The need for privacy, particularly as it related to medical information, is a component of that training. Other Department personnel do not receive specific training on the use of CadView, but they do receive yearly training from the City Privacy Program regarding privacy and security awareness.

More detailed information on applicable training, see Appendix I.

7.3 Given the specific data elements collected, describe the privacy risks identified and for each risk, explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

There is potential privacy risk associated with personal information related to accidental disclosure or breach as well as public disclosure requests. Mitigations include adherence to City rules and policy regarding answering public disclosure requests, attention data and system security requirements.

Changes to program ownership and participation can result in a large number of administrators within SFD who have access to the CAD system. Mitigations include stringent attention to physical and virtual access protocols to systems and hardware.

7.4 Is there any aspect of the project/technology that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?

Sharing of incident records with law enforcement is likely the greatest cause for privacy concern. Data sharing with law enforcement occurs only when criminal involvement is suspected in an emergency event. SPD complies with CJIS requirements for investigative data collection.

Another privacy concern would be associated with the protection of records associated with emergency medical services. Mitigations are in place to adhere to the data management and security requirements of the Health Care Information Access and Disclosure Law: UHCIA under RCW 70.02.

8.0 Monitoring and Enforcement

8.1 Describe how the project/technology maintains a record of any disclosures outside of the department.

Disclosures to any other entities, including the public, are only authorized if processed and approved by the Department's Public Disclosure Officer. All disclosures are tracked in a log, which is continually updated and retained on a secure server accessible only to select employees based on departmental roles and responsibilities.

8.2 What auditing measures are in place to safeguard the information, and policies that pertain to them, as well as who has access to the audit data? Explain whether the project/technology conducts self-audits, third party audits or reviews.

The Department's FAC quality assurance specialist audits CAD data obtained via dispatch calls. After the fact, calls are reviewed and evaluate for performance and recommendations and adjustments to behaviors and protocols are made as needed.

Financial Information

Purpose

This section provides a description of the fiscal impact of the surveillance technology, as required by the surveillance ordinance.

1.0 Fiscal Impact

Provide a description of the fiscal impact of the project/technology by answering the questions below.

1.1 Current or potential sources of funding: initial acquisition costs.

Current ☒ potential ☐

Date of initial acquisition	Date of go live	Direct initial acquisition cost	Professional services for acquisition	Other acquisition costs	Initial acquisition funding source
2003	2003	$151,380	N/A	N/A	N/A

Notes:

N/A

1.2 Current or potential sources of funding: on-going operating costs, including maintenance, licensing, personnel, legal/compliance use auditing, data retention and security costs.

Current ☒ potential ☐

Annual maintenance and licensing	Legal/compliance, audit, data retention and other security costs	Department overhead	IT overhead	Annual funding source
$151,380	N/A	N/A	N/A	N/A

Notes:

N/A

1.3 Cost savings potential through use of the technology

This question is not applicable.

1.4 Current or potential sources of funding including subsidies or free products offered by vendors or governmental entities

This question is not applicable.

Expertise and References

Purpose

The following information is provided to ensure that Council has a group of experts to reference while reviewing the completed surveillance impact report ("SIR"). Any individuals or agencies referenced must be made aware ahead of publication that their information has been included. All materials must be available for Council to access or review, without requiring additional purchase or contract.

1.0 Other Government References

Please list any other government bodies that have implemented this technology and can speak to the implementation of this technology.

Agency, municipality, etc.	Primary contact	Description of current use
NORCOM 911	(425) 577-5700	Emergency dispatch
Valley Communications Center	(253) 372-1300	Emergency dispatch

2.0 Academics, Consultants, and Other Experts

Please list any experts in the technology under consideration, or in the technical completion of the service or function the technology is responsible for.

Agency, municipality, etc.	Primary contact	Description of current use
Tritech Software Solutions	Not available	Technical support contact at Tritech

3.0 White Papers or Other Documents

Please list any authoritative publication, report or guide that is relevant to the use of this technology or this type of technology.

Title	Publication	Link
Tritech Software Admin Guide	Tritech Software Systems	https://www.tritech.com/downloads/Brochure_NewCorporateCover_TriTech_CAD_911.pdf
"Technology Supplement: CAD and the Fire Service" by Charles Werner, 2014	Firehouse.com	https://www.firehouse.com/tech-comm/cad-dispatch-systems/article/12024459/fire-service-technology

City of Seattle

Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet

Purpose

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit ("RET") in order to:

- Provide a framework for the mindful completion of the SIR in a way that is sensitive to the historic exclusion of vulnerable and historically underrepresented communities. Particularly, to inform the public engagement efforts departments will complete as part of the surveillance impact report.
- Highlight and mitigate any impacts on racial equity from the adoption and the use of the technology.
- Highlight and mitigate any disparate impacts on individuals or vulnerable communities.
- Fulfill the public engagement requirements of the surveillance impact report.

Adaptation of the RET for Surveillance Impact Reports

The RET was adapted for the specific use by the Seattle Information Technology Departments' ("Seattle IT") Privacy Team, the Office of Civil Rights ("OCR"), and Change Team members from Seattle IT, Seattle City Light, Seattle Fire Department, Seattle Police Department, and Seattle Department of Transportation.

Racial Equity Toolkit Overview

The vision of the Seattle Race and Social Justice Initiative ("RSJI") is to eliminate racial inequity in the community. To do this requires ending individual racism, institutional racism and structural racism. The RET lays out a process and a set of questions to guide the development, implementation and evaluation of policies, initiatives, programs, and budget issues to address the impacts on racial equity.

1.0 Set Outcomes

1.1. Seattle City Council has defined the following inclusion criteria in the surveillance ordinance, and they serve as important touchstones for the risks departments are being asked to resolve and/or mitigate. Which of the following inclusion criteria apply to this technology?

☐ The technology disparately impacts disadvantaged groups.
☐ There is a high likelihood that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service.
☒ The technology collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection.
☐ The technology raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice.

1.2 What are the potential impacts on civil liberties through the implementation of this technology? How is the department mitigating these risks?

Some personally identifiable information (PII) gathered during emergency responses could be used to identify individuals, such as their name, home address or contact information. Medical privacy is particularly relevant in the case of pictures taken during medical emergencies. Victims of criminal activity may also be identified during incident responses, whose identities should be protected in accordance with RCW 42.56.240 and RCW 70.02.

1.3 What are the risks for racial or ethnicity-based bias through each use or deployment of this technology? How is the department mitigating these risks?

Include a description of any issues that may arise such as algorithmic bias or the possibility for ethnic bias to emerge in people and/or system decision-making.

The Seattle Fire Department is committed to equitable service delivery regardless of race, sexual orientation, income, immigration or refugee status. All individuals, including non-residents and visitors to the City will be treated with compassion, professionalism and respect by SFD personnel.

1.4 Where in the City is the technology used or deployed?

☒ all Seattle neighborhoods

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County.

If possible, please include any maps or visualizations of historical deployments / use.

Not available.

1.4.1 What are the racial demographics of those living in this area or impacted by these issues?

City of Seattle demographics: White - 69.5%; Black or African American - 7.9%; Amer. Indian & Alaska Native - 0.8%; Asian - 13.8%; Native Hawaiian & Pacific Islander - 0.4; Other race - 2.4%; Two or more races - 5.1%; Hispanic or Latino ethnicity (of any race): 6.6%; Persons of color: 33.7%.

King County demographics: White – 70.1%; Black or African American – 6.7%; American Indian & Alaskan Native – 1.1%; Asian, Native Hawaiian, Pacific Islander – 17.2%; Hispanic or Latino (of any race) – 9.4%

1.4.2 How does the Department to ensure diverse neighborhoods, communities, or individuals are not specifically targeted through the use or deployment of this technology?

The entire set of CAD data is only made available to members of the Seattle Fire Department and some Seattle IT employees who may manage the system from a technical standpoint. External agencies, including law enforcement, are only provided data for specific incidents as part of a law enforcement investigation.

1.5 How do decisions around data sharing have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

The most important consideration is the sharing of CAD data with law enforcement officials. Sensitive information on individuals and locations are often contained in CAD, including comments from dispatchers while taking calls. This information could potentially be used by law enforcement to target members of historically marginalized communities. To mitigate this risk, the Seattle Fire Department only provides information to law enforcement officials if they are conducting an active law enforcement investigation. This is confirmed by the Public Disclosure Officer and every request and outgoing record is recorded for auditing purposes.

The Public Records ACT (RCW 42.56) is also a concern, as much of the information contained in CAD data is subject to disclosure. With the exception of medical information, there is generally not a valid exemption to exert. For example, phone numbers, addresses, and even names found in CAD data are not exempt from disclosure, so members of the public and other governmental agencies can obtain the information following a formal records request. To mitigate this, the Department's Public Disclosure Officer (PDO) will work with requesters to voluntarily redact the information before disclosure. When appropriate, the Department will provide third party notice to individuals to allow them a chance to enjoin the release of records via a court order.

1.6 How do decisions around data storage and retention have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

Access to some information in CAD could be used by external actors to identify or target individuals or groups. In particular, CAD data sometimes include security or access information for some locations. The Department mitigates the risk of this information being disclosed by requiring all requests from external agencies to make a request to the Public Disclosure Officer and Privacy Champion, which in this case are the same individual. The PDO ensures the request and any information being disclosed are in accordance with applicable laws, such as RCW 42.56 (Public Records) and RCW 70.02 (Healthcare Information), as well as the City's Privacy Principles.

1.7 What are potential unintended consequences (both negative and positive potential impact)? What proactive steps can you can / have you taken to ensure these consequences do not occur.

A potential unintended consequence includes the ability for external agencies, law enforcement in particular, to track the location and history of requests for services for specific locations and individuals.

A positive potential impact includes the ability to inform first responders of dangerous locations or people that may be a threat during an emergency response. For example, some premise notes in CAD alert first responders that a building has a large basement or an individual requiring a special type of care. This does have a negative aspect though, as some notes in CAD could be used to access sensitive areas or even gather information on a individual's medical history.

The best way to prevent this is to have a subject matter expert evaluate any disclosure of CAD data and instituting strict controls over who can access the information contained in CAD, steps that have already been taken by the Department. A quality assurance manager also regularly checks the data for accuracy and compliance with Department policies and procedures related to dispatching.

2.0 Public Outreach

2.1 Organizations who received a personal invitation to participate.

Please include a list of all organizations specifically invited to provide feedback on this technology.

1. ACLU of Washington	2. Ethiopian Community Center	3. Planned Parenthood Votes Northwest and Hawaii
4. ACRS (Asian Counselling and Referral Service)	5. Faith Action Network	6. PROVAIL
7. API Chaya	8. Filipino Advisory Council (SPD)	9. Real Change
10. API Coalition of King County	11. Friends of Little Saigon	12. SCIPDA
13. API Coalition of Pierce County	14. Full Life Care	15. Seattle Japanese American Citizens League (JACL)
16. CAIR	17. Garinagu HounGua	18. Seattle Neighborhood Group
19. CARE	20. Helping Link	21. Senior Center of West Seattle
22. Central International District Business Improvement District	23. Horn of Africa	24. Seniors in Action
25. Church Council of Greater Seattle	26. International ImCDA	27. Somali Family Safety Task Force
28. City of Seattle Community Police Commission (CPC)	29. John T. Williams Organizing Committee	30. South East Effective Development
31. City of Seattle Community Technology Advisory Board	32. Kin On Community Health Care	33. South Park Information and Resource Center SPIARC
34. City of Seattle Human Rights Commission	35. Korean Advisory Council (SPD)	36. STEMPaths Innovation Network
37. Coalition for Refugees from Burma	38. Latina/o Bar Association of Washington	39. University of Washington Women's Center
40. Community Passageways	41. Latino Civic Alliance	42. United Indians of All Tribes Foundation
43. Council of American Islamic Relations - Washington	44. LELO (Legacy of Equality, Leadership, and Organizing)	45. Urban League
46. East African Advisory Council (SPD)	47. Literacy Source	48. Wallingford Boys & Girls Club
49. East African Community Services	50. Millionair Club Charity	51. Washington Association of Criminal Defense Lawyers
52. Education for All	53. Native American Advisory Council (SPD)	54. Washington Hall
55. El Centro de la Raza	56. Northwest Immigrant Rights Project	57. West African Community Council
58. Entre Hermanos	59. OneAmerica	60. YouthCare
61. US Transportation expertise	62. Local 27	63. Local 2898
64. (SPD) Demographic Advisory Council	65. South Seattle Crime Prevention Coalition (SSCPC)	66. CWAC
67. NAAC		

2.2 Additional Outreach Efforts

Department	Outreach Area	Description
ITD	Social Media Outreach Plan: Twitter	Directed Tweets and Posts related to Open Public Comment Period for Group 2 Technologies, as well as the BKL event.
SPD, SFD, OPCD, OCR, SPL, SDOT, SPR, SDCI, SCL, OLS, Seattle City Council	Social Media Outreach Plan: Twitter	Tweets and Retweets regarding Group 2 comment period and/or BKL event.
ITD	Press Release	Press release sent to several Seattle media outlets.
ITD	Ethnic Media Press Release	Press Release sent to specific ethnic media publications.
ITD	Social Media Outreach Plan: Facebook Event Post	Seattle IT paid for boosted Facebook posts for their BKL event.
ITD	CTAB	Presented and utilized the Community Technology Advisory Board (CTAB) network and listserv for engaging with interested members of the public
ITD	Blog	Wrote and published a Tech Talk blog post for Group 2 technologies, noting the open public comment period, BKL event, and links to the online survey/comment form.
ITD	Technology Videos	Seattle IT worked with the Seattle Channel to produce several short informational/high level introductory videos on group 2 technologies, which were posted on seattle.gov/privacy. And used at a number of Department of Neighborhoods-led focus groups.

2.3 Scheduled public meeting(s).

Meeting notes, sign-in sheets, all comments received, and questions from the public will be included in Appendix B, C, D, E, F and G. Comment analysis will be summarized in section 3.0 Public Comment Analysis.

Location	Bertha Knight Landes Room, 1st Floor City Hall 600 4th Avenue, Seattle, WA 98104
Time	February 27, 2018; 6 p.m. – 8 p.m.
Capacity	100+
Link to URL Invite	BKL Event Invitation

2.4 Scheduled focus Group Meeting(s)

Meeting 1

Community Engaged	Council on American-Islamic Relations - Washington (CAIR-WA)
Date	Thursday, February 21, 2019

Meeting 2

Community Engaged	Entre Hermanos
Date	Thursday, February 28, 2019

Meeting 3

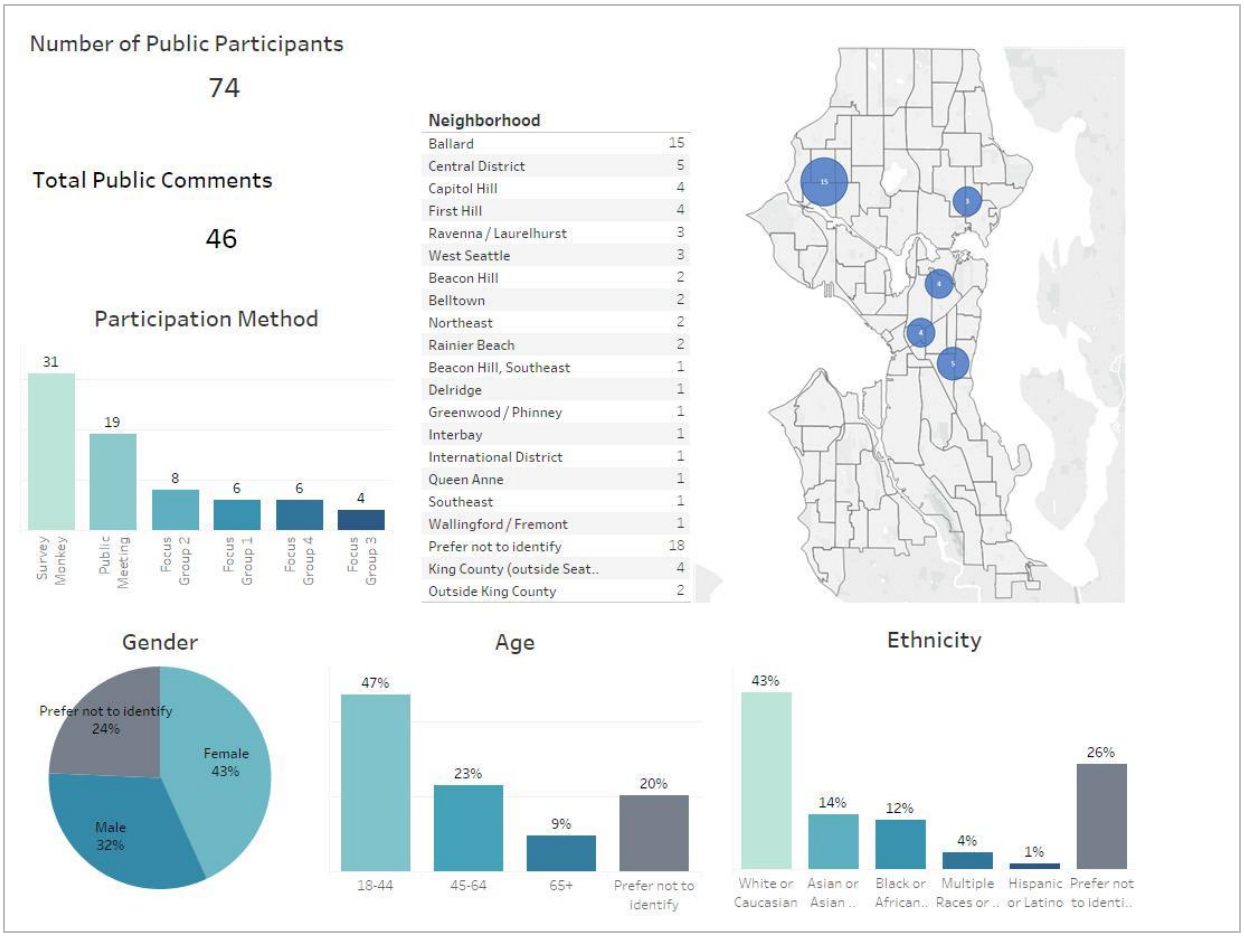
Community Engaged	Byrd Barr Place
Date	Thursday, February 28, 2019

Meeting 4

Community Engaged	Friends of Little Saigon
Date	Wednesday, February 27, 2019

3.0 Public Comment Analysis

3.1 Summary of Response Volume



3.2 Question One: What concerns, if any, do you have about the use of this technology?

Due to the low volume of responses received about this technology, a comment analysis was not able to be completed. Please see Appendix E for all comments received from the public about this technology.

3.3 Question Two: What value, if any, do you see in the use of this technology?

Due to the low volume of responses received about this technology, a comment analysis was not able to be completed. Please see Appendix E for all comments received from the public about this technology.

3.4 Question Three: What do you want City leadership to consider about the use of this technology?

Due to the low volume of responses received about this technology, a comment analysis was not able to be completed. Please see Appendix E for all comments received from the public about this technology.

3.5 Question Four: Do you have any other comments?

Due to the low volume of responses received about this technology, a comment analysis was not able to be completed. Please see Appendix E for all comments received from the public about this technology.

4.0 Equity Annual Reporting

4.1 What metrics for this technology be reported to the CTO for the annual equity assessments?

The Seattle Fire Department is currently working to finalize these metrics.

Privacy and Civil Liberties Assessment

Purpose

This section shall be completed after public engagement has concluded and the department has completed the racial equity toolkit section above. The privacy and civil liberties assessment is completed by the community surveillance working group ("working group"), per the surveillance ordinance which states that the working group shall:

"Provide to the executive and the City Council a privacy and civil liberties impact assessment for each SIR that must be included with any departmental request for surveillance technology acquisition or in-use approval. The impact assessment shall include a description of the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities. The CTO shall share with the working group a copy of the SIR that shall also be posted during the period of public engagement. At the conclusion of the public engagement period, the CTO shall share the final proposed SIR with the working group at least six weeks prior to submittal of the SIR to Council for approval. The working group shall provide its impact assessment in writing to the executive and the City Council for inclusion in the SIR within six weeks of receiving the final proposed SIR. If the working group does not provide the impact assessment before such time, the working group must ask for a two-week extension of time to City Council in writing. If the working group fails to submit an impact statement within eight weeks of receiving the SIR, the department and City Council may proceed with ordinance approval without the impact statement."

Working Group Privacy and Civil Liberties Assessment

The Working Group's Privacy and Civil Liberties Impact Assessment for this technology is below, and is also included in the Ordinance submission package, available as an attachment.

From: Seattle Community Surveillance Working Group (CSWG) To: Seattle City Council

Date: June 4, 2019

Re: Privacy and Civil Liberties Impact Assessment for Computer-Aided Dispatch (Seattle Fire Department)

Executive Summary

On April 25, 2019, the CSWG received the Surveillance Impact Report (SIR) on Computer-Aided Dispatch (CAD), a surveillance technology used by the Seattle Fire Department (SFD) included in Group 2 of the Seattle Surveillance Ordinance technology review process. This document is CSWG's Privacy and Civil Liberties Impact Assessment for this technology as set forth in SMC 14.18.080(B)(1), which we provide for inclusion in the final SIR submitted to the City Council.

This document first provides background information on CAD technology (SFD) (TriTech), and then lists key concerns, outstanding questions, and recommendations on the technology.

Our assessment of CAD (SFD) focuses on three major issues rendering protections around this technology inadequate:

(1) No limits on data retention.
(2) Lack of clarity on what data is accessible to the vendor.
(3) Lack of clarity on data sharing partners.
(4) Lack of clarity on whether original contracts and privacy policies have remained unchanged as a result of the CentralSquare merger (TriTech joined a merger with 3 other companies in 2018).

Background on Computer-Aided Dispatch (CAD) (TriTech)– Seattle Fire Department (SFD)

Computer Aided Dispatch (CAD) is a suite of software packages, provided by TriTech, and used by SFD to provide unit recommendations for 9-1-1 emergency calls based on the reported problem and location of a caller. CAD allows SFD to manage emergency and non-emergency call taking and dispatching operations. The technology allows SFD to quickly enable personnel to execute rapid aid deployment.

In September 2018, TriTech joined a merger with Superion, Zuercher, and Aptean, leading to the creation of a new entity called CentralSquare.[1] Though TriTech is still the underlying technology supplying SFD with CAD services, CentralSquare is now the dispatch service provider.

To its credit, SFD clearly defines the purpose of use and specifies policies on operation and training. However, SFD should justify its data retention policies, clarify what data is retained within CAD, provide information about its data sharing partners, and clarify if the original contracts and privacy policies with TriTech have remained unchanged as a result of the CentralSquare merger.

Key Concerns

(1) **No limits on data retention.** Section 5.4 of the SIR states: "Data is retained for the life of the system." It is not clear how indefinite retention of this data is justified by the purpose of the technology, which is management of emergency calls. Additionally, this data likely includes personally identifiable information (e.g., names, addresses, and phone numbers), but exactly what data is being retained is not clearly specified.

(2) **Lack of clarity on what data is accessible to the vendor (TriTech/CentralSquare).** It is unclear if the CAD system stores data, and what data is accessible to the vendor (e.g., call logs).

(3) **No clear limits on and terms of third party data sharing.** In Section 6.3 of the SIR, SFD states that in rare cases where CAD data is shared with partners other than those specifically named in the SIR (e.g., University of Washington's Harborview Medical Center, American Medical Response, and King County), a third-party nondisclosure agreement is signed. However, there are no examples or details of who these other partners are and the purposes for which CAD data would be shared. Furthermore, the diagram on page 306, "Seattle Fire Department: Computer Aided Dispatch Environment"[2] depicts an SFD-owned reporting server that has a database replication of the TriTech server CAD data. That reporting server then connects to "SFDINTSPD" which in turn connects to "SPD CAD (Versaterm) & COPS Application". The network lines on this diagram indicate that Seattle Police Department's (SPD) access to SFD CAD data is continuous and not on an as-needed basis, and is reviewed by SFD before being supplied to SPD. Whether or not SPD has continuous/full access to SFD CAD data, and for what purpose, needs to be clarified.

[1] https://www.centralsquare.com/article/superion-tritech-zuercher-and-apteans-public-sector-business-merge-form-centralsquare

(4) **Lack of clarity on whether original contracts and privacy policies have remained unchanged as a result of the CentralSquare merger.** Due diligence should be exercised to ensure that CentralSquare is keeping up to date with industry best practices for security and data protection, and that the original contracts and privacy policies as described in the SIR have remained unchanged as a result of the merger.

Outstanding Questions

- Does the CAD system itself store data? If so, what data and for how long? Who can access that data?
- What is the exhaustive list of SFD's data sharing partners? For what purpose is data shared with them? Is there a contract or NDA with each one?
- Does SPD have continuous/full access to SFD CAD data or is that data provided on an as-needed basis after review by SFD? If not, what limits the scope of data sharing with SPD?
- Have the original contracts and privacy policies as described in the SIR remained unchanged as a result of the CentralSquare merger?

Recommendations

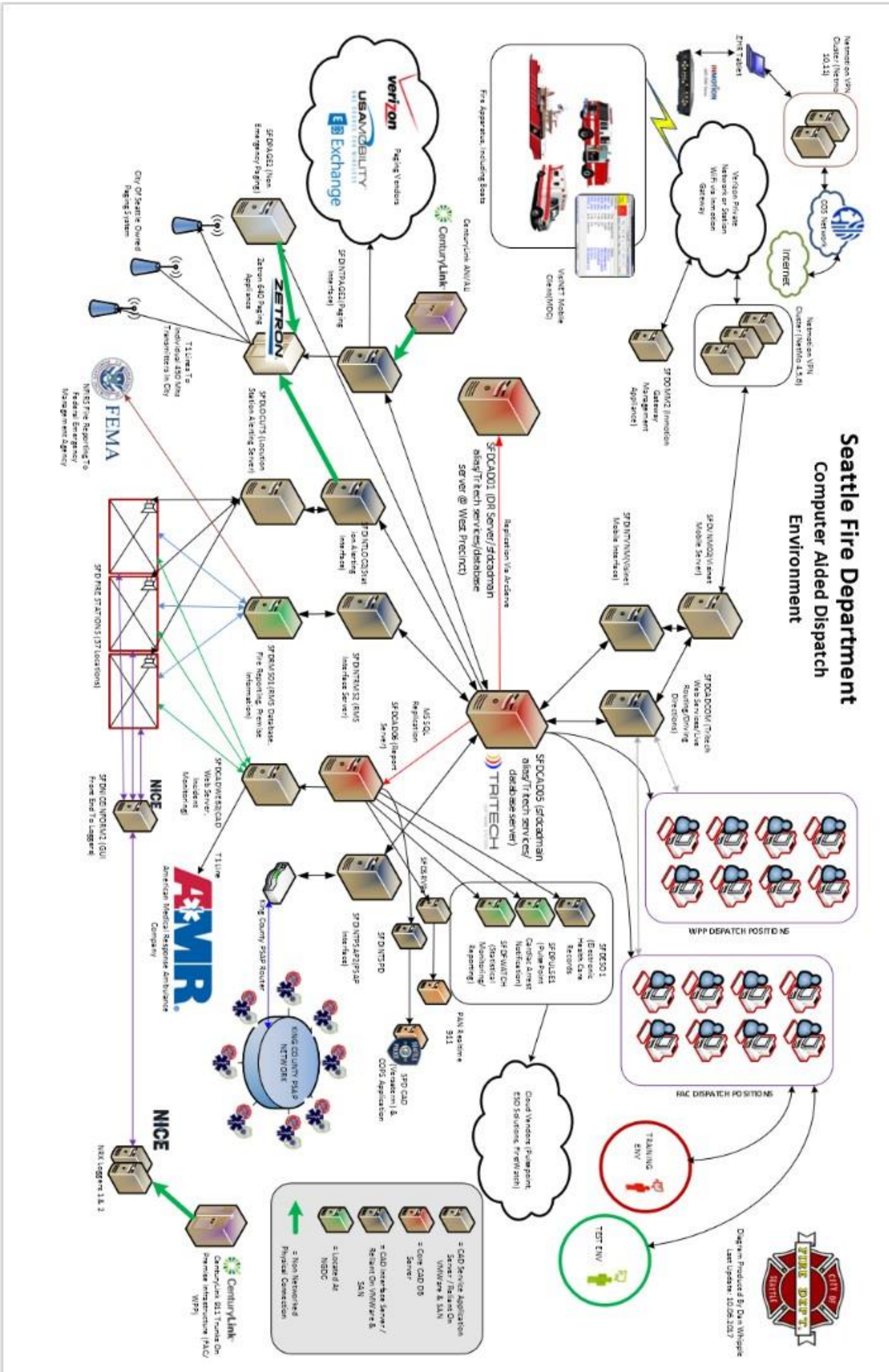
Depending on the answers to the questions above, additional recommendations may be added.

The Council should ensure that SFD adopt clear and enforceable policies that ensure, at a minimum, the following:

(1) The purpose of use of CAD (SFD) must be clearly defined as emergency operations, and its operation and data collected must be explicitly restricted to that purpose only.
(2) Data retention must be limited to the time needed to effectuate the purpose defined (i.e., CAD data that is no longer needed must be promptly deleted)—in other words, the current indefinite retention policy should be justified or ended.
(3) Data sharing with third parties, if any, must be limited to those held to the same restrictions as SFD, and all partnerships and data flows between SFD and third parties must be explicitly disclosed and protected by written agreements.
(4) Clear policies must govern operation of CAD, and all operators should be trained in those policies.

[2] See Appendix 1: Seattle Fire Department: Computer Aided Dispatch Environment

Appendix 1: Seattle Fire Department: Computer Aided Dispatch Environment



City of Seattle

CTO Response

Memo

Date: 11/16/2020

To: Seattle City Council, Transportation and Utilities Committee

From: Saad Bashir

Subject: CTO Response to the Surveillance Working Group SFD Computer Aided Dispatch SIR Review

---

To the Council Transportation and Utilities Committee Members,

I look forward to continuing to work together with Council and City departments to ensure continued transparency about the use of surveillance technologies and finding a mutually agreeable means to use technology to improve City services while protecting the privacy and civil rights of the residents we serve. Specific concerns in the Working Group comments about SFD CAD are addressed below:

As provided in the Surveillance Ordinance, SMC 14.18.080, this memo outlines the Chief Technology Officer's (CTO's) response to the Surveillance Working Group assessment on the Surveillance Impact Report for Seattle Fire Department's Computer Aided Dispatch

Background

The Information Technology Department (ITD) is dedicated to the Privacy Principles and Surveillance Ordinance objectives to provide oversight and transparency about the use and acquisition of specialized technologies with potential privacy and civil liberties impacts. All City departments have a shared mission to protect lives and property while balancing technology use and data collection with negative impacts to individuals. This requires ensuring the appropriate use of privacy invasive technologies through technology limitations, policy, training and departmental oversight.

The CTO's role in the SIR process has been to ensure that all City departments are compliant with the Surveillance Ordinance requirements. As part of the review work for surveillance technologies, ITD's Privacy Office has facilitated the creation of the Surveillance Impact Report documentation, including collecting comments and suggestions from the Working Group and members of the public about these technologies. IT and City departments have also worked collaboratively with the Working Group to answer additional questions that came up during their review process.

Technology Purpose

Computer Aided Dispatch (CAD) is a suite of software packages that provide unit recommendations for 911 emergency calls based on the reported problem and location of a caller. The Seattle Fire Department uses

CAD to manage dispatches for thousands of responses each year. TriTech's Respond CAD, Computer Aided Dispatch (CAD) solution was developed exclusively for EMS agencies to manage emergency and non-emergency call taking and dispatching operations. This solution captures all major data points throughout each call to provide comprehensive data collection to immediately enable personnel to execute rapid aid deployment in emergency situations.

Working Group Concerns

In their review, the Working Group has raised concerns about these devices being used in a privacy impacting way, including data retention and data sharing. Their specific concerns include:

(1) No limits on data retention.
(2) Lack of clarity on what data is accessible to the vendor.
(3) Lack of clarity on data sharing partners.
(4) Lack of clarity on whether original contracts and privacy policies have remained unchanged as a result of the CentralSquare merger (TriTech joined a merger with 3 other companies in 2018).

We believe that policy, training and technology limitations enacted by Seattle Fire Department provide adequate mitigation for the potential privacy and civil liberties concerns raised by the Working Group about the use of this important operational technology.

Response to Specific Concerns: Computer Aided Dispatch

Concern: No limits on data retention

SIR Response:
Section 5.2: How will the owner allow for departmental and other entities, to audit for compliance with legal deletion requirements?

All records are kept in accordance with state retention requirements.

Section 5.4: which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

Data is retained for the life of the system. The following roles are responsible for ensuring compliance with data retention requirements:

- Assistant Chief of Risk Prevention
- Communications Deputy Chief

Concern: Lack of clarity on what data is accessible to the vendor

CTO Assessment: The contract between SFD and the vendor ESO stipulates protections to customer information, including Personal Health Information (PHI) collected through the system. Contractually, ESO may only access aggregated information for reporting purposes only. ESO will not, without Customer consent or permitted by law, disclose PHI. This is consistent with privacy protections in all City vendor agreements concerning data collected in the course of providing application and computerized platform services.

The data specifically protected (PHI) is defined under the federal Health Insurance Portability and Accountability Act (HIPAA, 1996) as any identifiable health information that is used, maintained, stored, or transmitted by a HIPAA-covered entity – a healthcare provider, health plan or health insurer, or a healthcare clearinghouse – or a business associate of a HIPAA-covered entity, in relation to the provision of healthcare or payment for healthcare services.

The 18 identifiers that make health information PHI are:

- Names
- Dates, except year
- Telephone numbers
- Geographic data
- FAX numbers
- Social Security numbers
- Email addresses
- Medical record numbers
- Account numbers
- Health plan beneficiary numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers including license plates
- Web URLs
- Device identifiers and serial numbers
- Internet protocol addresses
- Full face photos and comparable images
- Biometric identifiers (i.e. retinal scan, fingerprints)
- Any unique identifying number or code[i]

SIR Response:
Vendor Contract, Section 15(f)

f. Aggregate Data Reporting. Customer hereby grants ESQ the right to collect and store its data for aggregate reporting purposes, but in no event shall ESQ disclose Protected Health Information ***("PHI")*** unless permitted by law. Moreover, ESO will not identify Customer without Customer's consent.

Concern: Lack of clarity on data sharing partners

CTO Assessment: The SIR clearly outlines the SFD partners, including City agencies, with whom they share data through the CAD system. All access is guided through role-based requirements to provide required services or support the technology. Data sharing documented through policy and audited to ensure compliance. These data-sharing partners include:

- SFD Dispatchers
- SFD personnel (role-based access)
- American Medical Response (AMR)
- King County (nightly extract)

- University of Washington /Harborview Medical Center
- Limited data to the public via Realtime 911; Link: http://www2.seattle.gov/fire/realtime911/getRecsForDatePub.asp?action=Today&incDate=&rad1=des
- SPD (in cases of suspected criminal activity)
- National Fire Protection Association –NFPA (Quarterly regulatory requirement)
- CPR volunteers (via Pulse Point phone app)
- ITD (Limited to staff supporting the SFD CAD system)
- ESO Solutions (vendor)

Further details about the specific data that is shared and why the data sharing is necessary is available in the SIR responses concerning data sharing and provided below:

SIR Response:
Section 4.7: How will data that is collected be accessed and by whom?

Access to CAD systems and data are as following:

- Caller information is collected by SFD dispatchers. The data is then accessible by all Fire Department personnel and is role-based depending on need to access the information and system.
- CAD data is also shared with American Medical Response (AMR) in real-time in order to coordinate resources needed for basic life support (BLS) EMS calls. AMR has their own access into the CAD system via Mobile Data Computer (MDC) in real time to aid in determining dynamic resource allocation and immediate response dispatch if warranted by the emergency.
- Some basic information including emergency response time, location, whether the incident is active or closed, and the date and time is also available online to the public via Realtime 911: http://www2.seattle.gov/fire/realtime911/ with a one-minute delay.
- Pulse Point, a phone app that coordinates CPR volunteers and the location of AEDs with emergency cardiac victims. The app receives CAD info on cardiac emergencies at the same rate as the SFD personnel do for specific cardiac event response and public assistance for CPR. This has saved lives over the use of the system.
- Additionally, incidental data access may occur through delivery of technology client services. All ITD employees are required to comply with appropriate regulatory requirements regarding security and background review. Information on the ITD roles associated with client services for City Departments can be found in Appendix I.

Section 4.8: If operated or used by another entity on behalf of the City, provide details about access, and applicable protocols.

The following are entities that use the CAD system:

- AMR accesses a limited view of CAD data for staging ambulances close to an incident. The data access and protocols for use are outlines in the memorandum of agreement (MOA) between the company of SFD, in Appendix I.

- King County gets a nightly extract of the data via an electronic health records (eHR) data export of CAD to a data secure FTP server.
- NFPA(FEMA/DHS) receives a quarterly update on performance measure, per regulatory requirement.

Section 6.1: Which entity or entities inside and external to the City will be data sharing partners?

Data sharing partners include:

- American Medical Response (AMR)
- The University of Washington, Harborview Medical Center (UWHMC)
- ESO Solutions, current vendor for electronic healthcare records (eHR)
- King County – King County Emergency Medical Services (KC EMS) contracts through KC for hosted records access
- In case of suspected criminal activity resulting in or from an emergency response, applicable event data is provided to SPD for investigative purposes.

Section 6.2: Why is data sharing necessary?

- Data sharing is necessary for coordinated, rapid responses to 911 incidents, particularly reducing the amount of time needed to make contact with patients and thereby improve outcomes.
- Specifically, sharing with the University of Washington is for quality assurance and research purposes, including cardiac arrest data. Aggregated CAD data is also shared with King County for quality assurance and comparison with other local Fire and EMS agencies. Sharing with AMR is necessary for coordinating EMS responses in real-time. The eHR software uses CAD data to fill out incident details in electronic healthcare records, which are subsequently provided to emergency room staff for continuity of patient care.

Concern: Lack of clarity on whether original contracts and privacy policies have remained unchanged as a result of the CentralSquare merger (TriTech joined a merger with 3 other companies in 2018).

CTO Assessment: As this SIR was drafted and finalized in 2018 prior to the CentralSquare merger, the SIR may not reflect any information around the contracts and policies surrounding the merger. Reviewing the contractual agreements post-merger, the privacy and contractual provisions remain unchanged. SFD's CAD data is not shared with the vendor or any of the other customers they have acquired.

SIR Response:
The SIR was drafted prior to the CentralSquare merger and does not currently contain reference to this change.

Appendix A: Glossary

Accountable: (taken from the racial equity toolkit.) Responsive to the needs and concerns of those most impacted by the issues you are working on, particularly to communities of color and those historically underrepresented in the civic process.

Community outcomes: (taken from the racial equity toolkit.) The specific result you are seeking to achieve that advances racial equity.

Contracting equity: (taken from the racial equity toolkit.) Efforts to achieve equitable racial outcomes in the way the City spends resources, including goods and services, consultants and contracting.

DON: "department of neighborhoods."

Immigrant and refugee access to services: (taken from the racial equity toolkit.) Government services and resources are easily available and understandable to all Seattle residents, including non-native English speakers. Full and active participation of immigrant and refugee communities exists in Seattle's civic, economic and cultural life.

Inclusive outreach and public engagement: (taken from the racial equity toolkit.) Processes inclusive of people of diverse races, cultures, gender identities, sexual orientations and socio-economic status. Access to information, resources and civic processes so community members can effectively engage in the design and delivery of public services.

Individual racism: (taken from the racial equity toolkit.) Pre-judgment, bias, stereotypes about an individual or group based on race. The impacts of racism on individuals including white people internalizing privilege, and people of color internalizing oppression.

Institutional racism: (taken from the racial equity toolkit.) Organizational programs, policies or procedures that work to the benefit of white people and to the detriment of people of color, usually unintentionally or inadvertently.

OCR: "Office of Civil Rights."

Opportunity areas: (taken from the racial equity toolkit.) One of seven issue areas the City of Seattle is working on in partnership with the community to eliminate racial disparities and create racial equity. They include: education, health, community development, criminal justice, jobs, housing, and the environment.

Racial equity: (taken from the racial equity toolkit.) When social, economic and political opportunities are not predicted based upon a person's race.

Racial inequity: (taken from the racial equity toolkit.) When a person's race can predict their social, economic, and political opportunities and outcomes.

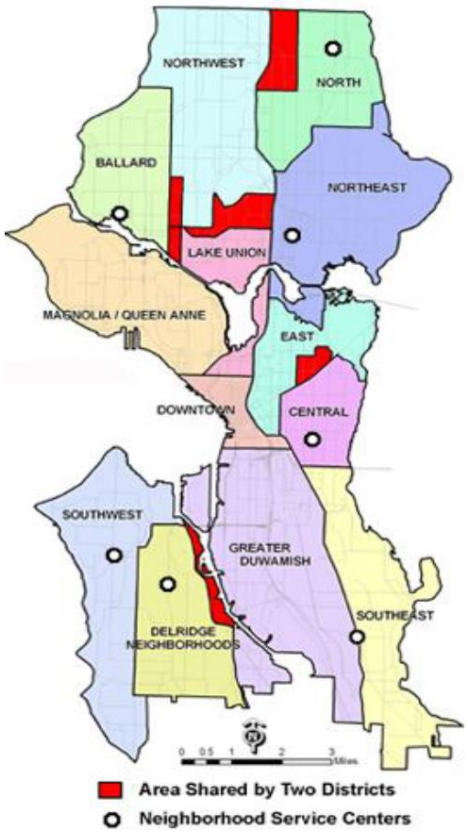
RET: "racial equity toolkit"

Seattle neighborhoods: (taken from the racial equity toolkit neighborhood.) Boundaries defined for the purpose of understanding geographic areas in Seattle.

Stakeholders: (taken from the racial equity toolkit.) Those impacted by proposed policy, program, or budget issue who have potential concerns or issue expertise. Examples might include: specific racial/ethnic groups, other institutions like Seattle housing authority, schools, community-based organizations, change teams, City employees, unions, etc.

Structural racism: (taken from the racial equity toolkit.) The interplay of policies, practices and programs of multiple institutions which leads to adverse outcomes and conditions for communities of color compared to white communities that occurs within the context of racialized historical and cultural conditions.

Surveillance ordinance: Seattle City Council passed ordinance 125376, also referred to as the "surveillance ordinance."



SIR: "surveillance impact report", a document which captures the fulfillment of the Council-defined surveillance technology review process, as required by ordinance 125376.

Workforce equity: (taken from the racial equity toolkit.) Ensure the City's workforce diversity reflects the diversity of Seattle.

Appendix B: Meeting Notice(s)

City of Seattle

City Surveillance Technology Fair

February 27, 2018
6:00 p.m. – 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Join us for a public meeting to comment on a few of the City's surveillance technologies:

Seattle City Light
- Binoculars
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation
- Acyclica

Seattle Fire Department
- Computer Aided Dispatch

Seattle Police Department
- 911 Call Logging Recorder
- Computer Aided Dispatch
- CopLogic

Can't join us in person?

Visit www.seattle.gov/privacy to leave an online comment or send your comment to **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** The Open Comment period is from **February 5 - March 5, 2019.**

Please let us know at Surveillance@seattle.gov if you need any accommodations. For more information, visit Seattle.gov/privacy.

Surveys, sign-in sheets and photos taken at this event are considered a public record and may be subject to public disclosure. For more information see the Public Records Act RCW Chapter 42.56 or visit Seattle.gov/privacy. All comments submitted will be included in the Surveillance Impact Report.

City of Seattle

Giám Sát Thành Phố Hội Chợ Công Nghệ

ngày 27 tháng 2 năm 2019
6 :00 giờ chiều – 8:00 giờ chiều
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Hãy tham gia cuộc họp công cộng cùng chúng tôi để nhận xét về một số công nghệ giám sát của Thành phố:

Seattle City Light
- Ống nhòm quan sát
- Sensorlink Ampstik
- Đồng hồ đo máy biến áp của Sensorlink

Seattle Department of Transportation (Sở Giao Thông Vận Tải Seattle)
- Acyclica

Seattle Fire Department (Sở Phòng Cháy Chữa Cháy Seattle)
- Hệ Thống Thông Tin Điều Vận Có Máy Tính Trợ Giúp

Seattle Police Department (Sở Cảnh Sát Seattle)
- Hệ Thống Ghi Âm Cuộc Gọi 911
- Hệ Thống Thông Tin Điều Vận Có Máy Tính Trợ Giúp
- CopLogic

Quý vị không thể tới tham dự trực tiếp cùng chúng tôi?

Hãy truy cập www.seattle.gov/privacy và để lại nhận xét trực tuyến hoặc gửi ý kiến của quý vị tới **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** Giai đoạn Góp Ý Mở từ **Ngày 5 tháng 2 - Ngày 5 tháng 3 năm 2019.**

Vui lòng thông báo cho chúng tôi tại Surveillance@seattle.gov nếu quý vị cần bất kỳ điều chỉnh nào. Để có thêm thông tin, hãy truy cập Seattle.gov/privacy.

Các khảo sát, danh sách đăng ký và ảnh chụp tại sự kiện này được coi là thông tin công cộng và có thể được tiết lộ công khai. Để biết thêm thông tin, hãy tham khảo Public Records Act (Đạo Luật Hồ Sơ Công Cộng) RCW Chương 42.56 hoặc truy cập Seattle.gov/privacy. Tất cả các ý kiến đóng góp mà quý vị gửi đến sẽ được đưa vào Báo Cáo Tác Động Giám Sát.

City of Seattle

Eksibisyon ng Teknolohiya Sa Pagmamatyag sa Lungsod

Pebrero 27, 2019

6:00 p.m. - 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Samahan kami para sa isang pampublikong pagpupulong upang magbigay ng komento sa ilan sa mga teknolohiya sa pagmamanman ng Lungsod:

Seattle City Light
- Mga Binocular
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation (Departamento ng Transportasyon ng Seattle)
- Acyclica

Seattle Fire Department (Departamento para sa Sunog ng Seattle)
- Pagdispatsa sa Tulong ng Computer

Seattle Police Department (Departamento ng Pulisya ng Seattle)
- Rekorder ng Pagtawag sa 911
- Pagdispatsa sa Tulong ng Computer
- CopLogic

Hindi kami masasamahan nang personal?

Bumisita sa www.seattle.gov/privacy upang mag-iwan ng online na komento o ipadala ang iyong komento sa **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** Ang panahon ng Bukas na Pagkomento ay sa **Pebrero 5 - Marso 5, 2019.**

Mangyaring ipaalam sa amin sa Surveillance@seattle.gov kung kailangan mo ng anumang tulong. Para sa higit pang impormasyon, bumisita sa Seattle.gov/privacy.

Itinuturing na pampublikong rekord ang mga survey, papel sa pag-sign-in at mga larawan na makukuha sa pangyayaring ito at maaaring mapasailalim sa paghahayag sa publiko. Para sa higit pang impormasyon, tingnan ang Public Records Act (Batas sa Mga Pampublikong Rekord) RCW Kabanata 42.56 o bumisita sa Seattle.gov/privacy. Isasama ang lahat ng isinumiteng komento sa Surveillance Impact Report (Ulat sa Epekto ng Pagmamanman).

City of Seattle

Feria de tecnología de vigilancia ciudadana

27 febrero de 2019

De 6:00 p. m. a 8:00 p. m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Acompáñenos en la reunión pública para dar su opinión sobre algunas de las tecnologías de vigilancia de la ciudad:

Seattle City Light
- Binoculars
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation (Departamento de Transporte de Seattle)
- Acyclica

Seattle Fire Department (Departamento de Bomberos de Seattle)
- Computer Aided Dispatch

Seattle Police Department (Departamento de Policía de Seattle)
- 911 Call Logging Recorder
- Computer Aided Dispatch
- CopLogic

¿No puede asistir en persona?

Visite www.seattle.gov/privacy para dejar un comentario en línea o enviar sus comentarios a **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** El período de comentarios abiertos es desde el **5 de febrero al 5 de marzo de 2019.**

Avísenos en Surveillance@seattle.gov si necesita adaptaciones especiales. Para obtener más información, visite seattle.gov/privacy.

Las encuestas, las planillas de asistencia y las fotos que se tomen en este evento se consideran de dominio público y pueden estar sujetas a la difusión pública. Para obtener más información, consulte la Public Records Act (Ley de Registros Públicos), RCW capítulo 42.56, o visite Seattle.gov/privacy. Todos los comentarios enviados se incluirán en el Informe del efecto de la vigilancia.

City of Seattle

Kormeerida Bandhigga Tiknoolajiyada ee Magaalada

Feebaraayo 27, 2019
6:00 p.m. - 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Nagulasoo biir bandhigga dadweynaha si fikir looga dhiibto dhawr kamid ah aaladaha tiknoolajiyada ee City surveillance:

Seattle City Light
- Binoculars
- Sensorlink Ampstik
- Sensorlink Cabiraha mitirka Gudbiyaha

Seattle Department of Transportation
(Waaxda Gaadiidka ee Seattle)
- Acyclica

Seattle Fire Department
(Waaxda Dab damiska ee Seattle)
- Adeeg Qaybinta Kumbuyuutarka loo adeegsado

Seattle Police Department
(Waaxda Booliiska ee Seattle)
- Qalabka Duuba Wicitaanada 911
- Computer Aided Dispatch
- CopLogic

Nooguma imaan kartid miyaa si toos ah?

Booqo barta www.seattle.gov/privacy si aad fikirkaaga oonleen ahaan uga dhiibato **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.**
Mudada Fikrad Dhiibashadu furantahay waxay kabilaabanaysaa **Feebaraayo 5 - Maarso 5, 2019.**

Fadlan noogusoo gudbi ciwaankaan Surveillance@seattle.gov hadaad ubaahantahay hooy laguusii qabto. Wixii macluumaad dheeri ah, booqo Seattle.gov/privacy.

Xog aruurinada, waraaqaha lasaxixaayo iyo sawirada lagu qaado munaasabadaan waxaa loo aqoonsanayaa diiwaan bulsho waxaana suuragal ah in bulshada lagu dhex faafiyo. Wixii macluumaad dheeri ah kafiiri Public Records Act (Sharciga Diiwaanada Bulshada) RCW Cutubkiisa 42.56 ama booqo Seattle.gov/privacy. Dhammaan fikradaha ladhiibto waxaa lagusoo darayaa Warbixinta ugu danbaysa ee Saamaynta Qalabka Muraaqabada.

City of Seattle

城市监控技术博览会

2019 年 2 月 27 日
下午 6:00 至下午 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 9810

加入我们的公众会议，留下您对纽约市监控技术的意见：

Seattle City Light
- 望远镜
- Sensorlink Ampstik
- Sensorlink 变压器表

Seattle Department of Transportation（西雅图交通局）
- Acyclica

Seattle Fire Department（西雅图消防局）
- 计算机辅助调度

Seattle Police Department（西雅图警察局）
- 911 通话记录录音器
- 计算机辅助调度
- CopLogic

无法亲自前来？

访问 www.seattle.gov/privacy 发表在线评论或将您的意见发送至 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124。开放评论期：2019 年 2 月 5 日至 3 月 5 日。

如果您需要任何住宿服务，请通过 Surveillance@seattle.gov 联系我们。
要获得更多信息，请访问 Seattle.gov/privacy。

此次活动中的调查、签到表和照片被视为公共记录，可能会被公开披露。有关更多信息，请参阅 Public Records Act（信息公开法）RCW 第 42.56 章或访问 Seattle.gov/privacy。提交的所有意见都将包含在监控影响报告内。

City of Seattle

도시 감시 기술 박람회

2019 년 2 월 27 일
오후 6:00 – 오후 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

공개모임에 참여하시고, 도시 감시 기술과 관련한 의견을 공유해 주십시오.

Seattle City Light
- 쌍안경
- Sensorlink Ampstik
- Sensorlink 변압기 미터

Seattle Department of Transportation(시애틀 교통국)
- Acyclica

Seattle Fire Department(시애틀 소방국)
- 컴퓨터 지원 출동 지시

Seattle Police Department(시애틀 경찰국)
- 911 전화 기록 녹음기
- 컴퓨터 지원 출동 지시
- CopLogic

현장 참여가 어려우신가요?

www.seattle.gov/privacy 를 방문하셔서 온라인 의견을 남기시거나 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124 로 의견을 송부해 주시기 바랍니다. 공개 의견 수렴 기간은 2019 년 2 월 5 일 – 3 월 5 일입니다.

편의사항이 필요하신 경우 Surveillance@seattle.gov 로 문의해 주시기 바랍니다.
자세한 정보는 Seattle.gov/privacy 를 참조해 주십시오.

본 행사에서 수집된 설문 조사, 참가 신청서 및 사진은 공개 기록으로 간주되며 일반에 공개될 수 있습니다. 자세한 사항은 Public Records Act(공공기록물법) RCW 챕터 42.56 을 참조하시거나, Seattle.gov/privacy 를 방문하시기 바랍니다. 제출된 모든 의견은 감시 영향 보고서에 수록됩니다.

City of Seattle

城市監視技術展覽會

2019 年 2 月 27 日
下午 6:00 至下午 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

加入我們的公眾會議，留下您對紐約市監視技術的意見：

Seattle City Light
- 望遠鏡
- Sensorlink Ampstik
- Sensorlink 變壓器表

Seattle Department of Transportation（西雅圖交通局）
- Acyclica

Seattle Fire Department（西雅圖消防局）
- 電腦輔助發送

Seattle Police Department（西雅圖警察局）
- 911 通話紀錄錄音機
- 電腦輔助發送
- CopLogic

無法親自前來？

造訪 www.seattle.gov/privacy 發表線上評論或將您的意見傳送至 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124。開放評論期：2019 年 2 月 5 日至 3 月 5 日。

如果您需要任何便利服務，請透過 Surveillance@seattle.gov 聯絡我們。要獲得更多資訊，請造訪 Seattle.gov/privacy。

此次活動中的調查、簽入表和照片被視為公共紀錄，可能會被公開披露。有關更多資訊，請查閱 Public Records Act（資訊公開法）RCW 第 42.56 章或造訪 Seattle.gov/privacy。提交的所有意見都將包含在監視影響報告內。

Appendix C: Meeting Sign-in Sheet(s)

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☒ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☒ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

☐ Include Middle Eastern

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☒ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☒ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☒ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☑ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☑ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☒ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☒ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☑ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☒ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☒ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☑ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☑ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☑ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Queen Anne

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☑ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☑ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☒ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- [x] Ballard
- [ ] Belltown
- [ ] Beacon Hill
- [ ] Capitol Hill
- [ ] Central District
- [ ] Columbia City
- [ ] Delridge
- [ ] First Hill
- [ ] Georgetown
- [ ] Greenwood / Phinney
- [ ] International District
- [ ] Interbay
- [ ] North
- [ ] Northeast
- [ ] Northwest
- [ ] Madison Park / Madison Valley
- [ ] Magnolia
- [ ] Rainier Beach
- [ ] Ravenna / Laurelhurst
- [ ] South Lake Union / Eastlake
- [ ] Southeast
- [ ] Southwest
- [ ] South Park
- [ ] Wallingford / Fremont
- [ ] West Seattle
- [ ] King county (outside Seattle)
- [ ] Outside King County

Race/Ethnicity

- [ ] American Indian or Alaska Native
- [ ] Asian
- [ ] Black or African American
- [ ] Hispanic or Latino
- [ ] Native Hawaiian or other Pacific Islander
- [x] White
- [ ] Prefer not to Identify

Age

- [ ] Under 18
- [x] 18-44
- [ ] 45-64
- [ ] 65+
- [ ] Prefer not to identify

Gender

- [x] Female
- [ ] Male
- [ ] Transgender
- [ ] Prefer not to identify

Neighborhood

- [ ] Ballard
- [ ] Belltown
- [ ] Beacon Hill
- [ ] Capitol Hill
- [ ] Central District
- [ ] Columbia City
- [ ] Delridge
- [ ] First Hill
- [ ] Georgetown
- [ ] Greenwood / Phinney
- [ ] International District
- [ ] Interbay
- [ ] North
- [ ] Northeast
- [ ] Northwest
- [ ] Madison Park / Madison Valley
- [ ] Magnolia
- [ ] Rainier Beach
- [ ] Ravenna / Laurelhurst
- [ ] South Lake Union / Eastlake
- [ ] Southeast
- [ ] Southwest
- [ ] South Park
- [x] Wallingford / Fremont
- [ ] West Seattle
- [ ] King county (outside Seattle)
- [ ] Outside King County

Race/Ethnicity

- [ ] American Indian or Alaska Native
- [ ] Asian
- [ ] Black or African American
- [ ] Hispanic or Latino
- [ ] Native Hawaiian or other Pacific Islander
- [x] White
- [ ] Prefer not to Identify

Age

- [ ] Under 18
- [x] 18-44
- [ ] 45-64
- [ ] 65+
- [ ] Prefer not to identify

Gender

- [ ] Female
- [x] Male
- [ ] Transgender
- [ ] Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☑ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☑ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☑ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☑ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☒ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☒ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☒ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☒ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☒ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☒ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☑ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

leighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
] Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☒ 18-44
☐ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☒ Female
☐ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☑ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
] Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☐ 45-64
☑ 65+
☐ Prefer not to identify

Gender

☐ Female
☑ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

☑ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
] Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☑ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☑ Female
☐ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

SE KING COUNTY

☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☑ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
✓ Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☑ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☐ Female
☑ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☒ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☒ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☒ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☒ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☒ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☑ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☑ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☑ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☑ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☑ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☑ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Appendix D: Department of Neighborhood Focus Group Notes

Friends of Little Saigon (FOLS)

Please select which technology you wish to comment on:

☐SCL: Binoculars ☐SCL: Sensorlink Transformer Meter (TMS) ☐SFD: Computer-Aided Dispatch ☐SPD:9-11 Call Recorder

☐SCL: Sensorlink Ampstik ☐SDOT: Acyclica ☐SPD: Computer-Aided Dispatch ☒SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

- Will they keep the data safe on coplogic?
- Can it be hacked?
- What if you report your neighbour and your neighbour hacks the system and find out?
- What is the money amount limit for coplogic / Why is there a limit for coplogic?: (a community member says that she believes that the limit $500 or under, but it's hard to have a limit because a lot of packages cost more than $500 such as electronics get stolen and you won't be able to report it online)
- The departement is having all these technologies being used but not letting the public aware of it
- Coplogic is not clear and is confusing to use (what you can report and what you can't report)
- If coplogic is known by the community would they use it ? (Community members agreed that no one would use coplogic because it's not in Vietnamese. Not even people who speak english fluently even use it.
- Many community members don't trust the system)

What value, if any, do you see in the use of this technology?

- Coplogic has been going on for a few years it's not very effective. The only effective thing is that coplogic is doing saving police hours and time.

What do you want City leadership to consider about the use of this technology?

- Most of the time, our community don't report things because they don't trust the system, they often tell someone that they trust a friend. Is there an option that someone and report a crime for someone else?

Other comments:

- The government should be more transparent with the technology system with the public.
- The translation is much far removed from the actual Vietnamese language.
- The translation is very hard to understand, the language is out of context (The flyer is poorly translate)
- Is there resources to support these technologies? Is there translations so that it is accessible for everyone? Will this accommodate everyone?
- Police should have a software that connects them to translation and interpretation right away instead of having to call a translator
- How will other people know of the technology if they can't come to focus group meetings? Such as flyers? Social media? Etc.
- Besides face to face meetings, are there plans to execute this information of the technology and surveillance to the community?
- Will the City of Seattle go to community events, temple, the church to reach out to the community and explain the technologies?
- These technologies are taking a part of our taxes, so everyone should know. It should be for everyone to know, not only catered to one group or population.

Are there any questions you have, or areas you would like more clarification?

- How effective are the tools/technology?
- How many people know of these technologies? Provide statistics
- What are the statistics of the coplogic?
- What is the data and statistics for coplogic and what are people reporting?
- What is the most common crime that they are reporting?
- And how effective is coplogic based on the statistics and data?

Friends of Little Saigon (FOLS)

Please select which technology you wish to comment on:

☐SCL: Binoculars ☐SCL: Sensorlink Transformer Meter (TMS) ☐SFD: Computer-Aided Dispatch ☒SPD:9-11 Call Recorder

☐SCL: Sensorlink Ampstik ☐SDOT: Acyclica ☒SPD: Computer-Aided Dispatch ☐SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

- CAD did not work from experience. A community member said that they reported that they needed assistance at 10:00pm and no one showed up, then had to call 911 at 12:00am and someone finally showed up at 4:30am
- Why create more options and technologies if the police department and government can not support it? It's a waste of time and money (taxes). Should have enough personals before they implement technology.
- Government should have enough personals to support translation if they choose to translate.

What do you want City leadership to consider about the use of this technology?

- The city should focus on having the community review the technologies that are yet to be implemented.
- The Vietnamese community is not getting the information we need to report crimes

Other comments:

- Engagement is very important. Engaging the community and engaging different demographics.
- Friday night, Saturdays, and Sunday afternoon work the best for the Vietnamese community.
- If the city wants to involve the vietnamese community and engage the Vietnamese community, it is important to accommodate with our community It is important to proofread the translation, have 3 people proofread. Someone
  pre 1975, post 1975 and current Vietnamese language. The government clearly does not proofread the translation.

Council on American Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington
Thursday, Feb. 21, 2019
Technology Discussed: CopLogic

1. Do you have concerns about this specific technology or how it's used?
    - Having used the system myself the one thing I noted was the type of report you can file, they ask questions like if you knew the suspect, and if you're saying no I don't know who did it. and you check a box that says I understand that no one is going to investigate this
        - What is the point of having a system in place than If no one is going to investigate it
        - It is for common things like my car is broken into and stuff was taken out of my car, you can file it if you need a report for insurance. But if you were to call that and report to the police, they wouldn't come for days
    - So for example if I can be a straight up Islamophobe and I can see a Muslim woman and make a bunch of false reports online, and how long would it take for someone to say I see you making all these reports. Because people can make so many different reports, how do you deal with that
        - There are very limited types of reports that it will accept. So if someone wanted to report graffiti and they were reporting more hate crime related graffiti an officer will review the report
        - So I think the review process would be really important
    - Another barrier is that it's an online system so we need to think about wifi access and there is this assumption that everyone has access to internet and computers. And what I'm hearing is that people can just file a report at a click of their finger. And if these people can do that on their computer what stops them from being able to file all these cases about certain groups and individuals.
    - Additional there have been cases in the past where people are abusing reporting system. This one doesn't allow you to report against known suspect but I could see that happening in the future so I wanted that to be mentioned. The other thing under protection is says all activity can be stored and the data Is monitored by lexis nexus… and this company does a lot of research on crime mapping which brings up some of the concerns on like CVE
        - But what you are saying is that lexis nexus does other mapping that it can use this information for
        - Yes, because I want to clarify what is the technological ambition of SPD because I don't think this would work well in the communities that SPD is supposed to served. And I would want a contract review of what lexis nexus does. Will the info stay on the data and server of lexis nexus, what happens to it
    - Another thing is has SPD given Lexis nexus to use this in any of the research data they do, because they put out a lot of information regarding mapping, and crime control. And what information are they allowed to take

- We have seen recently people doing interesting things when reporting crimes. I think its important to realize that when reporting crime people have a different perception when reporting crime. People will see you in a certain neighborhood and might think they stole that car, or are doing something bad here. So when we give people the ability to report online we need to be concerned with accessibility about people being able to report freely… and we saw for a year that if an African American person came to use a swimming pool someone can call and say they don't live here. I think SPD is trying alleviate some of those calls they are getting, but I don't think this is the solution to the problem
- What is the logic behind this overall, because is seems like it presents more cons than pros, and what is analytics database you use to look at these reports. Because when I am using government data base I can see where I need more surveillance etc. so we are getting all these open wholes in the system. Is this a right wing Donald trump agenda to watch neighbors of color and surveillance
- I think im more concerned with where does this information end up and how is it used
- What is the usefulness of the information that is not followed up on. And how does it help the people it's actually serving? So for example someone works for an anti-Muslim white supremacy group and they have people in different areas report issues about different Muslim groups in Seattle how do you prove the validity of these information and make sure they aren't just causing harm

2. What value do you think this brings to our city?
    - I think technology saves time, money, makes filing a report easy, I had to do that once it takes a lot of time.
    - I appreciate that it is easier so something like a hit or run or a car breaking in, that's fine.
3. What worries you about how this is used?
    - The only issues I can think of right now is it seems like it would be very easy to make a fraudulent report or a report that is for a small thing that you can make into a big thing, like the things you see go viral on the internet. So now it seems like the barrier to making a police report is smaller
    - I agree I think the bar is lowered and different people are perceived differently. And we have seen how SPD criminalizes different communities for behaviors that don't need to be criminalizing
    - A lot of different kinds of reports have to do with peoples perceived notion, so my concern comes from how do we make sure that this kind of technology isn't used to map our where Muslims live/are, and there types of religious belief. Or isn't being used to monitor them. How do we ensure that this isn't used to map our communities
    - The only comment I have that in the forms I have filled out is it won't allow you to fill out the form if you are naming a specific individual, you can name a group, but a not a person. The following criteria is there no known suspects, it happens in Seattle, so things like thefts. So you can report, graffiti, identity theft, credit card fraud, simple shop lift. So when I click report it says if you have a suspect it says please call. And when I press report it allows me to report anonymously, so I could report against a community with no follow up

        - Well that doesn't stop them from targeting al-Noor masjid, or Safeway in new holly, or new holly gathering hall, and it can target the people in that community. And people don't feel comfortable with increase police presences, so it targets area if not targeting people
    - When I was buying the house in Dallas (participant currently still lives/works/plays in Seattle) one of the first things I did was looking at a crime map and based off of that if someone is making a lot of reports can that be used for crime mapping because than that can lower the property value. And if the police isn't following up then how is it being used
    - Its definitely possible for people to report inaccurate information
4. What recommendations would you give policy makers at the City about this technology?
    a. But my concern is reporting someone that can really target people of color. And that happens much more threatening to people. So the concept of an upset black women is more intimidating than an upset women that is another race and how many times will behavior like that be reported. Or how many times will a black man be reported against because it seems scary. So I think it lowers the bar when you don't have to talk to an individual when you don't have to talk to a police
    b. My questions are, how accessible are cop logic to people who don't read or speak English. How is SPD going to do what they can to make sure that this doesn't negatively impact communities they are already having issues with like the Sea Tac community that already feels threaten and criminalized by communities.

5. Can you imagine another way to solve the problem this technology solves?
    - So the SPD is very data driven these days and the one thing we repeat is report report report, call 911 and report online whatever you thinking is happening because all of that goes into their data base and is used for them to use resources and put police based off of where there is more crime. The report report report mentality assumes there are good relationships between the community and police, so even if someone doesn't do something bad, I don't know that they would feel comfortable reporting, even if online
    - From the community I have come from I am almost certain that they haven't even used online reporting so how do we make sure that we are giving everyone access to use online reporting. And there are certain crimes that are so common in areas that they don't even report it because they think the police should already know about it
    - I think the department should solely rely on the technology only as a way of collecting info they should still use in personal resources to actively participant in local community and make connections you can't rely only on this technology alone to do this

6. Other comments
    a. Also in this day in age we need to consider that immigration is a issue, and this administrative has blended the different agencies so people have a hard time knowing where SPD starts and ICE starts and those lines have been blurred and that is a real concern for many families

Council on Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington

Thursday, Feb. 21, 2019

Technology Discussed: Binoculars/Spotting Scope

1. Do you have concerns about this specific technology or how it's used?
    . People in our community don't have the access to say or be apart of these conversation. A lot of these people are literate, and might not have the same cultural values. For Muslim women there are a type of consent that you have when you walk outside and are covered in a certain away versus when you are in the privacy of your own home. And people might not have that cultural and religious awareness
    a. I had one quick concerns, as far as the data that is collected using these binoculars, who has access to it
        - Seattle City Light: Information goes into the billing system, which customers can access if they have the automated reader but do not have access to under the current system
    - I know the focus is on binoculars but my mind is on new technologies and when people who are consumers and feel like I am overcharged how do I follow up and get those issues resolved. For systems that are completed based off of technologies how will I know if that data is being altered.
    b.
2. What value do you think this brings to our city?
    . I would just add this is more my general comments I think its good that Seattle city lights is providing notifications to people when this is happening. Are they wearing something visible that show people they are from Seattle city lights? And is there a way for people to complain?
        - Yes they are wearing vests that are very visible. Yes we have a couple different avenues the easiest is to call the customer service line and to submit a complaint there
3. What worries you about how this is used?
    . My primary concerns on my end is if someone is looking into my home with binoculars its a privacy concern. Most Muslim women wear hijab and I don't feel comfortable if someone is using binoculars looking from the outside when we are not wearing the hijab. My concern is that it is a huge invasion of privacy
    a. I have a question as the women expressed the feeling of people reading the meters with binoculars, if the meter has abnormal behavior or is in a different place of the house. Have there been situations where someone sees the person

looking at someone house with binoculars, and they might not have gotten notified. Or the meter might be on the opposite side of where they are looking. Are they getting background checks? Or are complaints being followed up

- Seattle City Light: Yes all city employees have background checks, and if a complaint gets called in they will go through disciplinary actions
- What are the average times for disciplinary actions. How long is the process for a full investigation
- Seattle City Light: It's a multiple step process in terms of different levels. There are warnings, and if there was undo actions. Timeline really depends, I'm not sure
- Cause I think that people who go through the different nuances of how privacy can be breach that is just the end all be all of how privacy can breach so I think there needs to be policy put in place so that people don't have their privacy breach and they are being monitored by a pedophile

4. What recommendations would you give policy makers at the City about this technology?
   . When I look at the Seattle city of light they do a lot of estimated guesses and as a consumer they might give you a $500 fee based off of the estimated guesses so I think it is important to have some sort of device that better clearly shows how much you use

5. Can you imagine another way to solve the problem this technology solves?
   . My other question is if its actually not efficient why do you get the option to opt out (of the new automated system). If there is an old school way of doing it that involves a breach of privacy because these are human beings using the binoculars, so If this other option is better why are people having the ability to opt out.
6. Other comments: (Many comments were discussed over Seattle City Light's upcoming change from binocular use to automated meter readers)
   . Who opted out was it home owners?
   a. When we go to a place with 12 tenements do all 12 of them have the ability to opt out or in, or just the owners of the building?
   b. Each home owner has a schedule provided to them and it is a 3 day period which they can come in and look at the system
   c. Is there a cost to them to have the new meter.
      - Seattle City Light: There is no cost with getting the new meter, but there is still a cost If we have to send someone out there to read it
      - What I don't understand is why the new practice is not to just use the new system since that is more accurate and it is doesn't require binoculars
      - What is the cost of opting out

    - Seattle City Light: There is a flat rate
- I was gonna reiterate when we talk about equity and equitable practices. You can opt out (of the automated system) but there is a fee. And it makes me think how much of It is a choose if one of these you have to pay for and the other one is free. So that sounds a little problematic when looking at choices of equity. I think choices are great, but also people need to be well informed. Like people within the community need to have more clear information to make the best decision for themselves
- Going back to people who make the decision. I want the person who are living in the house to know what decision is being made. So not just the person who owns the house, but the person living in the home. And not everyone it literate and not everyone speaks English. And its really important that you are giving them information they can actually consume. Instead of giving them notices they cant read

Council on Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington
Thursday, Feb. 21, 2019
Technology Discussed: Acyclica

1. Do you have concerns about this specific technology or how it's used?
    - Where does this data go? Does it go to SDOT? Google maps?
    - My other question is, it said whatever is being transferred is encrypted. All encrypted means to me is getting data from one device to another will be transferred without it being intercepted. What I don't know is, how much information are people getting
    - My concern is related to data, yeah we like to use gps. But what is the perimeter, what is the breach of access. Where is the data being used, and what can that turn into. we might be okay if the data is only being used for traffic related updates, but they might use it for more
    - I also would like to see how acyclica actually does what they do. They are using a lot of words that normally don't know. So I want to know how exactly they are hashing and salting. So for them to be clear about how they doing it. like when whatsapp encrypted they didn't give us the exact code but told us how they are doing it
    - Asking for a greater transparency for how they are doing this
    - I think the purpose of it is really important but the biggest concern is collecting all of this information without consent of passersby.
    - So the specific identifier that acyclica uses it mac addresses? You could potentially use that number to track that phone for the lifetime of the phone, for as long as that phone is on and being used. And that is very concerning.
    - Also I want to understand more where is this data going, and I want to know if this data is going to be used for future projects.
    - I want to ask is this something people opt into
    - People don't even know this is being used

2. What value do you think this brings to our city?
    - I like getting places and I like getting traffic information.
3. What worries you about how this is used?
    - What I don't like is you using my phone to get that information. I want whatever is in my cellphone to be protected. And I wanna know what you can access
    - I think based on Seattle and Seatac's higher up wanting to monitor and map out Muslims and where they are, and I don't like people being able to use our phone to track our location or actions they might think is violent. So based off of Seattle's track record and law enforcement agencies I don't like it
    - People who live outside of Seattle are also being impacted by it anytime they drive in Seattle

- Could someone "opt out" by having wifi disabled on their device? I don't know if this covers cell towers. Because if it covers cell towers the only thing you could is having your phone on airplane mode

4. What recommendations would you give policy makers at the City about this technology?
    - I think the big question is why aren't we using other vendors, like I mentioned google maps, or waze, in fact komo 4 uses ways. Where other options we're looked at, and what were the trade off there's. And I want to see some transparency between the decision-making processes
    - I don't think this data should be shared with other private agencies, or other interagency programs
    - If all you're looking at is traffic flow, why are you not using the sensors in the road to give traffic flow updates.
    -
5. Can you imagine another way to solve the problem this technology solves?
    - I don't know if this already exists but something that makes it that data can't be used from one technology and use it for a different purposes
    - I think speaking from an industry perspective that is really important to have a processes for. Because all of this data is being used regardless of if you live in Seattle, or people live in different countries even who are visiting. That data is being collected. My understanding is that SDOT doesn't get the data directly. So my concern is how long can acyclica keep this data, use this data. Why wasn't a different option used, one in which some sort of consent can be used, so something like waze, google maps where people can opt in can get that information.
    - Road sensors or ways to count cars
    - I think its better to count cars than phones, because there is some expectation that your car will be monitored.
    - Using vehicle level granularity

Entre Hermanos

Please select which technology you wish to comment on:

☐SCL: Binoculars	☐SCL: Sensorlink Transformer Meter (TMS)	☐SFD: Computer-Aided Dispatch	☐SPD:9-11 Call Recorder
☐SCL: Sensorlink Ampstik	☒SDOT: Acyclica	☐SPD: Computer-Aided Dispatch	☐SPD: CopLogic

1) **What concerns, if any, do you have about the use of this technology?**

El uso de wifi en Acyclica porque pueden obtener toda la información de los teléfonos.

Si vale la pena la inversión

Enfocando al grupo: La tecnología ya está instalada. que les preocupa de su uso?

El tráfico sigue igual.

Quien usa o almacena la información.

La preocupación es la colección de data.

Colección y almacenamiento de información es la mayor preocupación.

No es la colección de data lo alarmante sino los recursos (dinero utilizado) ya que o la tecnología no están funcionando porque el tráfico sigue igual. No hay cambio con la nueva tecnología, esos gastos no son válidos ya que no hay resultados. Esos gastos pudieran ser utilizados para la comunidad.

También tienen que ver si la tecnología emite radiación o alguna otra cosa dañina; perjudicial a la salud.

El gobierno tiene todos los datos.

No necesitan esta tecnología para tener los datos porque ya existen métodos para eso, incluso aplicaciones o alguna otra cosa.

La otra preocupación del grupo es que no haya un cambio al problema que se quiere resolver. En el caso de Acrylica sería el mejorar el tráfico.

- Tecnologías como esta necesitan recolectar más opiniones de expertos.
- Sería bueno que la información sea compartida con la comunidad. (Transparencia en fines y objetivos de la tecnología y datos guardados, tácticas implementadas.)

2) What do you want City leadership to consider about the use of this technology?

Hay lugares donde no se necesitan. En algunas partes de Magnolia, Queen Anne, Northgate, no se ocupan.

Seguimiento de pregunta: En las comunidades donde viven los latinos que tanto se ocupa Acyclica?

Participante no cree que allí se ocupan.

Hablaron sobre la necesitad de puntos estratégicos y calles con más necesidad de ayuda por causa del tráfico.

What do you think about this technology in particular ?

Bien, la tecnología ayuda con la velocidad o el movimiento de los coches.

La información se guarda y analizan por donde viajas o cuantas veces cruzas este rastreo.

Si es solo para ver el tráfico está bien.

Está bien en algunas partes. Puede que sea algo bueno. Pero puede que esta tecnología pueda compartir información personal que puede ser utilizada de otra forma en especial si hay Hacking (forma negativa, uso de datos).

La tecnología en sí no es tan grande (de tamaño) para ser algo visualmente desagradable. La información captada a través de estos medios puede que ayude a conducir el tráfico de mejor manera pero también puede que tome información personal.

Are there any questions you have, or areas you would like more clarification? ●

La tecnología no es un router, sino colección de data para planeaciones urbanas.

Participante: “quiero creer” “convencerme” que los sensores están allí para ayudar con el tráfico.

No se sabe cuándo las instalaron, los resultados deberían de ser públicos. Si la tecnología es para aliviar el flujo de tráfico entonces por qué no extienden el programa? O por qué no hay mejoramiento del tráfico?

Alternatives to this technology

- Alguna pantalla que indique cuáles vías son alternativas puede reemplazar esto.
- Cambios al límite de velocidad puede que alivie el flujo del tráfico.
- Dejar de construir tanto.
- Rediseño de calles ayudaría flujo de tráfico.
- El rediseñar las vías servirá para las futuras generaciones.

Entre Hermanos

Please select which technology you wish to comment on:

☒SCL: Binoculars	☒SCL: Sensorlink Transformer Meter (TMS)	☐SFD: Computer-Aided Dispatch	☐SPD:9-11 Call Recorder
☐SCL: Sensorlink Ampstik	☐SDOT: Acyclica	☐SPD: Computer-Aided Dispatch	☐SPD: CopLogic

1) What concerns, if any, do you have about the use of this technology?

Los binoculares son preocupantes si la persona no tiene ética. Es preocupante que una persona vea a través de binoculares a que una tecnología mida el uso de la electricidad

Al grupo le incomoda el uso de binoculares

Sensorlynk específicamente la preocupación sería que le quita el trabajo a una persona.

Si es para detectar robo el grupo cree que hay otras maneras de saber quien roba

que no tan solo será para leer la electricidad sino para obtener otros tipos de información si cámaras fueran usadas

2) What value, if any, do you see in the use of this technology?

Ahorro de energía

Record y datos mas precisos

Oportunidad de trabajo a quien utiliza los binoculares

Estabiliza los precios de la electricidad

3) What do you want City leadership to consider about the use of this technology?

: Usar background check, uso de uniforme por trabajadores, cámara en binoculares.

What do you think about this technology in particular ?

Sensorlink Si

Binoculares son invasivos

Are there any questions you have, or areas you would like more clarification? ●

La confianza en estos medidores serán confiables? Serán efectivos?

El uso de binoculares se puede acompañar de una cámara añadida

Alternatives to this technology

Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad

Please select which technology you wish to comment on:

☐SCL: Binoculars ☐SCL: Sensorlink Transformer Meter (TMS) ☐SFD: Computer-Aided Dispatch ☐SPD:9-11 Call Recorder

☐SCL: Sensorlink Ampstik ☐SDOT: Acyclica ☐SPD: Computer-Aided Dispatch ☒SPD: CopLogic

Entre Hermanos

1) What concerns, if any, do you have about the use of this technology?

Las fallas electrónicas son preocupantes especialmente en reportes policiacos.

Las preocupaciones es que el reporte no salió, no llegó por cualquier razón.

No todos podrán o saben usar las computadoras.

Fallas de los algoritmos de cada demanda es alarmante.

Que y cuando determina la urgencia de respuesta

Las personas le temen a los policías. Y este medio puede ayudar a que el miedo disminuya.

La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

2) What value, if any, do you see in the use of this technology?

La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

El uso de computadora está bien para las denuncias.

Si personas usan esta tecnología y es analizada en tiempo real por otras personas no hay problema.

Es otro método para denunciar

Está de acuerdo con el uso de computadoras para denunciar solo que no todos son capaz de usar este método/tecnología.

3) What do you want City leadership to consider about the use of this technology?
Que sea multi-idioma, implementar audio, implementar sistemas que ayuden a múltiples personas con diversas capacidades/necesidades

Si es usada de manera adecuada y como han dicho está bien.

El uso de la tecnología es bueno para dar respuesta para todas las cosas y personas

What do you think about this technology in particular ?

Grupo están de acuerdo con su uso.

Puede salvar una vida.

Los riesgos y acciones determinan la urgencia de la intermisión policiaca.

Alguna gente se siente más capaz de presentar una queja a través de este sistema, la tecnología en uso tiene validez.

Bueno para la violencia doméstica.

Are there any questions you have, or areas you would like more clarification?

La computadora decidirá la importancia/urgencia del reporte/emergencia dando a llevar acciones de emergencia.

Gravedad de emergencia es determina por tecnología.

La definición de emergencia es diferente con cada persona.

Cada uno tiene la definición de vigilancia, pero ¿que tal la definición de emergencia?

SITUATIONS TO APPLY ITS USE

Una pelea en la calle, un malestar corporal, cuestiones de vida, abuso doméstico

Si nos basamos en la definición de emergencia sólo en cuanto estemos en peligro inmediato o en tiempos mínimos/ de transcurrencia alarmante/peligrosa el uso de será implementado o limitado solo a instantes inmediatos de peligro.

Para reportar algo que ya sucedió o que son recurrentes.

Basado en el concepto de emergencia, las personas pueden tomar el método adecuado para reportar su caso y a través del medio necesario.

Los reportes no son anónimos.

Los datos son recolectados aun, a pesar de la opción escogida.

Alternatives to this technology

Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad

Entre Hermanos

City of Seattle
Surveillance

Inicio

Resumen: El departamento de vecindarios quiere saber la opinión de este grupo. Ellos verán videos de un minuto y medio y encontrarán folletos en sus mesas donde encontraran más información sobre lo visto.

Demográficos:

Ocho personas participaron, una de West Seattle, una de First Hill, dos de Ravenna/Laurelhurst y cuatro de King County (outside Seattle).

Cuatro personas se consideraron hispano o latino, una como india americana o nativa de Alaska, y tres no opinaron.

Cinco personas marcaron 18-44 como su rango de edad, dos marcaron 45-64 como el suyo y una no opinó.

Cinco personas marcaron masculino como género, una como transgénero, una como femenino, y otra no opinó.

Otra Información Importante:

- Preguntas serán hechas.
- Habrá una hoja para poder conversar sobre videos de interés
- Se les agradeció por venir.
- El concepto de vigilancia será manejado como la ciudad de Seattle lo maneja.
- Tom: Agradeció a los invitados por venir

Surveillance. In 2017 city council passed an ordinance to see what technology fit the definition of surveillance. The information gathered by these surveillance technologies are as follows: to “observe or analyze the movements, behaviors, or actions of identifiable individuals in a manner” which "is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice.”

Presentador: Preguntó si la conversación en inglés fue entendida.

Grupo: Concordó.

Tom: Do not let information on videos stop you from making comments or raising questions.

Presentador: Dio a entender el concepto de vigilancia como ha sido interpretada por la ciudad de Seattle. Fue analizada de esta manera: "La vigilancia es definida como tecnologías que observan o analizan los movimientos, comportamientos, o acciones de individuales identificables de una manera que razonablemente levanta inquietudes sobre libertades civiles, la libertad de expresión o asociación, igualdad racial o justicia social."

- Los movimientos de la gente son observados a través de esta tecnología y puede que para algunas personas esto sea incómodo.
- Las cámaras de policía no califican como tecnologías de vigilancia en este tema.
- La presentación mostrada en la pantalla a través de los videos será transmitida en inglés.
- Se pidió que todos se traten con respeto y que opinen y que su nombre sea mencionado e incluso la vecindad donde viven.

El Grupo

Participante vino porque quiere obtener más información y dar su opinión. Es de Seattle.

Participante viene de Shoreline/Seattle para ver cuánto la tecnología entra afecta

Participante vino porque quiere saber qué información es colectada por el gobierno y para qué usan esa información. Puede que la información obtenida a través de la tecnología sea usada para perseguir a personas de color/minorías/personas marginadas.

Participante vino de First Hill, porque quiere ver el punto de vista de la ciudad y ver que opiniones surgirán.

Participante viene de Seatac porque tiene interés en el tema y porque la seguridad es importante y quiere saber a dónde llega la información.

Participante vine en Ravenna/Northgate, quiere ver que tan confiable es la tecnología y para qué es utilizada. Perjudicial o beneficial?

Participante vine en Seatac y vino porque es un tema muy interesante ya que se tiene que saber/mantener informado de lo que hacen los gobernantes.

Participante vino de Burien por la importancia del tema y la privacidad.

Presentador: La tecnología no es nueva. Ya está siendo usada. Y quieren saber el formato para que las futuras tecnologías tengan.

El video de Seattle Department of Transportation de Acyclica fue mostrado

Esta tecnología es un sensor que detecta el wifi. Es un sensor que detecta la tecnología wifi.

Seattle Metering Tool fue mostrada

Nadie del grupo sabe del tema más el presentador no hablará a fondo de esto para no influenciar opiniones.

Video de Fire Department's Computer Aided Dispatch fue mostrado

El 9-1-1 logging recorder video fue mostrado

Aclaración: Información impresa fue entregada explicando cada una de las tecnologías.

Video de Coplogic fue mostrado

El grupo no conocía que se puede reportar a la policía a través de su página/en línea.

El video de Seattle Police Computer Aided Dispatch fue mostrado

Esta tecnología es similar a la de los bomberos.

Se preguntó cuál video era de interés para analizar

Se acordó el análisis de Acyclica, Binoculares/Sensorlink, y Coplogic

Las Preguntas que sea harán serán las siguientes:

¿Qué piensan de este sistema de tecnología en específico y el motivo de usarla?
¿Cuál creen que sea el aporte de esta tecnología a la cuidad?
¿Qué preocupación les causa el uso que se le dará a este sistema?
¿Qué recomendarían a el grupo de políticos de la cuidad responsables de tomar las decisiones de implementar estas tecnologías?
¿Qué otra manera habría de resolver el problema que esta tecnología esta designada a resolver?

La Acyclica

Pregunta: ¿Qué piensan de este sistema de tecnología en específico y el motivo de usarla? (Como se usa y cuál es el uso)

- Bien, la tecnología ayuda con la velocidad o el movimiento de los coches.
- La información se guarda y analizan por donde viajas o cuantas veces cruzas este rastreo.
- Si es solo para ver el tráfico está bien.
- Está bien en algunas partes. Puede que sea algo bueno. Pero puede que esta tecnología pueda compartir información personal que puede ser utilizada de otra forma en especial si hay Hacking (forma negativa, uso de datos).
- La tecnología en sí no es tan grande (de tamaño) para ser algo visualmente desagradable. La información captada a través de estos medios puede que ayude a conducir el tráfico de mejor manera pero también puede que tome información personal.

Pregunta: Qué es lo que aporta esta tecnología a la ciudad?

- Seria algo bueno el aporte por la agilidad del tráfico solo si la tecnología está sincronizada con los semáforos, de otra manera no es útil si no aporta para el mejoramiento del tráfico.
- Participante dice que hay alternativas para esquivar el tráfico.
- Participante opina que la tecnología es interesante ya que usa google maps y está de acuerdo con el mejoramiento del tráfico.
- Si el objetivo es de mejorar el tráfico está de acuerdo. Pero también quiere saber en qué lugar(es) estarán los aparatos, si algunas personas serán beneficiadas más que otras.

Pregunta: Qué preocupaciones tienen con posible uso/uso potencial de esta tecnología?

- Le preocupa el uso de wifi en Acyclica porque pueden obtener toda la información de los teléfonos.
- Si el potencial puede ser aplicada a la inversión.

Enfocando al grupo: La tecnología ya está instalada, que les preocupa de su uso?

- El tráfico sigue igual.

- Quien usa o almacena la información.

- La preocupación es la colección de data.

Más de la mitad de grupo opina que esa (el almacén y colección de información) es la preocupación.

- Participante no está de acuerdo. No es la colección de data lo alarmante sino los recursos (dinero utilizado) ya que o la tecnología no están funcionando porque el tráfico sigue igual. No hay cambio con la nueva tecnología, esos gastos no son válidos ya que no hay resultados. Esos gastos pudieran ser utilizados para la comunidad.

- También tienen que ver si la tecnología emite radiación o alguna otra cosa dañina; perjudicial a la salud.

- El gobierno tiene todos los datos.

- Opinión de otro participante: No necesitan esta tecnología para tener los datos porque ya existen métodos para eso, incluso aplicaciones o alguna otra cosa.

La otra preocupación del grupo es que no haya un cambio al problema que se quiere resolver. En el caso de Acrylica sería el mejorar el tráfico.

- Tecnologías como esta necesitan recolectar más opiniones de expertos.

- Sería bueno que la información sea compartida con la comunidad. (Transparencia en fines y objetivos de la tecnología y datos guardados, tácticas implementadas.)

Pregunta: Le dirían algo a los políticos algo del lugar donde se encuentran estos aparatos?

- Hay lugares donde no se necesitan. En algunas partes de Magnolia, Queen Anne, Northgate, no se ocupan.

Seguimiento de pregunta: En las comunidades donde viven los latinos que tanto se ocupa Acyclica?

- Participante no cree que allí se ocupan.

Hablaron sobre la necesitad de puntos estratégicos y calles con más necesidad de ayuda por causa del tráfico.

Presentrador: Crees que Acylica es como el router de google?

- La tecnología no es un router, sino colección de data para planeaciones urbanas.

- Participante: “quiero creer” “convencerme” que los sensores están allí para ayudar con el tráfico.

- No se sabe cuándo las instalaron, los resultados deberían de ser públicos. Si la tecnología es para aliviar el flujo de tráfico entonces por qué no extienden el programa? O por qué no hay mejoramiento del tráfico?

Otra pregunta: Alguna otra tecnología que pueda ser utilizada en vez de Acyclica?

Alternativas:

- Alguna pantalla que indique cuáles vías son alternativas puede reemplazar esto.
- Cambios al límite de velocidad puede que alivie el flujo del tráfico.
- Dejar de construir tanto.
- Rediseño de calles ayudaría flujo de tráfico.
- El rediseñar las vías servirá para las futuras generaciones.

Tecnologia #2

Sensorlink/Binoculares

Pregunta: Que opina el grupo de la tecnología?

- Los binoculares son preocupantes si la persona no tiene ética. Es preocupante que una persona vea a través de binoculares a que una tecnología mida el uso de la electricidad.

- Un sensor que detecta la electricidad sería mejor.

- Al grupo le incomoda el uso de binoculares.

Pregunta: Qué opinas sobre la tecnología medidora de electricidad (sensorlink) y que sea usada en tu casa?

- No le incomoda o afecta a dos participantes.

- La preocupación sería que le quita el trabajo a una persona.
- Los binoculares son invasivos.
- Para que usar binoculares si es que se puede llegar a el hogar y ver el medidor en persona, pidiendo permiso? Si la tecnología es usa para ver que las personas se roban la electricidad, creen que no saben quiénes roban?
- El grupo cree que si saben.

Pregunta: Cual creen que sea el aporte que esta tecnología?

- El video dice que 3 millones de dólares son ahorrados.

Pregunta: De qué manera beneficia esto a la cuidad/ciudadanos/comunidad?

- El robo de la luz es preocupante.
- Si ya llevan el record y datos y le hacen saber a la comunidad puede que ahorren dinero.
- Uso de binoculares puede dar trabajo a una persona y dinero puede ser ahorrado con esta tecnología.
- La tecnología trae gasto de electricidad para poder ver gastos de luz? Si pretende evitar el robo entonces los gastos de la factura eléctrica deberían de seguir estables.

Pregunta: La confianza en estos medidores serán confiables? Serán efectivos?

- Ayuda a la precisión, a bajar precios.
- Que quiten los binoculares sería una sugerencia, o usar binoculares que graban con video.
- Si ya tienen récord sobre la energía (consumo, gastos, etc.), el robo de energía no es suficiente para establecer este tipo de tecnología ya que puede ser identificado el robo o alguna otra anomalía dependiendo en el nivel alto o bajo o repentino analizado/visto/detectado por métodos convencionales ya establecidos.
- Otra recomendación: Usar background check, uso de uniforme por trabajadores, cámara en binoculares.

- Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad

- .La preocupación es que no tan solo será para leer la electricidad sino para obtener otros tipos de información si cámaras fueran usadas.

Tecnologia #3 Coplogic

- Esta tecnología no solo el ahorro de tiempo, sino el ahorro de tiempo policial ya que ellos trabajarían en otras cosas

- El uso de computadora está bien para las denuncias.

- Si personas usan esta tecnología y es analizada en tiempo real por otras personas no hay problema.

Enfoque: Lo que estamos queriendo dialogar es el uso del internet y las denuncias.

- Es otro método para denunciar

- Está de acuerdo con el uso de computadoras para denunciar solo que no todos son capaz de usar este método/tecnología.

Pregunta: En que ayuda a la comunidad?

- Por qué usar estos métodos?

- Grupo están de acuerdo con su uso.

- Puede salvar una vida.

- Los riesgos y acciones determinan la urgencia de la intermisión policiaca.

- Alguna gente se siente más capaz de acudir a través de este sistema la tecnología en uso tiene validez.

- Bueno para la violencia doméstica.

- Las fallas electrónicas son preocupantes especialmente en reportes policiacos.

- Las preocupaciones es que el reporte no salió, no llegó por cualquier razón.

- No todos podrán o saben usar las computadoras.

- Fallas de los algoritmos o cuando o que promueve urgencia de cada demanda es alarmante.

- Criterio de demandas y que clase de preocupación de parámetros son confiables tienen que ser cuestionados/analizados, y que/quien es digno de prioridad o importancia o de ayuda.

Pregunta: De qué manera este uso beneficiaria a la comunidad?

- Personas pueden ser discriminadas

- Las personas le temen a los policías. Y este medio puede ayudar a que el miedo disminuya.

- La computadora decidirá la importancia/urgencia del reporte/emergencia dando a llevar acciones de emergencia.

- Gravedad de emergencia determina uso de tecnología.

Pregunta: Alguna inquietud sobre el uso de esta tecnología?

- La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

Pregunta: En qué situación usarán esta tecnología?

- Una pelea en la calle, un malestar corporal, cuestiones de vida, abuso doméstico
- Cada uno tiene la definición de vigilancia, pero que tal la definición de emergencia?
- La definición de emergencia es diferente con cada persona.
- Si nos basamos en la definición de emergencia sólo en cuanto estemos en peligro inmediato o en tiempos mínimos/ de transcurrencia alarmante/peligrosa el uso de será implementado o limitado solo a instantes inmediatos de peligro

Pregunta: Para qué sirve el reporte de la computadora?

- Para reportar algo que ya sucedió o que son recurrentes.
- Basado en el concepto de emergencia, las personas pueden tomar el método adecuado para reportar su caso y a través del medio necesario.

- Los reportes no son anónimos.
- Los datos son recolectados aun, a pesar de la opción escogida.

Pregunta: Qué les recomendarían a los políticos?

- Que sea multi-idioma, implementar audio, implementar sistemas que ayuden a múltiples personas con diversas capacidades/necesidades

Pregunta: Algún otro comentario en general sobre la tecnología de vigilancia?

- Si es usada de manera adecuada y como han dicho está bien.

- El uso de la tecnología es bueno para dar respuesta para todas las cosas y personas.

Consejo:

- Den información más información sobre lo que están haciendo. (transparencia/divulgación de información)

- Que haya más transparencia.

Ser transparentes sobre la colección de datos, para que haya discusiones y decisiones Informadas, en todas las tecnologías implementadas/por implementar.

Byrd Barr Place

2/28/2019 Surveillance Technology Focus Group

Thursday, February 28, 2019
1:42 PM

Disclaimer: some of these notes are written in first-person. These should not be considered direct quotes

Videos:

- Acyclica: sensors recognize when a wifi enabled device is in range of it. Attached to street lights
- 911 recorder: records the conversation with the person calling 911, and conversation with the dispatched officers
- CopLogic: Online police report, treated as a regular policy report
- Computer Aided Dispatch
- Seattle City Light: Binoculars for meter readers; sensor to see if someone is stealing electricity

Tom: Read definition of surveillance

Craig: invasion of privacy?

- Electric one: I never even know they had the sensor one.

Community Member: used to be in the tech industry for thirty years. Writing a book about surveillance and technology
Wanda: I like the online police report. If someone is experiencing a crisis or trauma, you can go ahead and report it.

- Surveillance, I understand the concern, but overall I think it's a good thing. There is good and bad in any location, you'll find people who are taking advantage of it, but hopefully there are systems in place.
- Used to work nights, and catching the bus at night is scary. Having the cameras and police out when catching the bus helps, I appreciate that. No one likes to be watched, but if it's gonna keep people safe, that's a good thing.

Mercy: security is a great safety issue
Craig: there are some parts of the neighborhood/city that need to be watched, and some that need to be left alone
Wanda: as long as it's even
Craig: Sometimes it's not even
Both: There are hot spots though

Which of the surveillance technologies do you think could be abused to pinpoint specific communities?

IG: The Computer Aided Dispatch

Talking about the International District:

- Lots of businesses and residential crammed together in a larger space
- Talking about a great community member who died; if they had surveillance technology them, maybe they would have found his killer

"Some neighborhoods need to be watched"

- Gangs; drug use

Tom: getting back to CAD, how do we feel about the information that is stored

- Craig: there are concerns, but who is allowed to see it, how is it stored? That's a concern
    - Is it used for BOLOs? Is it everyone who is in the area, all of the police officers? Or is there some discretion as to which police officers would be given the information?
- Wanda: plenty of people are arrested who "fit a description"
    - Discussion about the racial discrimination: how people who think that "all [insert race here] look alike".
    - Individuals may think like that, but police officers have the capability to ruin someone's life.
- Marjorie: just recently got a smart phone, and it's new to me that someone could know where I'm going and I wouldn't be aware of it

    - Without my consent.
- Mercy: grew up with the idea that big brother is watching you
    - Tracking how many times I go to the library seems like a waste of money
    - People who are not law abiding citizens, they are the ones to be worried
- Craig: What about selling weed, coke, etc. Should they be worried?
    - Mercy: well at least in Seattle, it's ok to sell
- Mercy: big brother is watching. We already know that, it's just more obvious now
- There is a lot of technology that we are not made aware of

Tom: So acyclica, is it worth it? Some people worried it's tracking, is it something that we can live without?

- Should we put up signs that this road is tracked?
    - Viron: Maybe
    - Mercy: let people out there know that you're on camera.
    - Viron: does it work if your device is not turned on?

Tom: what do you want to tell the city council about tech that is collecting personal information?

- Wanda: they should get our individual consent
- Martha: putting it on the ballot doesn't mean that you are getting individual consent, because if you vote no but it still passes, you didn't give your consent
- Deana: there are some places around Capitol Hill that I don't feel safe at at night
    - Talking about fire department responding to a fire in her building: when one building alarm system goes off, it goes directly to the fire department - affects multiple buildings.
        - Response time is very good.
    - I choose to turn off the GPS tracking, because I don't need people to know where I'm at
        - If others are watching where I'm at, that's an invasion of privacy. I should be able to walk out my front door and go wherever I want without anyone knowing.
- Location privacy: you can tell a lot about a person based on where they go, and tracking that can build a pretty extensive profile of who you are
- IG: now that I know they are tracking, I will turn it off.

Mr. Surveillance: Surveillance is always secret, and it's an aggressive act. It's meant to exert power over others.

Do you think any individual could raise enough concern that it would change anything?

- Resounding no
- Maybe with a larger group
    - Maybe with the whole city

SCL binoculars:

- Craig: they should warn their customers and let them know they are coming into their yard/looking through binoculars.
- Wanda: as long as they aren't looking in people's windows.
    - When we're walking down the street, it's a little different. Certain neighborhoods do need more surveillance than others

Regarding being watched in public:

- Eydie: in public, it depends on how long. If it's a short period of time, that's one thing, but if you're tracked the whole time you're out, it's unreasonable.
    - I don't know what the solutions would be.
    - Even when the meter read just walks into your yard, it's unnerving.
    - What's the purpose of tracking it this way?
- Mercy: (referring to the acyclica) Why are they doing it all the time? Have they not gotten the information yet?
    - They should already know what the traffic flow would be.
    - We lost a lane to the bicyclist
- Craig: facial recognition used on the street is bad.
- Vyron: sometimes you can't walk down the street and shake someone's hand without getting in trouble
- Mr. Surveillance: The technology has gotten ahead of the law, and it means they have to pay less people

Tom: Are we willing to accept more technology to have less police?

- Craig: how about just making it even? Police have an image to people of color; they are afraid of why they are going to be there. We can police ourselves
- Wanda: I disagree. There are some who think there should be less, but there are also a lot of people who worry about walking down the street
    - As a woman and DV survivor, I appreciate the police and appreciate living in a country where I can call a number for help.
    - I have a big problem with the shooting of unarmed black men, but as an individual I still appreciate the police.
    - But I have a problem being tracked, and I have a problem being watched in my home.
- General comment: The number of police being on the corner is a touchy situation
    - Knowing the police that are on your corner makes a difference. They can police the community better if there is more of a relationship between the two.
- Craig: it has to be both, even. You can't trade off the technology for the police.
- Mr. Surveillance: The trend is they want to go to more technology and less police.

Tom: If right now we have lots of technology, and we want a balance, then how do we do that?

- Craig: keep it the way it is but clean up the police department. Make sure the people who are working there are good at their jobs, not biased or discriminating

CopLogic: making police reports online

- Craig: I think it's stupid.
  - Would use that technology for stupid crimes
- Mercy: you could report your neighbor for silly things
  - Anonymous reporting of crimes that could target people for things they might not call 911 for
- Wanda: there were some lines of traffic where I saw cars lined up with their windows smashed in; nothing taken, but glass all over the place.
  - Police response when called: maybe you should get a cheaper type of car
  - Would he have said that to us if we were a different skin color, or lived in a different neighborhood?
- IG: I think it's a bad thing: someone could make up a story and the officer didn't have to check it.
- Marjorie: I think the online reporting could be abused

Appendix E: All Comments Received from Members of the Public

ID: 10617628638
Submitted Through: Survey Monkey
Date: 3/25/2019 1:05:41 PM
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SFD: Computer-Aided Dispatch (CAD)
What concerns, if any, do you have about the use of this technology?
Highest Concerns: 1) Page 12 item 5.4 of the SIR says "Data is retained for the life of the system." That data would include general personal information (names, addresses, phone numbers, building access codes, etc) and personal medical information. Why does this data need to be retained indefinitely? Does all of the data need to be retained that long or does only certain "metadata" (such as CAD event ID, type of medical incident, etc) have a "business need" to be kept that long? Should there be a lifetime imposed on this data? 2a) The draft SIR doesn't include a contract between SFD and AMR. Is there a contract between SFD and AMR? 2b) If so, does that contract specify any data handling and/or data retention requirements that AMR needs to follow? 3) The diagrams embedded in the draft SIR on pages 182 and 183 don't include University of Washington's Harborview Medical Center (UW HMC), which the SIR mentions that SFD does share data with. The mechanism of that data sharing is unclear though. 3a) How does UW HMC access the SFD CAD data? Do they have direct access to the SFD CAD; or are they periodically given a download of certain CAD data by SFD manually (though likely digitally)? 3b) Does UW HMC have recurring access to the data (perhaps say weekly/monthly updates of the data from SFD); or was the date sharing one-time only? 3c) Is the data made available to UW HMC as part of the PRA process or is there another process being used? If it's not via PRA request, then is there a contract between SFD and UW HMC? 3d) Is there any redaction happening to the data before it is provided to UW HMC (perhaps the same level of redaction as would occur for PRA disclosures)? 4) The diagram on page 183 shows an SFD-owned reporting server that has a database replication of the TriTech server CAD data. That reporting server then connects to "SFDINTSPD" which in turn connects to "SPD CAD (Versaterm) & COPS Application". From the discussion at the SIR tech fair, I was under the impression that SPD's access to SFD CAD data was on an as-needed basis and reviewed by SFD before being supplied to SPD, but network lines in the diagram would imply to me that the SPD access is actually continuous/constant. Is that correct? Does SPD have full access to the data in the SFD CAD? If not, what supposedly limits that scope? 5) The diagram on page 183 lists FirstWatch as one of the cloud vendors that receives data from the SFD CAD, but the draft SIR doesn't mention "FirstWatch". 5a) What type of data is being provided to FirstWatch? 5b) If the data provided to FirstWatch is beyond what is provided publicly (such as via "Realtime 911"), then is there a contract between SFD and FirstWatch? 5c) Does said contract also specifically define requirements for the handling/storage/security/privacy of non-public SFD CAD data? Medium Concerns: 1) Domestic violence victims may have their personal information (address, phone number, etc) exposed to their abuser via SFD PRA disclosure, even if they have a restraining order against the abuser, since SFD doesn't have a built in mechanism for knowing that a restraining order is in play when processing a PRA request (and the PRA law itself doesn't explicitly contain such an exemption for SFD either - so the PRA law should be improved). 2) Page 16 item 7.3 says "Changes to program ownership and participation can result in a large number of administrators within SFD who have access to

the CAD system." That statement points to SFD/IT likely having difficulty in managing Active Directory and Group Policy Objects, which has a direct impact on the security and privacy of the data in the SFD CAD. This would be considered a common skill for a Windows administrator to have mastered, so this type of problem should not be cropping up with SFD's CAD access controls. 3) The TriTech CAD pdf linked off of page 5 item 2.2, lists the feature "Media Log allows automatic redaction of Sensitive information". However, the SFD rep at the SIR tech fair didn't know what exactly would be detected and redacted in the logs. 4) It is unclear if or how SFD uses/is integrated with "Alert Seattle"/"Seattle 911" for the receiving of personal details (potentially medical in nature) pre-provided by citizens in an effort to help first responders should they have a medical emergency. 5) The ESO subscription agreement on page 153 sub-item 8..b.ii., requires that SFD not "allow any third party to use the Software", which presumably means that SFD/IT could never enter into a contract with an external security company to conduct a penetration test (aka a pen test). Pen tests are used to detect security vulnerabilities in software (in a controlled manner). This agreement would appear to me (not a lawyer) to hinder SFD's ability to find such security vulnerabilities (or even confirm that certain vulnerabilities were NOT present thus confirming more confidently that the system is secure). That being said, I don't know if SFD/IT has the budget to normally be conducting pen tests, even for high risk/concern applications (such as those that handle medical info). 6) It is unclear SFD has final control over the decision-assistance technology embedded in the TriTech CAD. Specifically, page 8 item 4.1 mentions that there is a CAD plug-in for the decision tree protocol. Is that SFD-defined or TriTech proprietary? Lesser Concerns: 1) Received clarification from the SFD rep at the SIR tech fair that the Automatic Location Identification (ALI) is only available for landlines and SFD gets mobile callers' locations by asking them. 2) No 2-step-verification/2-factor-authentication (2SV/2FA) for login to TriTech vCAD; however, an individual would need to first logon to an SFD workstation and then login to the CAD. 3) The draft SIR did not specify what (if any) other vendors SFD/IT considered before deploying TriTech's CAD software. Is this the optimal CAD solution for the City of Seattle? Is there perhaps another CAD software provider that is more competitive and perhaps has better security/privacy/audit features? 4) The diagram on page 183 of the draft SIR includes a legend that certain servers in the diagram would be "Located At NGDC", but "NGDC" is not defined in the SIR. My assumption is that "DC" stands for DataCenter, but I don't know what "NG" stands for (maybe "NextGen"?); and that the NGDC is likely located on-premise to some part of City of Seattle (though unknown if that is a SFD-specific location or if "NGDC" is shared by multiple city agencies). This is just my speculation though.

What value, if any, do you see in the use of this technology?

It helps facilitate a speedy response appropriate to the type of CAD event, thus hopefully helping save lives and homes.

What do you want City leadership to consider about the use of this technology?

1) Data retention is an issue. Why does this data need to be retained indefinitely? Does all of the data need to be retained that long or does only certain "metadata" (such as CAD event ID, type of medical incident, etc) have a "business need" to be kept that long? Should there be a lifetime imposed on this data? 2) Potential lack of a contract between SFD/IT and AMR. Is there a contract between SFD and AMR If so, does that contract specify any data handling and/or data retention requirements that AMR needs o follow? 3) Data sharing with University of Washington's Harborview Medical Center (UW HMC). How does UW HMC access the SFD CAD data? Do they have direct access to the SFD CAD; or are they periodically given a download of certain CAD data by SFD manually (though likely digitally)? Does UW HMC have recurring access to the data (perhaps say weekly/monthly updates of the data from SFD); or was the date sharing one-time only? Is the data made available to UW HMC as part of the PRA process or is there another process being used? If it's not via PRA request, then is there a contract between SFD and

UW HMC? Is there any redaction happening to the data before it is provided to UW HMC (perhaps the same level of redaction as would occur for PRA disclosures)? 4) Data sharing with SPD. From the discussion at the SIR tech fair, I was under the impression that SPD's access to SFD CAD data was on an as-needed basis and reviewed by SFD before being supplied to SPD, but network lines in the diagram would imply to me that the SPD access is actually continuous/constant. Is that correct? Does SPD have full access to the data in the SFD CAD? If not, what supposedly limits that scope? 5) Is there a contract between SFD/IT and FirsWatch? What data is being provided Firstwatch (only public data or more)? 6) There is a gap in the PRA law regarding the protecting the safety/privacy of domestic violence victims. Domestic violence victims may have their personal information (address, phone number, etc) exposed to their abuser via SFD PRA disclosure, even if they have a restraining order against the abuser, since SFD doesn't have a built in mechanism for knowing that a restraining order is in play when processing a PRA request (and the PRA law itself doesn't explicitly contain such an exemption for SFD either). Amending the PRA law to include required exemptions from disclosure of personal information of people with active restraining orders. 7) City leadership should specifically inquire as to the results of SFD's analysis of potential racial bias in their medical services (that analysis is based partially on CAD data).

Do you have any other comments?

1) I was pleased to hear (via the SFD rep at the SIR tech fair) that SFD is working on improving the data they gather for medic events, so that they can then assess if there is a racial bias in their 911 patient care. (However this analysis is only going to be possible for medical events, not fire events, since they don't have the same such data for fire events to conduct such an analysis.) 2) The SIR notes that the SFD CAD is integrated with PulsePoint; however not very much information is provided about PulsePoint in the SIR itself. Searching around online, I was able to address my top questions/concerns about the use of the technology by reading the online materials about Pulse Point from fire departments outside of Seattle (such as this: http://www.siouxfalls.org/fire/professional-standards/pulse-point). Searching the Seattle website, it doesn't even mention PulsePoint. Why has SFD seemingly done nothing to market the existence of this technology (such as https://www.pulsepoint.org/resources/#outreach)? Why isn't this on the SFD website? Why (seemingly) haven't local medical groups been contacted to be informed and tell their medical provider employees about this technology so that they may chose to opt-in to volunteering in a crisis? (I brought Pulsepoint up with a friend who is a local medical provider and they had never heard of this before either.)

Are there any questions you have, or areas you would like clarification?

The diagram on page 183 happens to show two types of servers labeled with the NICE logo (one set is called "NRX Loggers 1 & 2" and the other is "SFDNICEINFORM2 (GUI Front End to Loggers)"), which would be the same vendor software SPD uses for 911 call logging. It is unclear from the diagram alone which calls SFD is logging. If it includes calls with the public, then wouldn't that be in scope just like SPD's usage of the same software? (I didn't see SFD call logging listed in the planned technologies for Group 3 or 4 – my understanding is that the next two groups are SPD-only.)

ID: 3
Submitted Through: Focus Group
Date: 2/27/2019
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars, SCL: CheckMeter, SCL: AmpFork, SFD: CAD, SPD: CAD, SPD: 911 Logging Recorder
What concerns, if any, do you have about the use of this technology?
That would be good with advanced technology
What value, if any, do you see in the use of this technology?
Yes, around the city.
What do you want City leadership to consider about the use of this technology?
Need good train to people who use new technologies
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

ID: 10550721152
Submitted Through: Survey Monkey
Date: 2/23/2019 12:21:02 PM
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SFD: CAD
What concerns, if any, do you have about the use of this technology?
It was mentioned civilians could possibly have access to this. Problem here will be one of discrimination towards people the officers or the city may feel do not require access. In these standards there isn't any language that guides or gives officers or the city to whom is eligible to see the information in CAD. We need transparency from our public appointed officials especially when it deals with information.
What value, if any, do you see in the use of this technology?
It's important for officers to have real-time data. We need a simple transparent process that everyone can look up and know what they rightfully can do. It's unfair to say civilians can see what's in CAD but not identify whom those civilians are. It could be so that the city can withhold information from one case or group of people as a norm and allow another group of people or cases to be able to have access to what's in CAD
What do you want City leadership to consider about the use of this technology?
Create a guide in which every single person is held to a standard and have the same rights to access information especially when regarding the law
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

Appendix F: Department Responses to Public Inquiries

No public inquiries were received regarding this technology.

Appendix G: Letters from Organizations or Commissions

City of Seattle

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

March 12th, 2019

Seattle City Council
600 4th Ave
Seattle, WA 98104

Re: Surveillance Ordinance Group 2 Public Comment

We would like to first thank City Council for passing one of the strongest surveillance technology policies in the country, and thank Seattle IT for facilitating this public review process.

These public comments were prepared by volunteers from the Community Technology Advisory Board (CTAB) Privacy & Cybersecurity Committee, as part of the surveillance technology review defined in Ordinance 125376. These volunteers range from published authors, to members of the Seattle Privacy Coalition, to industry experts with decades of experience in the information security and privacy sectors.

We reviewed and discussed the Group 2 Surveillance Impact Reports (SIRs) with a specific emphasis on privacy policy, access control, and data retention. Some recurring themes emerged, however, that we believe will benefit the City as a whole, independent of any specific technology:

- **Interdepartmental sharing of privacy best practices**: When we share what we've learned with each other, the overall health of the privacy ecosystem goes up.
- **Regular external security audits**: Coordinated by ITD (Seattle IT), routine third-party security audits are invaluable for both hosted-service vendors and on-premises systems.
- **Mergers and acquisitions**: These large, sometimes billion-dollar ownership changes introduce uncertainty. Any time a vendor, especially one with a hosted service, changes ownership, a thorough review of any privacy policy or contractual changes should be reviewed.
- **Remaining a Welcoming City**: As part of the Welcoming Cities Resolution, no department should comply with a request for information from Immigration and Customs Enforcement (ICE) without a criminal warrant. In addition, the privacy of all citizens should be protected equally and without consideration of their immigration status.

Sincerely,

Privacy & Cybersecurity Committee volunteers
Torgie Madison, Co-Chair
Smriti Chandashekar, Co-Chair
Camille Malonzo
Sean McLellan
Kevin Orme
Chris Prosser
Rabecca Rocha
Adam Shostack
T.J. Telan

Community Technology Advisory Board
Steven Maheshwary, CTAB Chair
Charlotte Lunday, CTAB Co-Vice Chair
Torgie Madison, CTAB Co-Vice Chair
Smriti Chandashekar, CTAB Member
Mark DeLoura, CTAB Member
John Krull, CTAB Member
Karia Wong, CTAB Member

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SFD: Computer-Aided Dispatch (CAD)

Comments

The use of a centralized Computer-Aided Dispatch (CAD) system is essential to protecting the health and safety for all Seattle citizens. The National Fire Protection Association (NFPA) standards outline specific alarm answering, turnout, and arrival times[1] that could only be accomplished in a city of this size with a CAD system.

In addition, with over 96,000 SFD responses per year (2017)[2], only a computerized system could meet the state's response reporting guidelines established in RCW 35A.92.030[3].

CentralSquare provides the dispatch service used by SFD. CentralSquare is a new entity resulting from the merger of Superion, TriTech, Zuercher, and Aptean[4] in September 2018.

Recommendations

- Tritech, the underlying technology supplying SFD with CAD services, has been in use since 2003 [SIR 4.3], making it 16 years old. As with any technology, advancements in security, speed, usefulness, and reliability come swiftly. Due to the age of the technology, we recommend conducting a survey into the plausibility of replacing Tritech as SFD's CAD solution.

- Tritech was merged very recently into CentralSquare in one of the largest-ever government technology mergers to date. Due diligence should be exercised to ensure that this vendor is keeping up to date with industry best practices for security and data protection, and that their privacy policies are still satisfactory after the CentralSquare merger. We recommend ensuring that the original contracts and privacy policies have remained unchanged as a result of this merger.

---

[1] "NFPA Standard 1710." https://services.prod.iaff.org/ContentFile/Get/30541
[2] "2017 annual report - Seattle.gov." https://www.seattle.gov/Documents/Departments/Fire/FINAL%20Annual%20Report_2017.pdf
[3] "RCW 35A.92.030: Policy statement—Service ... - Access WA.gov." https://app.leg.wa.gov/rcw/default.aspx?cite=35A.92.030
[4] "Superion, TriTech, Zuercher, and Aptean's Public Sector Business to " 5 Sep. 2018, https://www.tritech.com/news/superion-tritech-zuercher-and-apteans-public-sector-business-to-form-centra

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SDOT: Acyclica

Comments

Traffic congestion is an increasingly major issue for our city. Seattle is the fastest-growing major city in the US this decade, at 18.7% growth, or 114,00 new residents[5]. Seattle ranks sixth in the nation for traffic congestion[6]. The need for intelligent traffic shaping and development has never been greater. Acyclica, a service provided by Western Systems and now owned by FLIR[7], is an implementation of surveillance technology specifically designed to address this problem.

We were happy to see the 2015 independent audit of Acyclica's systems [SIR 8.2]. This is an excellent industry best practice, and one that we'll be recommending to other departments throughout this document.

In addition, we are pleased to see the hashing function's salt value rotated every 24-hours [SIR 4.10]. This ensures that even the 10-year retention policy [SIR 5.2] cannot be abused to correlate multiple commute sessions and individually identify a person.

Recommendations

- FLIR Systems' acquisition of Acyclica is a recent development (September 2018). We recommend verifying that the Western Systems terms [SIR 3.1] still apply. If they have been superseded by new terms from FLIR Systems, those should be subject to an audit by SDOT and Seattle IT. Specifically, section 2.5.1 of Western Systems' terms must still apply:

> 2.5.1. It is the understanding of the City that the data gathered are encrypted to fully eliminate the possibility of identifying individuals or vehicles. In no event shall City or Western Systems and its subcontractors make any use of the data gathered by the devices for any purpose that would identify the individuals or vehicles included in the data.

- FLIR Systems is known primarily as an infrared technology vendor. Special care should be taken if FLIR/Acyclica attempt to couple IR scanning with WiFi/MAC sniffing. Implementation of an IR system would necessitate a new public surveillance review.

---

[5] "114,000 more people: Seattle now decade's fastest-growing big city in ...." 24 May. 2018, https://www.seattletimes.com/seattle-news/data/114000-more-people-seattle-now-this-decades-fastest-growing-big-city-in-all-of-united-states/
[6] "INRIX Global Traffic Scorecard." http://inrix.com/scorecard/
[7] "FLIR Systems Acquires Acyclica | FLIR Systems, Inc.." 11 Sep. 2018, http://investors.flir.com/news-releases/news-release-details/flir-systems-acquires-acyclica

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SCL: Binoculars, Check Meter, SensorLink

Comments

As these three technologies are serving the same team and mission objectives, we will review them here in a combined section.

The mission of the Current Diversion Team (CDT) is to investigate and gather evidence of illegal activity related to the redirection and consumption of electricity without paying for its use. As such, none of these technologies surveil the public at large. They instead target specific locations and equipment, albeit without the associated customer's knowledge.

It appears as though all data collected through the Check Meter Device and SensorLink Amp Fork are done without relying on a third-party service, so the usual scrutiny of a vendor's privacy policies does not apply.

Recommendations

- **Binoculars**: We have no recommendations for the use of binoculars.
- **Check Meter Device & SensorLink Amp Fork**: As noted in the comments above, we have no further recommendations for the use of the Check Meter Device and SensorLink Amp Fork technologies.
- **Racial Equity**: As with any city-wide monitoring practice, it can be easy to more closely scrutinize one neighborhood over another. Current diversion may be equally illegal (and equally prevalent) across the city, but the enforcement of this law may be unevenly applied. This could introduce racial bias by disproportionately burdening specific neighborhoods with a higher level of surveillance.

  As described, DPP 500 P III-416 section 5.2[8] asserts that all customers shall receive uniform consideration [SIR RET 1.7]. To ensure this policy is respected, we encourage City Light to track and routinely review the neighborhoods where CDT performs investigations, with a specific emphasis on racial equity. This information should be made publicly available.

  When asked at the February 27th Surveillance Technology public meeting, SDOT indicated that no tracking is currently being done on where current diversion is enforced.

[8] "SCL DPP 500 P III-416 Current Diversion - Seattle.gov." 11 Jan. 2012, http://www.seattle.gov/light/policies/docs/III-416%20Current%20Diversion.pdf

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: 911 Logging Recorder

Comments

This is a technology that the general public would likely already assume is in place. Some of the more sensational 911 call logs have been, for example, played routinely on the news around the country. Since it would not alarm the public to know that 911 call recording is taking place, our recommendations will focus primarily on data use, retention, and access control.

Call logging services are provided by NICE Ltd., an Israeli company founded in 1986. This vendor has had a troubling history with data breaches. For example, a severe vulnerability discovered in 2014 allowed unauthorized users full access to a NICE customer's databases and audio recordings[9]. Again, in 2017, a NICE-owned server was set up with public permissions, exposing phone numbers, names, and PINs of 6 million Verizon customers[10].

Recommendations

- SIR Appendix K includes a CJIS audit performed in 2017. SIR section 4.10 also mentions that ITD (Seattle IT) periodically performs routine monitoring of the SPD systems.

  However, given the problematic history with the quality of the technology vendor, if any of the NICE servers, networks, or applications were installed by the vendor (or installation was overseen/advised by the vendor), we recommend an external audit of the implementation of the call logging technology.

- SIR sections 3.3 and 4.2 outline the SPD-mandated access control and data retention policies, however it is not apparent if there is a policy that strictly locks down the use of this technology to a well-defined list of allowed cases. We recommend formally documenting the allowed 911 Logging use cases, and creating a new SIR for any new desired applications of this technology.

  With a 90-day retention policy [SIR 4.2], and with SPD receiving 900,000 calls per year[11], there are about 220,000 audio recordings existing at any given time. This is enough for a data mining, machine learning, or voice recognition project.

---

[9] "Backdoor in Call Monitoring, Surveillance Gear — Krebs on Security." 28 May. 2014, https://krebsonsecurity.com/2014/05/backdoor-in-call-monitoring-surveillance-gear/
[10] "Nice Systems exposes 14 million Verizon customers on open AWS ...." 12 Jul. 2017, https://www.techspot.com/news/70106-nice-systems-exposes-14-million-verizon-customers-open.html
[11] "9-1-1 Center - Police | seattle.gov." https://www.seattle.gov/police/about-us/about-policing/9-1-1-center

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: Computer-Aided Dispatch (CAD)

Comments

As mentioned in the section "SFD: Computer-Aided Dispatch (CAD)" and the section "SPD: 911 Logging Recorder", these dispatch technologies are mandatory for functional emergency services of a city this size. No other system would be able to meet the federal- and state-mandated response times and reporting requirements.

SIR section 4.10 mentions that ITD (Seattle IT) performs routine inspections of the Versaterm implementation.

Versaterm, founded in 1977, provides the technology used by SPD's CAD system. SPD purchased this technology in 2004. In September of 2016, there was a legal dispute between Versaterm and the City of Seattle over a Public Records Act (PRA) disclosure of certain training and operating manuals[12]. The court ruled in favor of Versaterm.

Recommendations

- It is not immediately clear what use cases are described in SIR 2.5 describing data access by "other civilian staff whose business needs require access to this data". All partnerships and data flows between SPD and businesses should be explicitly disclosed.

- This system has been in place for 15 years. As with any technology, advancements in security, speed, usefulness, and reliability come swiftly. Due to the age of the technology, and the potential damaged relationship between Seattle and Versaterm due to the aforementioned legal dispute, we recommend conducting a survey into the plausibility of replacing Versaterm as SPD's CAD solution.

- As mentioned in the introduction to this document, Seattle has adopted the Welcoming Cities Resolution[13]. In honoring this resolution, we recommend that SPD never disclose identifying information, from CAD or any system, to Immigrations and Customs Enforcement (ICE) without a criminal warrant.

[12] "Versaterm Inc. v. City of Seattle, CASE NO. C16-1217JLR | Casetext." 13 Sep. 2016, https://casetext.com/case/versaterm-inc-v-city-of-seattle-2
[13] "Welcoming Cities Resolution - Council | seattle.gov." http://www.seattle.gov/council/issues/past-issues/welcoming-cities-resolution

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: CopLogic

Comments

Track 1 - Public reporting of no-suspect, no-evidence, non-emergency crimes

CTAB understands that in cases where no evidence or suspect is available, a crime should be reported (for statistical or insurance purposes) but does not require the physical appearance of an SPD officer.

Track 2 - Retail Loss Prevention

This track is more problematic, as it could be used by retailers as a method to unreasonably detain, intimidate, or invade the privacy of a member of the public accused of, but not proven guilty of, shoplifting.

Recommendations

- **Track 2**: If not already done, retailers should be trained and informed that having a CopLogic login does not allow them to act as if they are law enforcement officers. Members of the public suspected of shoplifting need to have an accurate description of their rights in order to make informed decisions before providing identifying information. Retailers are also held to a lower standard than SPD regarding racial bias. It is virtually guaranteed that people of color are disproportionately apprehended and entered into the retail track of CopLogic.

  We recommend discontinuing Track 2 entirely.

- **Track 1 & 2**: If not already done, SPD, in coordination with Seattle IT, should perform or hire a company to perform an audit of the vendor's systems. If this audit has not been performed in the 8 years since purchasing this system, it should absolutely be done before the 10-year mark in 2020.
- **Track 1 & 2**: It is not immediately clear in the SIR or LexisNexis's Privacy Policy what CopLogic does with these records long-term, after SPD has imported them into their on-premises system. A written statement from LexisNexis on how this data is used, mined, or sold to affiliates/partners should be acquired by SPD.
- **Track 1 & 2**: We recommend migrating CopLogic to an on-premises solution. We found the LexisNexis privacy policy to be obfuscated and vague[14]. Such sensitive information should not be protected by trust alone.

[14] "Privacy Policy | LexisNexis." 7 May. 2018, https://www.lexisnexis.com/en-us/terms/privacy-policy.page

City of Seattle

AMERICAN CIVIL LIBERTIES UNION
Washington

901 Fifth Ave, Suite #630
Seattle, WA 98164
(206) 624-2184
aclu-wa.org

Tana Lin
Board President

Michele Storms
Executive Director

Shankar Narayan
Technology & Liberty Project Director

March 20, 2019

RE: ACLU-WA Comments Regarding Group 2 Surveillance Technologies

Dear Seattle IT:

On behalf of the ACLU of Washington, I write to offer our comments on the surveillance technologies included in Group 2 of the Seattle Surveillance Ordinance process. We are submitting these comments by mail and electronically because they do not conform to the specific format of the online comment form provided on the CTO's website, and because the technologies form groups in which some comments apply to multiple technologies.

These comments should be considered preliminary, given that the Surveillance Impact Reports (SIR) for each technology leave a number of significant questions unanswered. Specific unanswered questions for each technology are noted in the comments relating to that technology, and it is our hope that those questions will be answered in the updated SIR provided to the Community Surveillance Working Group and to the City Council prior to their review of that technology. In addition to the SIR, our comments are also based on independent research relating to the technology at hand.

The 8 technologies in Group 2 are covered in the following order.

I. Acyclica (SDOT)

II. CopLogic (SPD)

III. Computer-Aided Dispatch & 911 Logging Recorder Group

1. Computer-Aided Dispatch (SPD)
2. Computer-Aided Dispatch (SFD)
3. 911 Logging Recorder (SPD)

IV. Current Diversion Technology Group

1. Check Meter Device (Seattle City Light)
2. SensorLink Amp Fork (Seattle City Light)
3. Binoculars/Spotting Scope (Seattle City Light)

I. Acyclica - SDOT

Background

Acyclica technology is a powerful location-tracking technology that raises a number of civil liberties concerns because of its ability to uniquely identify individuals and their daily movements. Acyclica (via its hardware vendor, Western Systems), manufactures Intelligent Transportation System (ITS) sensors called RoadTrend that are used by the Seattle Department of Transportation for the stated purpose of traffic management. These RoadTrend sensors collect encrypted media access control (MAC) addresses, which are transmitted by any Wi-Fi enabled device including phones, cameras, laptops, and vehicles. Collection of MAC addresses, even when hashed (a method of de-identifying data irreversibly),[1] can present locational privacy challenges.

Experts analyzing a dataset of 1.5 million individuals found that just knowing four points of approximate spaces and times that individuals were near cell antennas or made a call were enough to uniquely identify 95% of individuals.[2] In the case of Acyclica's operation in Seattle, the dataset is comprised of MAC addresses recorded on at least 301 intersections,[3] which allows Acyclica to generate even more precise location information about individuals. Not only do the RoadTrend sensors pick up the MAC addresses of vehicle drivers and riders, but these sensors can also pick up the MAC addresses of all nearby individuals, including pedestrians, bicyclists, and people in close structures (e.g., apartments, offices, and hospitals). Acyclica technology's location tracking capabilities means that SDOT's use of Acyclica can not only uniquely identify individuals with ease, but can also create a detailed map of their movements. This raises privacy concerns for Seattle residents, who may be tracked without their consent by this technology while going about their daily lives.

These location-tracking concerns are exacerbated by the lack of clarity around whether SDOT has a contract with Acyclica (see below). Without a contract, data ownership and scope of data sharing and repurposing by Acyclica is unclear. For example, without contractual restrictions, Acyclica

[1] Hashing is a one-way function that scrambles plain text to produce a unique message digest. Unlike encryption—which is a two-way function, allowing for decryption—what is hashed cannot be un-hashed. However, hashed location data can still be used to uniquely identify individuals. While it is infeasible to compute an input given only its hash output, pre-computing a table of hashes is possible. These types of tables consisting of pre-computed hashes and their inputs are called rainbow tables. With a rainbow table, if an entity has a hash, then they only need to look up that hash in their table to then know what the original MAC address was.
[2] Montjoye, Y., Hidalgo, C., Verleysen, M., and Blondel, V. 2013. Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports.* 3:1375.
[3] The SIR states that SDOT has 301 Acyclica units installed throughout the City. However, an attached location excel sheet in Section 2.1 lists 389 Acyclica units, but only specifies 300 locations.

would be able to share the raw data (i.e., the non-aggregated, hashed data before it is summarized and sent to SDOT) with any third parties, and these third parties would be able to use the data in any way they see fit, including combining the data with additional data such as license plate reader or facial recognition data. Acyclica could also share the data with law enforcement agencies that may repurpose the data, as has happened with other City data. For example, in 2018, U.S. Immigration and Customs Enforcement (ICE) approached Seattle City Light with an administrative subpoena demanding information on a particular customer location, including phone numbers and information on related accounts.[4] ICE also now has agency-wide access to a nationwide network of license plate readers controlled by Vigilant Solutions,[5] indicating the agency may seek additional location data for immigration enforcement purposes in the future. Data collected via Acyclica should never be used for law enforcement purposes.

The uncertainty around the presence or absence of a contract contributes to two key issues: (1) lack of a clearly defined purpose of use of Acyclica technology; and (2) lack of clear restrictions on the use of Acyclica technology that track that purpose. With no contract, SDOT cannot enforce policies restricting the use of Acyclica technology to the intended purpose.

There are also a number of contradictory statements in the SIR concerning the operation of Acyclica technology,[6] as well as discrepancies between the SIR, the information shared at the technology fair (the first public meeting to discuss the Group 2 technologies),[7] and ACLU-WA's conversation with the President of Acyclica, Daniel Benhammou. All these leave us with concerns over whether SDOT fully understands (and the SIR reflects) the capabilities of the technology. In addition, there remain a number of critical unanswered questions that the final SIR must address (set forth below).

Of additional concern is the recent acquisition of Acyclica by FLIR Systems, an infrared and thermal imaging company funded by the U.S. Department of Defense.[8] As of March 2019, FLIR has discontinued Acyclica RoadTrend sensors.[9] Neither the implications of the FLIR acquisition nor the discontinuation of the RoadTrend sensors are mentioned in the SIR—but if the sensors used will change, the SIR should make clear how that will impact the technology.

a. Specific Concerns

- *Inadequate Policies Defining Purpose of Use.* Policies cited in the SIR are vague,

[4] https://crosscut.com/2018/02/immigration-officials-subpoena-city-light-customer-info
[5] https://www.theverge.com/2018/3/1/17067188/ice-license-plate-data-california-vigilant-solutions-alpr-sanctuary
[6] Explained in further detail in 1. Acyclica – SDOT *Major Concerns* below.
[7] http://www.seattle.gov/tech/initiatives/privacy/events-calendar#/?i=3
[8] https://www.crunchbase.com/acquisition/flir-systems-acquires-acyclica--e6043a1a#section-overview
[9] https://www.flir.com/support/products/roadtrend#Specifications

short, and impose no meaningful restrictions on the purposes for which Acyclica devices may be used.[10] Section 1.1 of the abstract set forth in the SIR states that Acyclica is used by over 50 agencies to "to help to monitor and improve traffic congestion." Section 2.1 is similarly vague, providing what appear to be examples of some types of information the technology produces (e.g., calculated average speeds) in order to facilitate outcomes (correcting traffic signal timing, providing information to travelers about expected delays, and allowing SDOT to meet traffic records and reporting requirements)—but it's not clear this list is exhaustive. Section 2.1 fails to describe the purpose of use, all the types of information Acyclica provides, and all the types of work that Acyclica technology facilitates. All these must be clarified.

- *Lack of Clarity on Whether Acyclica and SDOT have a Written Contract.* The SIR does not state that any contract exists, and in the 2018 conversation ACLU-WA had with Benhammou, he stated that there was no contract between the two parties. However, at the 2019 technology fair, the SDOT representative affirmatively stated that SDOT has a contract with Acyclica. As previously mentioned, the lack of a contract limits SDOT's ability to restrict the scope of data sharing and repurposing. The only contractual document provided appears to be a terms sheet in Section 3.0 detailing SDOT's terms of service with Western Systems (the hardware vendor that manufactures the Acyclica RoadTrend sensors), which states that Western Systems only deals with the maintenance and replacement of the hardware used to gather the data, and not the data itself.

- *Lack of Clarity on Data Ownership.* At the technology fair, the SDOT representative stated that SDOT owns all the data collected (including the raw data), but the SIR only states that the aggregated traffic data is owned by SDOT. In the 2018 conversation, Benhammou stated that Acyclica owns all the raw data. There is an apparent lack of clarity between SDOT and Acyclica concerning ownership of data that must be addressed.

- *Data Retention Periods are Unclear.* Section 5.2 of the SIR states that there is a 10-year internal deletion requirement for the aggregated traffic data owned by SDOT, but pg. 37 of the SIR states that "the data is deleted within 24 hours to prevent tracking devices over time." In the 2018 interview, Benhammou stated that Acyclica retains all non-aggregated data indefinitely. It is unclear whether the different retention periods stated in the SIR are referring to different types of data. The lack of clarity on data retention periods also relates to the lack of clarity on data ownership given that data retention periods may depend on data ownership.

[10] As noted in 1. Acyclica – SDOT *Background* above.

- *Inaccurate Descriptions of Anonymization/Data Security Practices.* The SIR appears to use the terms "encryption" and "hashing" interchangeably in some parts of the SIR, making it difficult to clearly understand Acyclica's practices in this area. For example, Section 7.2 states: "Contractually, Acyclica guarantees that the data gathered is encrypted to fully eliminate the possibility of identifying individuals or vehicles." But by design, encryption allows for decryption with a key, meaning anyone with that key and access to the data can identify individuals. (Also, if there is no contract between SDOT and Acyclica, the use of 'contractually' is misleading). This language is also used in the terms sheet detailing SDOT's contract with Western Systems (in Section 2.5.1 in the embedded contract). The SIR compounds this confusion with additional contradictory statements. For example, the SIR states in multiple sections that the data collected by the RoadTrend sensors are encrypted and hashed on the actual sensor. However, according to a letter from Benhammou provided by SDOT representatives at the technology fair,[11] the data is never hashed on the sensor—the data is only hashed after being transmitted to Acyclica's cloud server. These contradictory descriptions cause concern.

- *No Restrictions on Non-City Data Use.* Section 6.3 of the SIR states that there are no restrictions on non-City data use. However, there are no policies cited making clear the criteria for such use, any inter-agency agreements governing sharing of Acyclica data with non-City parties, or why the data must be shared in the first place.

- *Not All Locations of Acyclica Devices are Specified.* Section 2.1 of the SIR states that there are 301 Acyclica locations in Seattle. However, in the embedded excel sheet detailing the serial numbers and specific intersections in which Acyclica devices are installed, there are 389 serial numbers, but only 300 addresses/locations specified. The total number and the locations of Acyclica devices collecting data in Seattle is unclear. This gives rise to the concern that there are unspecified locations in which Acyclica devices are collecting MAC addresses.

- *No Mention of RoadTrend Sensor Discontinuation.* As noted in the background,[12] Acyclica has been acquired by FLIR, an infrared and thermal imaging company. As of March 2019, FLIR's product webpage states that the Acyclica RoadTrend sensors (those currently used by SDOT) have been discontinued.[13] From the information we have, it is unclear if SDOT will be able to continue using the RoadTrend sensors described in the 2019 SIR. Given that FLIR sensors, such as the TrafiOne, have capabilities that go much farther than those of the

[11] Included in Appendix 1.
[12] As noted in 1. Acyclica – SDOT *Background* above.
[13] https://www.flir.com/support/products/roadtrend#Specifications

RoadTrend sensors (e.g., camera technology and thermal imaging)[14] as well as potentially different technical implementations, their use would give rise to even more serious privacy and misuse concerns. Neither the implications of the FLIR acquisition nor the discontinuation of the RoadTrend sensors are mentioned in the SIR.

- *No Mention of Protecting MAC Addresses of Non-Drivers/Riders (e.g., people in nearby buildings).* The Acyclica sensors will pick up the MAC addresses of all nearby individuals, regardless of whether they are or are not driving or riding in a vehicle. The SIR does not mention any steps taken to reduce the privacy infringements on non-drivers/riders.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- For what specific purpose or purposes will Acyclica be used, and what policies state this?
- Does SDOT have a contract with Acyclica, and if so, why is the contract not included in the SIR?
- Who owns the raw, non-aggregated data collected by Acyclica devices?
- What is the retention period for the different types of collected data (aggregated and non-aggregated)—for both SDOT and Acyclica?
- Provide accurate descriptions of Acyclica's data security practices, including encryption and hashing, consistent with the letter from Daniel Benhammou, including any additional practices that prevent reidentification.
- What third parties will access Acyclica's data, for what purpose, and under what conditions?
- Why are 89 locations not specified in the embedded Acyclica locations sheet in Section 2.1 of the SIR?
- Will SDOT continue to use Acyclica RoadTrend Sensors, and for how long? If SDOT plans to switch to other sensors, which ones, and how do their capabilities differ from the RoadTrend Sensors?
- Did SDOT consider any other alternatives when deciding to acquire Acyclica? Did SDOT consider other, more privacy protective traffic management tools in use (for example, inductive-loop detectors currently used by the Washington State Department of Transportation and the US

[14] https://www.flir.com/support/products/trafione#Resources

Department of Transportation)?[15]

- How does SDOT plan to reduce the privacy infringements on non-drivers/riders?

c. Recommendations for Regulation:

At this stage, pending answers to the questions set forth above, we can make only preliminary recommendations for regulation of Acyclica. We recommend that the Council adopt, via ordinance, clear and enforceable rules that ensure, at a minimum, the following:

- There must be a binding contract between SDOT and Acyclica.
- The contract between SDOT and Acyclica must include the following minimum provisions:
  - A data retention period of 12 hours or less for any data Acyclica collects, within which time Acyclica must aggregate the data, submit it to SDOT, and delete both non-aggregated and aggregated data.
  - SDOT receives only aggregated data.
  - SDOT owns all data, not Acyclica.
  - Acyclica cannot share the data collected with any other entity besides SDOT for any purpose.
- The ordinance must define a specific purpose of use for Acyclica technology, and all use of the tool and its data must be restricted to that purpose. For example: Acyclica may only be used for traffic management purposes, defined as activities concerning calculating average travel times, regulating traffic signals, controlling traffic disruptions, determining the placement of barricades or signals for the duration of road incidents impeding normal traffic flow, providing information to travelers about traffic flow and expected delays, and allowing SDOT to meet traffic records and reporting requirements.
- SDOT must produce an annual report detailing its use of Acyclica, including details how SDOT used the data collected, the amount of data collected, and for how long it was retained and in what form.

II. CopLogic – SPD

[15] https://www.fhwa.dot.gov/publications/research/operations/its/06108/03.cfm

Background

CopLogic (LexisNexis's Desk Officer Reporting System-DORS)[16] is a technology owned by LexisNexis and used by the Seattle Police Department to allow members of the public and retailers to submit online police reports regarding non-emergency crimes. Members of the public and retailers can submit these reports through an online portal they can access via their phone, tablet, or computer. Community members can report non-emergency crimes that have occurred within the Seattle city limits, and retail businesses that participate in SPD's Retail Theft Program may report low-level thefts that occur in their businesses when they have identified a suspect. This technology is used by SPD for the stated purpose of freeing up resources in the 9-1-1 Center, reducing the need for a police officer to be dispatched for the sole purpose of taking a police report.

This technology gives rise to potential civil liberties concerns because it allows for the collection of information about community members, unrelated to a specific incident, and without any systematic method to verify accuracy or correct inaccurate information. In addition, there is lack of clarity surrounding data retention and data sharing by LexisNexis, and around how CopLogic data will be integrated into SPD's Records Management System.

a. Concerns

- *Lack of Clarity on CopLogic/LexisNexis Data Collection and Retention.* There is no information in the SIR or in the contract between SPD and LexisNexis detailing the data retention period by LexisNexis (Section 5.2 of the SIR). This lack of clarity stems in part from an unclear description of what's provided by LexisNexis—it's described as an online portal, but the SIR and the contract provided appears to contemplate in Section 4.8 that LexisNexis will indeed access and store collected data. If true, the nature of that access should be clarified, and data restrictions including clear access limitations and retention periods should accordingly be put in place. Once reports are transferred over to SPD's Records Management System (RMS), the reports should be deleted by CopLogic/LexisNexis.

- *Lack of Clarity on LexisNexis Data Sharing with Other Agencies or Third Parties.* If LexisNexis does access and store data, it should do so only for purposes of fulfilling the contract, and should not share that data with third parties. But the contract between SPD and LexisNexis does not make clear whether LexisNexis is prohibited entirely from sharing data with other entities (it does contain a restriction on "transmit[ting]" the data, but without reference to third parties.

[16] https://risk.lexisnexis.com/products/desk-officer-reporting-system

- *No Way to Correct Inaccurate Information Collected About Community Members.* Community members or retailers may enter personally-identifying information about third parties without providing notice to those individuals, and there is no immediate, systematic method to verify the accuracy of information that individuals provide about third parties. There are also no stated measures in the SIR to destroy improperly collected data.

- *Lack of clarity on how the CopLogic data will be integrated with and analyzed within SPD's RMS.* At the technology fair, SPD stated that completed complaints will go into Mark43[17] when it is implemented. ACLU-WA has previously raised concerns about the Mark43 system, and it should be made clear how CopLogic data will enter that system, including to what third parties it will be made available.[18]

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What data does LexisNexis collect and store via CopLogic? What are LexisNexis's data retention policies for CopLogic data?

- Are there specific policies restricting LexisNexis from sharing CopLogic data with third parties? If so, what are they?

- Is there any way to verify or correct inaccurate information collected about community members?

- How will CopLogic data be integrated with Mark43?

c. Recommendations for Regulation:

Pending answers to the questions set forth above, we can make only preliminary recommendations for regulation of CopLogic. SPD should adopt clear and enforceable policies that ensure, at a minimum, the following:

- After CopLogic data is transferred to SPD's RMS, LexisNexis must delete all CopLogic data.

- LexisNexis is prohibited from using CopLogic data for any purpose other than those set forth in the contract, and from sharing CopLogic data with third parties.

[17] https://www.aclu-wa.org/docs/aclu-letter-king-county-council-regarding-mark-43
[18] A Records Management System (RMS) is the management of records for an organization throughout the records-life cycle. New RMSs (e.g., Mark43) may have capabilities that allow for law enforcement agencies to track and analyze the behavior of specific groups of people, leading to concerns of bias in big data policing, particularly for communities of color.

- Methods are available to the public to correct inaccurate information entered in the CopLogic portal.
- Measures are implemented to delete improperly collected data.

III. Computer-Aided Dispatch & 911 Logging Recorder Group

Overall, concerns around the Computer-Aided Dispatch (CAD) and 911 Logging Recorder technologies focus on use of the technologies and/or collected data them for purposes other than those intended, over-retention of data, and sharing of that data with third parties (such as federal law enforcement agencies). Therefore, for all of these technologies as appropriate, we recommend that the responsible agency should adopt clear and enforceable rules that ensure, at a minimum, the following:

- The purpose of use must be clearly defined, and its operation and data collected must be explicitly restricted to that purpose only.
- Data retention must be limited to the time needed to effectuate the purpose defined.
- Data sharing with third parties, if any, must be limited to those held to the same restrictions.
- Clear policies must govern operation, and all operators should be trained in those policies.

Specific comments follow:

1. Computer-Aided Dispatch – SPD

Background

CAD is a software package (made by Versaterm) utilized by the Seattle Police Department's 9-1-1 Center that consists of a set of servers and software deployed on dedicated terminals in the 9-1-1 center, in SPD computers, and as an application on patrol vehicles' mobile data computers and on some officers' smart phones. The stated purpose of CAD is to assist 9-1-1 Center call takers and dispatchers with receiving requests for police services, collecting information from callers, and providing dispatchers with real-time patrol unit availability. Concerns include lack of clarity surrounding data retention and data sharing with third parties.

a. Concerns:

- *Lack of clarity on data retention within CAD v. RMS.* While the SIR makes clear that at some point, CAD data is transferred to SPD's RMS, it is unclear what data, if any, the CAD system itself retains and for how long. If the CAD system does retain some data (for example, call logs)

independent of the RMS, and that data is accessible to the vendor, appropriate data protections should be put in place. But because the SIR usually references "data collected by CAD," it is unclear where that data resides.

- *Lack of a policy defining purpose of the technology and limiting its use to that purpose*: Unlike SFD's similar system, SPD appears to have no specific policy defining the purpose of use for CAD and limiting its use to that purpose.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- Does the CAD system itself store data? If so, what data and for how long? Who can access that data?

c. Recommendations for Regulation:

Depending on the answer to the question above, appropriate data protections may be needed as described above. In addition, SPD should adopt a policy similar to SFD's, clearly defining purpose and limiting use of the tool to that purpose.

2. Computer-Aided Dispatch – SFD

Background

Computer Aided Dispatch (CAD) is a suite of software packages used by SFD and made by Tritech that provide unit recommendations for 911 emergency calls based on the reported problem and location of a caller. The stated purpose of CAD is to allow SFD to manage emergency and non-emergency call taking and dispatching operations. The technology allows SFD to quickly enable personnel to execute rapid aid deployment.

Generally and positively, SFD clearly defines the purpose of use, restricts CAD operation and data collection to that purpose only, limits sharing with third parties, and specifies policies on operation and training. However, SFD must clarify what data is retained within CAD, data retention policies, and provide information about its data sharing partners.

d. Concerns

- *Lack of clarity on data retention within CAD*. It is unclear what data, if any, the CAD system itself retains and for how long. If the CAD system does retain some data (for example, call logs) and that data is accessible to the vendor, appropriate data protections should be put in place.
- *Lack of clarity on data retention policies*. At the technology fair, we learned that CAD data is retained indefinitely. It is not clear what justifies indefinite retention of this data.

- *Lack of clarity on data sharing partners.* In Section 6.3 of the SIR, SFD states that in rare case where CAD data is shared with partners other than those specifically named in the SIR, a third-party nondisclosure agreement is signed. However, there are no examples or details of who those partners are and the purposes for which CAD data would be shared.

e. Outstanding Questions That Must be Addressed in the Final SIR:

- Does the CAD system itself store data? If so, what data and for how long? Who can access that data?
- Who are SFD's data sharing partners? For what purpose is data shared with them?

f. Recommendations for Regulation:

Depending on the answer to the question regarding if the CAD system itself stores data, appropriate data protections may be needed as described above. SFD should adopt a clear policy requiring deletion of CAD data no longer needed. In addition, depending on how data is shared, SFD should adopt a policy that clearly limits what for what purposes CAD data would be shared, and with what entities.

3. 911 Logging Recorder – SPD

Background

The NICE 911 logging recorder is a technology used by SPD to audio-record all telephone calls to SPD's 9-1-1 communications center and all radio traffic between dispatchers and patrol officers. The stated purpose of the 9-1-1 Logging Recorder is to allow SPD to provide evidence to officers and detectives who investigate crimes and the prosecutors who prosecute offenders. These recordings also provide transparency and accountability for SPD, as they record in real time the interactions between 9-1-1 call takers and callers, and the radio traffic between 9-1-1 dispatchers and police officers. The NICE system also supports the 9-1-1 center's mission of quickly determining the nature of the call and getting the caller the assistance they need as quickly as possible with high quality, consistent and professional services.

Concerns include lack of clarity surrounding data retention schedules and data sharing with third parties.

a. Concerns

- *Lack of clarity on data retention.* Section 4.2 of the SIR states: "Recordings

requested for law enforcement and public disclosure are downloaded and maintained for the retention period related to the incident type." Similar to other technologies noted above, it is unclear whether the 9-1-1 system itself stores these recordings, or if they are stored on SPD's RMS. If the former, it should be made clear how the technology vendor accesses these recordings and for what purpose, if at all.

- *More clarity needed on data sharing with third parties.* There are no details or examples of the "discrete pieces of data" that are shared outside entities and individuals as referenced in Section 6.0 of the SIR.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What is SPD's data retention schedule for data stored in the NICE system, if any?
- What "discrete pieces of data" does SPD share with third parties?

c. Recommendations for Regulation:

SPD should adopt a clear policy requiring deletion of data no longer needed. In addition, depending on how data is shared, SPD should adopt a policy that clearly limits what for what purposes data would be shared, and with what entities.

IV. Current Diversion Technology Group – Seattle City Light

The technologies in this group—the Check Meter device (SensorLink TMS), the SensorLink Amp Fork, and the Binoculars/Spotting Scope raise civil liberties concerns primarily due to lack of explicit, written policies imposing meaningful restrictions on use of the technologies. While the purpose of the current diversion technologies appears clear—to assess whether suspected diversions of current have occurred and/or are continuing to occur—there are no explicit policies in the SIR detailing restrictions on what can and cannot be recorded by these technologies.

Below are short descriptions of the technologies, followed by concerns and recommendations.

Background

1. Check Meter Device (SensorLink TMS)

The SensorLink TMS device measures the amount of City Light-provided electrical energy flowing through the service-drop wire over time, digitally capturing the instantaneous information on the device for later retrieval by the Current Diversion Team via the use of a secure wireless protocol.

The stated purpose of use is to allow Seattle City Light to maintain the integrity of its electricity distribution system, to determine whether suspected current diversions have taken place, and to provide the valuation of the diverted energy to proper authorities for cost recovery.

2. SensorLink Amp Fork

The SensorLink Amp Fork is an electrical device mounted on an extensible pole allowing a circular clamp to be placed around the service-drop wire that provides electrical service to a customer location via its City Light-provided meter. The device then displays instantaneous readings of the amount of electrical energy (measured in amperage, or "amps") that the Current Diversion Team may compare against the readings displayed on the meter, allowing them to determine if current is presently being diverted.

The stated purpose of use of the Amp Fork is to allow Seattle City Light to assess whether suspected diversions of current have occurred and/or are continuing to occur. The Amp Fork allows the Utility to determine the valuation of the energy illegally diverted, which supports City Light's mission of recovering this value for ratepayers via a process called "back-billing."

3. Binoculars/Spotting Scope

The binoculars are standard, commercial-grade, unpowered binoculars. They do not contain any special enhancements requiring power (e.g., night-vision or video-recording capabilities). They are used to read a meter from a distance when the Current Diversion Team is otherwise unable to access physically the meter for the purpose of inspection upon suspected current diversion.

The stated purpose of the binoculars is to allow Seattle City Light to inspect meters and other implicated electrical infrastructure at a distance. If a determination of diversion is sustained, data may be used to respond to lawful requests from the proper law enforcement authorities for evidence for recovering the value of the diverted energy.

a. Concerns Regarding all Three Current Diversion Technologies

- *Absence of explicit, written policies imposing meaningful restrictions on use.* At the technology fair, a Seattle City Light representative stated that these technologies are used only for the purpose of checking current diversions, but could not confirm that Seattle City Light had clear, written policies for what data could and could not be recorded (e.g., an employee using the binoculars to view non-meter related information). The absence of written, specific policies increases the risk of unwarranted surveillance of individuals. There is also no mention in the SIRs of

specific data protection policies in place to safeguard the data (e.g., encryption, hashing, etc.).

- *Seattle City Light's records retention schedule is mentioned in the SIRs, but details about it are omitted.* It is unclear how long Seattle City Light retains data collected, and for what reason.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What enforceable policies, if any, apply to use of these three technologies?
- What is Seattle City Light's data retention schedule?

c. Recommendations for Regulation:

Seattle City Light must create clear, enforceable policies that, at a minimum:

- Define purpose of use for each technology and restrict its use to that purpose.
- Clearly state what clear data protection policies exist to safeguard stored data, if any, and ensure the deletion of data collected by the technology immediately after the relevant current diversion investigation has closed.

Thank you for your consideration, and please don't hesitate to contact me with questions.

Best,

Shankar Narayan
Technology and Liberty Project Director

Jennifer Lee
Technology and Liberty Project Advocate

Appendix 1: Benhammou Letter

City of Seattle

Acyclica

February 6th, 2015

RE: Acyclica data privacy standards

To whom it may concern:

The purpose of this letter is to provide information regarding the data privacy standards maintained by Acyclica. Acyclica is a traffic information company specializing in traffic congestion information management and analysis. Among the various types of data sources which make of Acyclica's traffic data portfolio including GPS probe data, video detection and inductive loops, Acyclica also utilizes our own patent-pending technology for the collection of Bluetooth and Wifi MAC addresses. MAC or Media Access Control addresses are unique 48-bit numbers which are associated with devices with Bluetooth and/or Wifi capable devices.

While MAC addresses themselves are inherently anonymous, Acyclica goes to great lengths to further obfuscate the original source of data through a combination of hashing and encryption to all but guarantee that information derived from the initial data bears no trace of any individual.

Acyclica's technology for collecting MAC addresses for congestion measurement operates by detecting nearby MAC addresses. The MAC addresses are then encrypted using GPG encryption before being transmitted to the cloud for processing. Encrypting the data prior to transmission means that no MAC addresses are ever written where they can be retrieved from the hardware. Once the data is received by our servers, the data is further anonymized using a SHA-256 algorithm which makes the raw MAC address nearly impossible to decipher from the hashed output. Furthermore, any customer seeking to download data for further investigation or integration through our API can only ever view the hashed MAC address.

Acyclica occasionally provides data to partners to help enhance the quality of congestion information. The information which is provided to such partners is received through API calls which only return aggregated information about traffic data over a given period such as the average travel-time over a 5-minute period. Aggregating the data provides a final layer of anonymization by reporting on the collective trend of all vehicles rather than the specific behavior of a single vehicle.

As always questions, comments and concerns are welcome. Please do let me know if we can provide further clarity and transparency on our internal operations with regards to data processing and privacy standards. We take the privacy of the public very seriously and always treat our customers and the data with the utmost respect.

Regards,

Daniel Benhammou
President
Acyclica Inc.

Appendix H: Comment Analysis Methodology

Overview

The approach to comment analysis includes combination of qualitative and quantitative methods. A basic qualitative text analysis of the comments received, and a subsequent comparative analysis of results, were validated against quantitative results. Each comment was analyzed in the following ways, to observe trends and confirm conclusions:

1. Analyzed collectively, as a whole, with all other comments received
2. Analyzed by technology
3. Analyzed by technology and question

A summary of findings are included in Appendix B: Public Comment Demographics and Analysis. All comments received are included in Appendix E: All Individual Comments Received.

Background on Methodological Framework

A modified Framework Methodology was used for qualitative analysis of the comments received, which "…*approaches [that] identify commonalities and differences in qualitative data, before focusing on relationships between different parts of the data, thereby seeking to draw descriptive and/or explanatory conclusions clustered around themes" (Gale, N.K., et.al, 2013).* Framework Methodology is a coding process which includes both inductive and deductive approaches to qualitative analysis.

The goal is to classify the subject data so that it can be meaningfully compared with other elements of the data and help inform decision-making. Framework Methodology is "not designed to be representative of a wider population, but purposive to capture diversity around a phenomenon" (Gale, N.K., et.al, 2013).

Methodology

Step One: Prepare Data

1. Compile data received.
    a. Daily collection and maintenance of 2 primary datasets.
        i. Master dataset: a record of all raw comments received, questions generated at public meetings, and demographic information collected from all methods of submission.
        ii. Comment analysis dataset: the dataset used for comment analysis that contains coded data and the qualitative codebook. The codebook contains the

qualitative codes used for analysis and their definitions.

2. Clean the compiled data.
    a. Ensure data is as consistent and complete as possible. Remove special characters for machine readability and analysis.
    b. Comments submitted through SurveyMonkey for "General Surveillance" remained in the "General Surveillance" category for the analysis, regardless of content of the comment. Comments on surveillance generally, generated at public meetings, were categorized as such.
    c. Filter data by technology for inclusion in individual SIRs.

Step Two: Conduct Qualitative Analysis Using Framework Methodology

1. Become familiar with the structure and content of the data. This occurred daily compilation and cleaning of the data in step one.
2. Individually and collaboratively code the comments received, and identify emergent themes.
    I. Begin with deductive coding by developing pre-defined codes derived from the prescribed survey and small group facilitator questions and responses.
    II. Use clean data, as outlined in Data Cleaning section above, to inductively code comments.
        A. Each coder individually reviews the comments and independently codes them.
        B. Coders compare and discuss codes, subcodes, and broad themes that emerge.
        C. Qualitative codes are added as a new field (or series of fields) into the Comments dataset to derive greater insight into themes, and provide increased opportunity for visualizing findings.
    III. Develop the analytical framework.
        A. Coders discuss codes, sub-codes, and broad themes that emerge, until codes are agreed upon by all parties.
        B. Codes are grouped into larger categories or themes.
        C. The codes are be documented and defined in the codebook.
    IV. Apply the framework to code the remainder of the comments received.
    V. Interpret the data by identifying differences and map relationships between codes and themes, using R and Tableau.

Step Three: Conduct Quantitative Analysis

1. Identify frequency of qualitative codes for each technology overall, by questions, or by

themes:

   I. Analyze results for single word codes.
   II. Analyze results for word pair codes (for context).

2. Identify the most commonly used words and word pairs (most common and least common) for all comments received.
   I. Compare results with qualitative code frequencies and use to validate codes.
   II. Create network graph to identify relationships and frequencies between words used in comments submitted. Use this graph to validate analysis and themes.
3. Extract CSVs of single word codes, word pair codes, and word pairs in text of the comments, as well as the corresponding frequencies for generating visualizations in Tableau.

Step Four: Summarization

1. Visualize themes and codes in Tableau. Use call out quotes to provide context and tone.
2. Included summary information and analysis in the appendices of each SIR.

Appendix I: Supporting Policy Documentation

Fire Alarm Center Policy and Operating Guidelines (POG)

FIRE ALARM CENTER

STANDARD OPERATING PROCEDURES

No. 500 TUB FILE PROGRAM

POLICY:

It shall be the policy of the Fire Alarm Center to adhere to the following procedures when using the Tub File program

DEFINITION: The Tub File is a program that will generate the correct unit stream to send on a response if CAD is down. It is a stand alone version

SEE ALSO: SOP No. 501 (Offline Incident Entry)

1.0 GENERAL

1.1 The "Tub File" laptop is kept behind the Officer position.

1.2 Whenever the FAC is evacuated, regardless of the situation, (relocation drill or emergency), the laptop **MUST** be taken to the new location.

1.3 CAD should run automatically. However, if necessary use the Log In: -

USER ID: dispatch1 PASSWORD: 911911

1.4 There are two rotating laptops that are rotated at the time of monthly CAD maintenance. The Tub File laptop may therefore not be the most current, but will be at most one month behind.

City of Seattle

STANDARD OPERATING PROCEDURES

No. 501 OFFLINE INCIDENT ENTRY

POLICY:

The following procedure shall be utilized when entering offline incidents into CAD following a CAD down situation (i.e., when MIS takes CAD down)

1.0 GENERAL

1.1 When MIS takes CAD down, MIS will provide the FAC staff with: *1) A starting incident number to be used for the next incident. Then additional incidents would continue in sequence. An example is T090025782 and b) Printouts of all the incidents taken on the training VisiCAD system during the offline period.*

1.2 Launch VisiCAD login.

(a) On the top menu select "**Tools\System tools\Offline Incident Entry**". It takes a minute or two to load so you need to be patient.

Response Date/Time (*07/30/2014 09:30:00*)

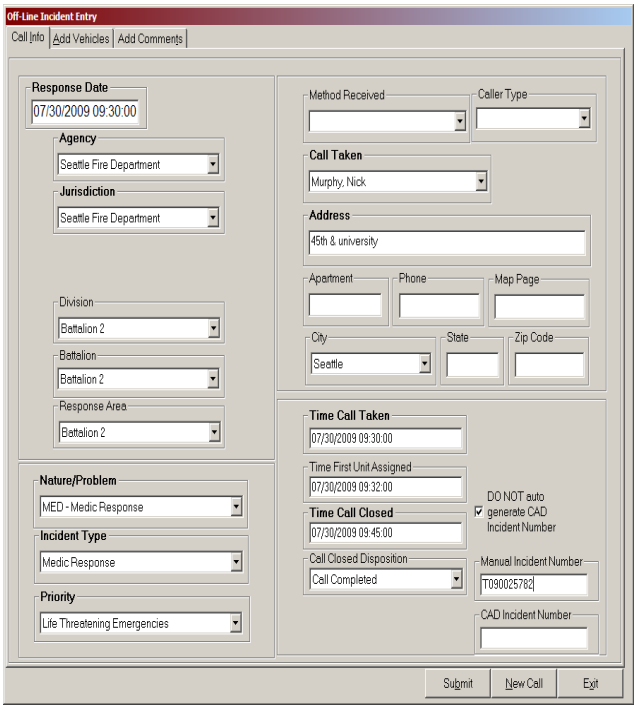
Agency, use drop down (*Seattle Fire Dept*)

Jurisdiction (*Seattle Fire Dept*)

Division & Response Area (*Battalion 2*)

Response Plan/Nature of Problem (*MED – Medic Response*)

Prior ity (*Fire/Medical*)



Call Taken (*Dispatcher)*

Address/Apt *(45 & University)*

City/State/Zip (Seattle)

Time Taken (*07/30/2014 09:30:00)*

Time First Unit Arrived (*07/30/2014 09:32:00)*

Time Call Closed (*07/30/2014 09:45:00)*

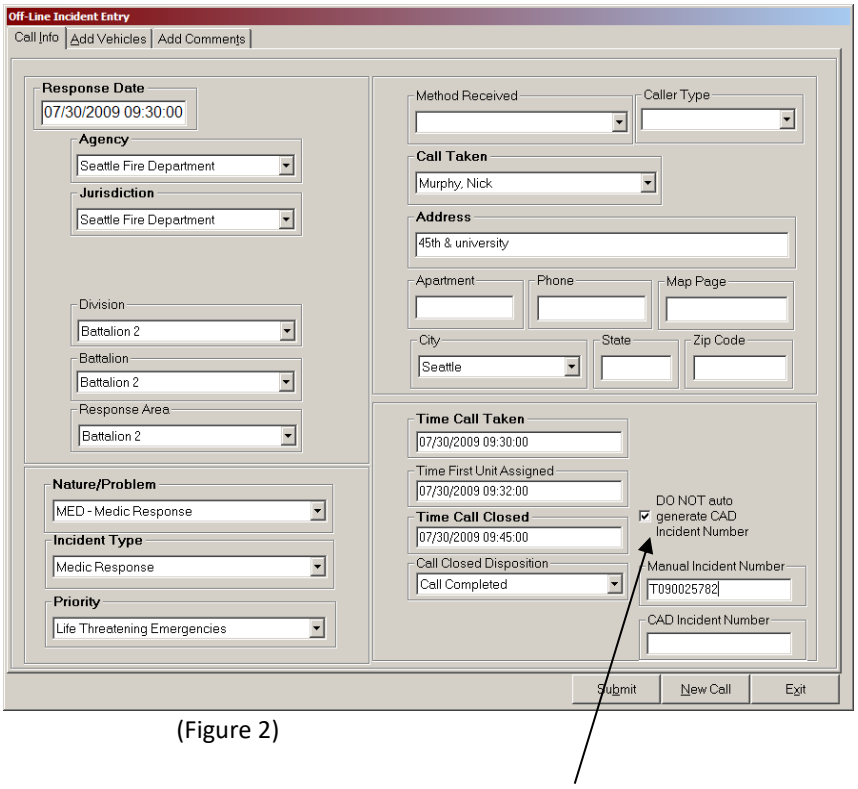
Call Closed Disposition *(Call Completed)*

Check box if MIS has provided Incident No.

Manual Incident No. *(T090025785)*

Figure 1

1.3

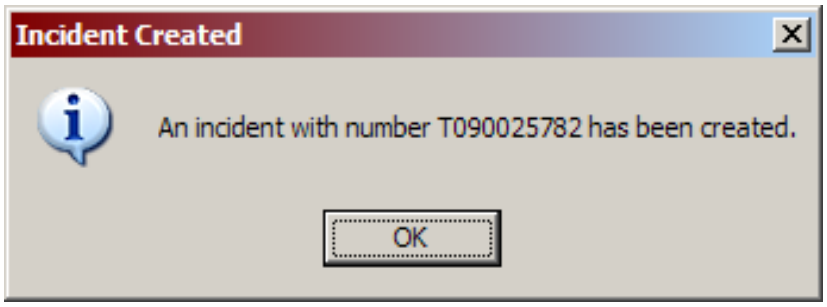


(Figure 2)

1.4 **<u>PLEASE NOTE</u>: Checking the box labeled "DO NOT auto generate CAD Incident Number "is very important" because it prevents you from burning an incident number.**

1.5 Enter the next incident number (or the starting one MIS provides) into the "Manual Incident Number "field and click "Submit".

(1) The software will inform you that an incident has been created by displaying the box in Figure 3.



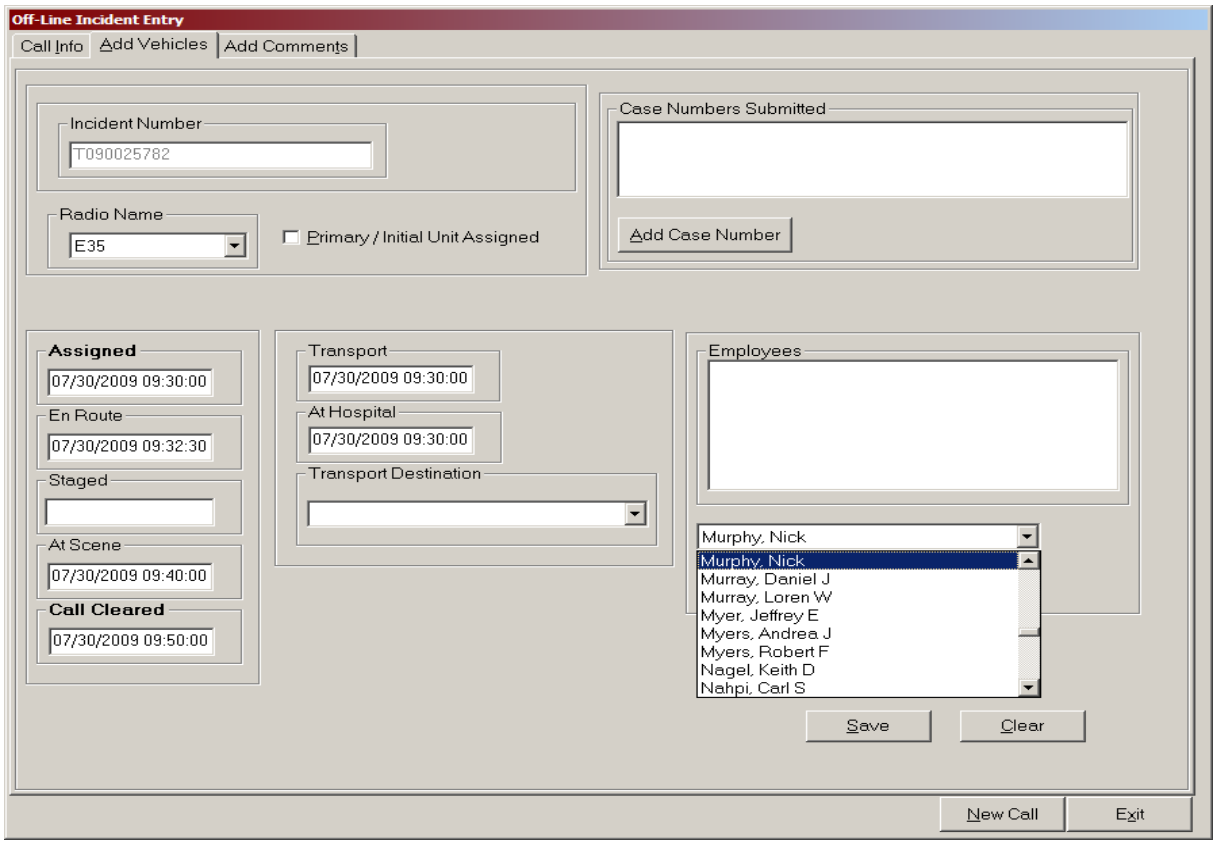
(Figure 3)

1.6 Complete the following steps; the second tab should look like Figure 4.

(1) Enter "**Radio Name**" (E2)

(2) Select "**Primary Unit**" check box if first unit assigned.

(3) Modify "**Assigned Time**" if needed.



(Figure 4)

(1) Modify or Delete "**En-route Time**" if needed.

(2) Delete "**Staged Time**"

(3) Modify or Delete "**At Scene Time**" if needed.

(4) Modify "**Call Cleared Time**"

(5) Modify or Delete "**Transport Time**" if needed.

(6) Modify or Delete "**At Hospital Time**" if needed.

(7) Select "**Transport Destination**" if needed.

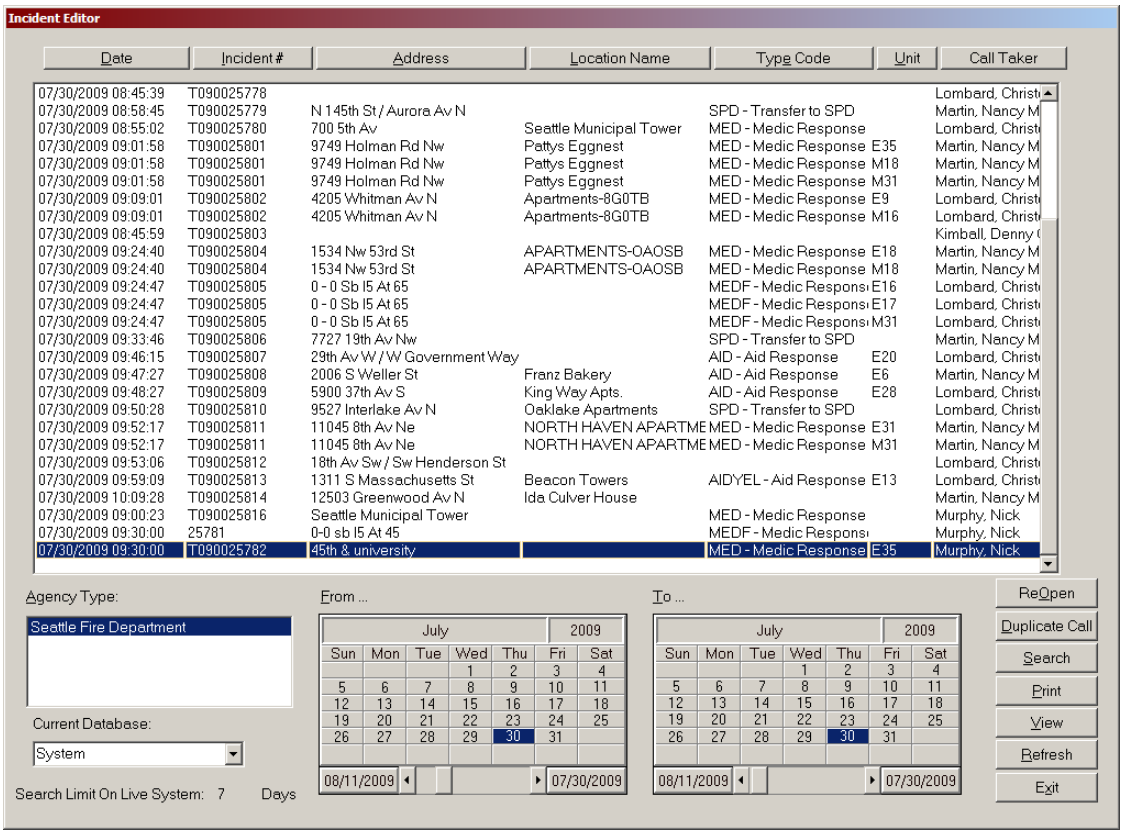
(8) Add "**Employees**" if needed.

(9) Click "**Save Button**"

(10) Enter additional units if needed.

(11) Click Save button and Exit when finished.

1.8 Once you have completed a call you can use the Incident Editor to verify the call in the correct day, see Figure 5.



(Figure 5)

STANDARD OPERATING PROCEDURES

No. 501a Agency Incident Report

City of Seattle

Seattle Fire Department Agency Incident Report

Incident Number **F100075540**

Base Response #

Response Date:	08/18/2010 08:05:20		
Priority:	2 Life Threatening Emergencies		
Incident Type:	Medic Response		
Confirmation#:			
Jurisdiction:	Seattle Fire Department		
Division:	Battalion 5		
Battalion:	Battalion 5		
Station:			
Response Area:	Battalion 5		
Response Plan:	MED – Medic Response		
Incident Type:	Medic Response		
Problem:	MED – Medic Reponse		
Location Name:			
Address:	2209 S Ferdinand St		
Apt/Bldg #:	/		
City, State, Zip	Seattle	WA	98108
County:	King		
Location Type:			
Cross Street:	COLUMBIA DR S/BEACON AV S		
Method of Call Rev Call Back Phone:			
Caller Type:			
Caller Name:			
Caller Loc Name:			
Caller Address:			
Caller Apt/Bldg #:			
Caller City,State,Zip:			
Caller, County:			
Time Phone Pick Up:			
Time 1st Call Taking Key Stroke			
Time Call Entered Queue:			
Time Call Taking Completed:			
Time First Unit Assigned:			
Time First Unit Enroute:			
Time First Unit Arrived:			
Authorization:			

STANDARD OPERATING PROCEDURES

Patient Name:			
Receiving Physician:			
Referring Physician:			
Request P/U Time:			
Promised P/U Time:			
Appointment Time:			
Call Rcvd To In-Queue:			
Call Rcvd To Call Taking Done:			
In-Queue To First Assign:			
Call Rcvd To First Assign:			
Assigned To First Enroute:			
Enroute To First At Scene:			
Call Rcvd To Call Closed:			
Time Incident Under Control **Time Call Closed:** **Time Sent To Other CAD:** **CallTaking Performed By:** **CallTaking Performed By:** **Command Channel:** **Primary TAC Channel:** **Alternate TAC Channel:** **Call Disposition:** **Performed By:** **Cancel Reason:** **NI/ALI Address:** **ANI/ALI City:** **ANI/ALI Phone:** **ANI/ALI Time Rcvd:**			

No. 502 CAD SIGN-ON

POLICY:

It shall be the policy of the Fire Alarm Center to adhere to the following procedures when logging Operations members on/off the CAD system.

SEE ALSO: SOP No. 511 (Task Force Log-On/Log-Off)
SOP No. 505 (Special Events Log-In)

1.0 GENERAL

1.1 The CAD Sign On application allows members to sign on radios to a unit without a person by selecting Employee 0000 from the list.

1.2 When this happens, CADView Roster shows the rank as "**FF**" and the name as "**Spare Radio**" previously listed as "Attached to Unit".

2.0 RADIO SIGN-ON ASSISTANCE FOR OPERATIONS

2.1 In order to maintain proper software communication and integrity, signing on to units and radios shall be done through CAD Sign-On (and not by VisiCAD).

2.2 Operations personnel are responsible for using CAD Sign-On to assign themselves to the appropriate Special Event.

2.3 The following procedures should be implemented in case the FAC must assist OPS personnel when they are having difficulty using CAD Sign-On and assigning portable radios.

(a) USING CAD SIGN-ON

CAD SignOn

(1) Double click on the CAD Sign-On icon located on the desktop.

(2) CAD Sign-On no longer requires the user to login with a username and password.

(3) Begin by typing the name of the unit you will be logging on to *(See Figure 1)*. Select the desired unit and hit the *Tab* or *Enter* key to display the selected unit.

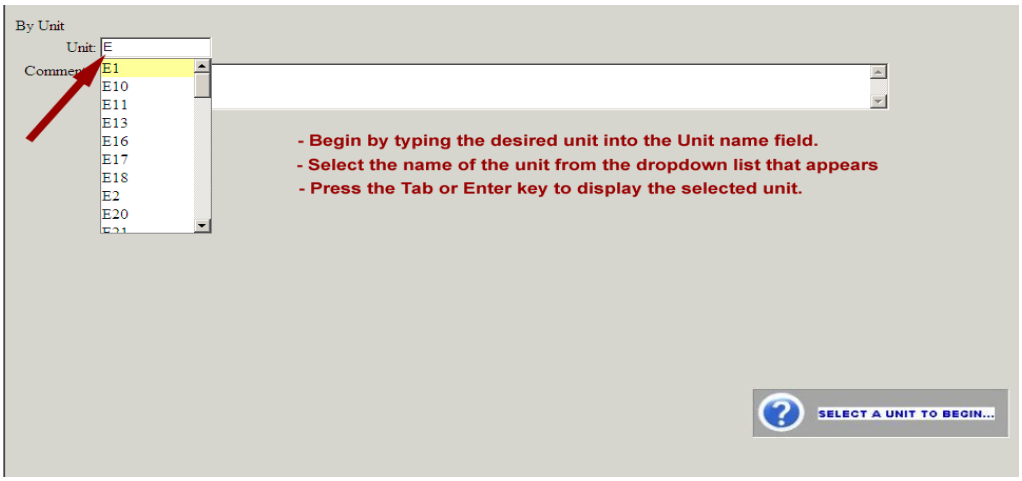


Figure 1

(b) ENTERING CREW MEMBERS INTO UNIT POSITIONS

(1) Enter shift officer or crew members into the appropriate unit positions on the selected unit in the same manner that was used in the previous version of CAD Sign-On.

(2) Unit positions can be filled by entering a member's Injury/Illness number or by beginning to type the member's last name and then selecting the appropriate name from the dropdown list that appears. (*See Figure 2)*

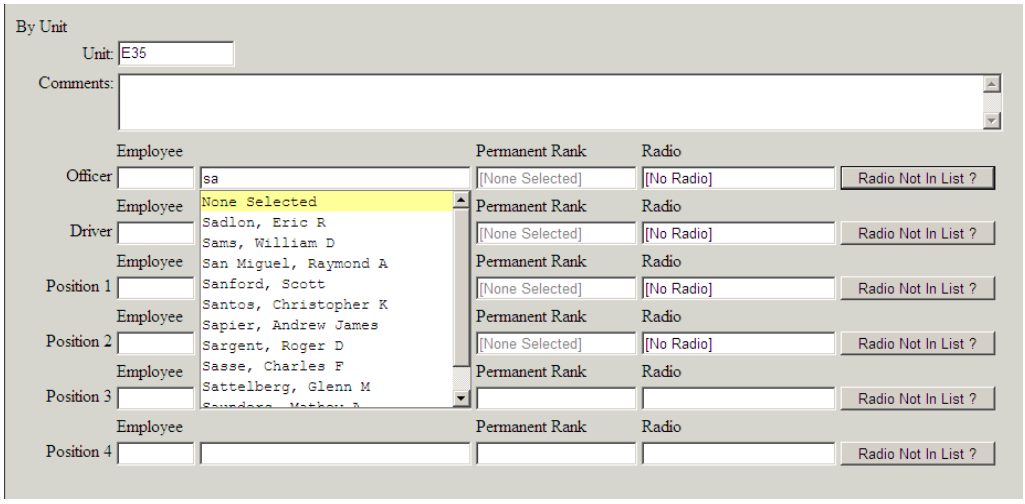


Figure 2

(c) ENTERING RADIOS INTO UNIT POSITIONS

(1) Enter radio numbers into each unit position in the same manner as the previous version of CAD Sign-On. Begin typing the radio number and a dropdown list will appear with all possible matches. Select the desired radio from the list. *(See Figure 3)*

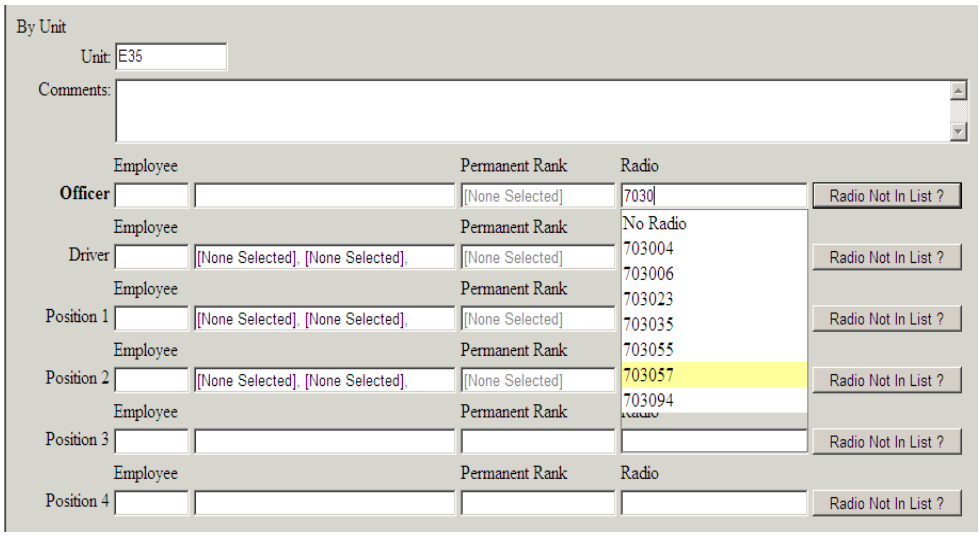


Figure 3

(d) ASSIGNING RADIO(S) TO A UNIT WITHOUT A MEMBER

(1) There are times when it is necessary to assign a radio to a position on a unit without assigning a Member to that position. Follow these steps:

a. In the position you want to assign a radio to, type "0000" as the Employee ID number and press the tab key.

b. In the Employee Name field the words "**Spare Radio**" previously listed as "Attached to Unit" will appear.

c. Tab over to the Radio ID field and enter the radio you wish to assign.

d. Submit your changes. *(See Figure 4)*

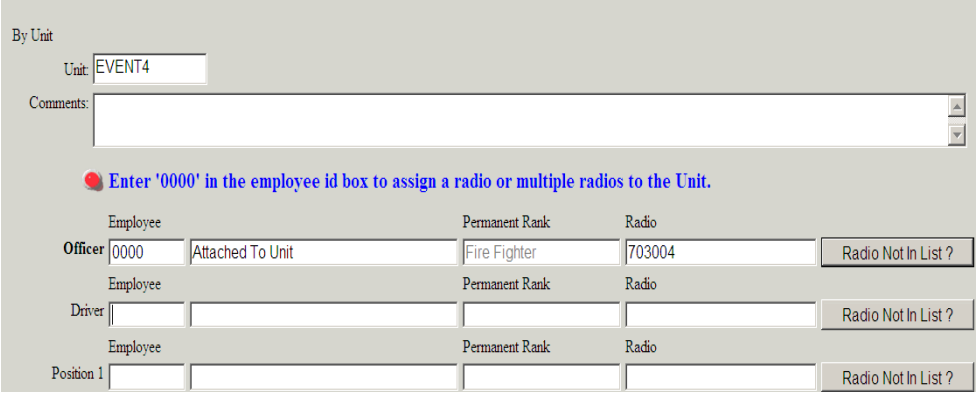


Figure 4

3.0 ERROR MESSAGE SOLUTION <u>NUMBER 1</u> FOR OPERATIONS

3.1 A radio cannot be assigned to more than one apparatus position as CAD Sign On only allows a radio to be assigned to one position on one unit

(a) When you click the submit button to send your sign-on information to CAD, <u>if any of the radio numbers</u> you are trying to submit are already currently assigned to a position on a different unit, you will see a message appear in the message box area at the bottom of the screen informing you which radio number is the problem and which unit, position and member the radio is currently assigned to.

3.2 If Operations personnel are attempting to assign a radio to a position in an EVENT and they find the error message, *"The selected radio (XXXX, EVENT) is already assigned to a position on the current apparatus*. Either pick another radio or un-assign the radio from Position first if you want to assign this radio, direct Operations personnel as follows:

(a) Verify that this member is no longer using the radio. **THIS IS VERY IMPORTANT.**

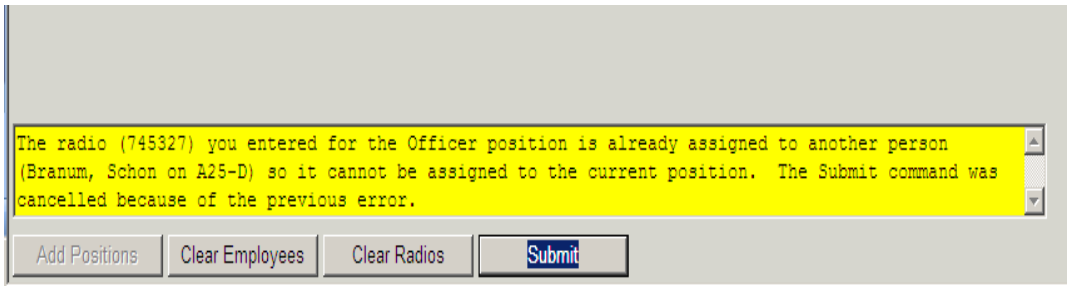
(b) Select the Unit from the "**Unit**" pull-down menu on the FDM Sign-On screen.

(c) At the position listed in the error noted above, set the radio to "**No Radio**" and press **SUBMIT** at the bottom. The "No Radio" selection is at the top of the radio list.

(d) Test the solution by trying to use the radio for the place or person where you would like it to be assigned.

4.0 ERROR MESSAGE SOLUTION NUMBER 2 FOR OPERATIONS

4.1 If Operations personnel are still attempting to assign a radio to a position in an EVENT and the following error message appears:



(a) Re-submit or call SFD MIS Help Desk with the exact error message, direct Operations personnel as follows:

(1) Verify that this person is no longer using the radio. **THIS IS VERY IMPORTANT**.

(2) Select the Unit from the "**Unit**" pulldown menu on the FDM Sign-On screen.

(3) At the position listed in error noted above, sign onto using your injury/illness number and using the radio listed in the error message.

- Press the **SUBMIT** button.
- After submitting, return to that position and set the radio to "No Radio." The "No Radio" selection is at the top of the radio list.
- Hit the **SUBMIT** button.

(4) Test the solution by trying to use the radio for the place or person where you would like it to be assigned.

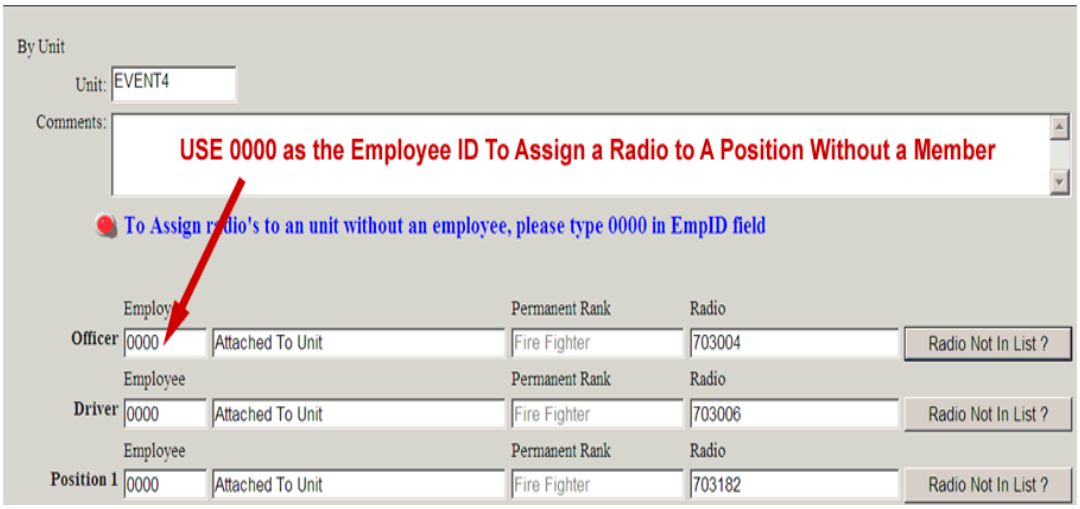
(5) If the radio is still not assigning to the proper position, see 10.0 below.

5.0 ERROR MESSAGE SOLUTION NUMBER 3 FOR OPERATIONS

5.1 Radio disappears when a member is NOT assigned to the Position

(a) If a radio is assigned to a position on a unit but a member is not also assigned to that position, the selected radio will disappear from the unit. Sign-On does not allow a radio to be assigned to a position on a unit without an Employee ID assigned.

(b) To assign a radio to a position without a Member, enter "0000" as the Employee ID and hit the tab key. The words "Spare Radio" previously listed as "Attached to Unit" will appear in the Employee Name field. Next, enter the desired Radio ID. Submit the changes. The radio is now assigned to the desired position without an Employee assigned to the position. (See Figure 6B)



(c) It is acceptable though to assign a member to a position on a unit and not assign that member a radio. This happens very infrequently when the member is a recruit/trainee, FAC, or other who is on a rig but doesn't have a radio.

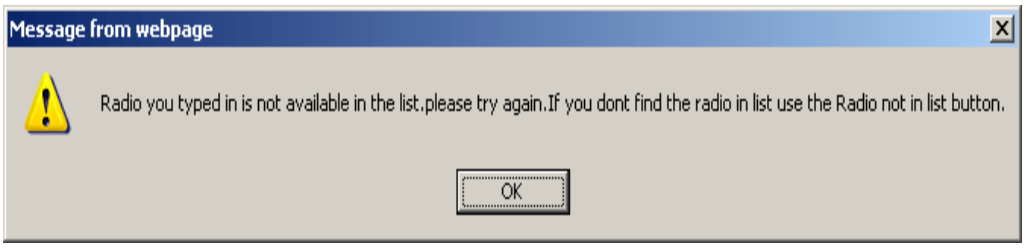
6.0 ERROR MESSAGE SOLUTION <u>NUMBER 4</u> FOR OPERATIONS

6.1 Radio number does not appear in the Radio Dropdown list:

(a) The Radio Dropdown list is populated with valid portable radio numbers from the Department's inventory tracking system. A valid portable radio is a radio that begins with the prefix of 703 or 745 and falls within a minimum and maximum range for each of those prefixes per valid radio ranges recorded into the CAD system itself.

(b) It is possible, although a rare occurrence, that a member can have physical possession of a radio does not appear in the radio dropdown list.

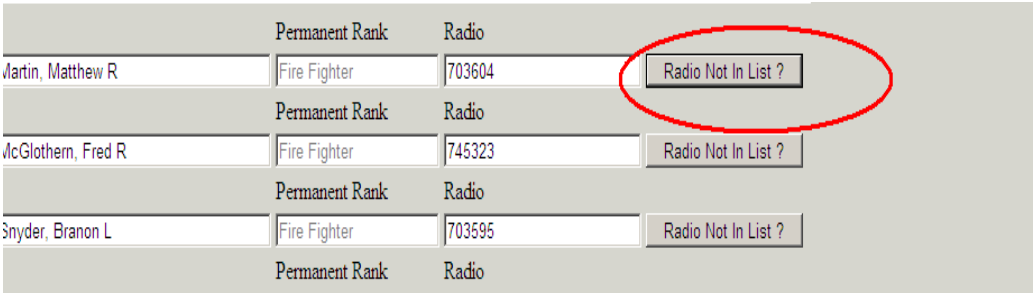
(c) In this case, CAD Sign-On will recognize that the radio number the member is entering is invalid and will display a pop-up message to the user informing them that the radio is not in the valid radio list.



(d) Click the OK button to clear the message and then do the following:

(1) Double check that you are correctly typing in the radio number of the radio you physically have in your possession. If you are sure you're trying to enter the correct number then go to step 2.

(2) Click the *Radio Not In List?* Button. An input box will appear as shown in Figures 8A, 8B and 8C below.



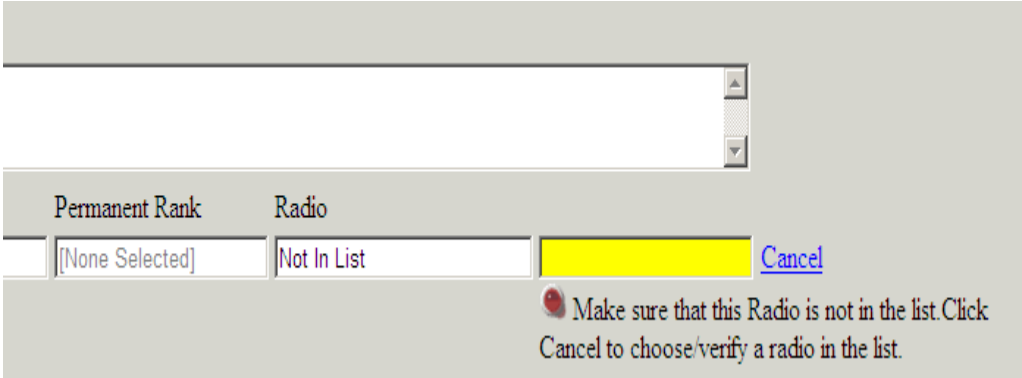


Figure 8B

(e) Type the radio number into the radio input box. When finished filling out the Sign-On form for the selected unit, click the Submit button to submit the sign-on(s).

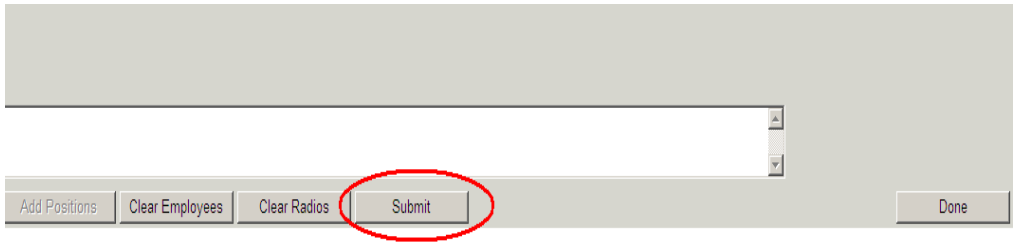


Figure 8C

(f) Clicking the Submit button at this point will allow the user to assign the radio to the desired position and member.

- An email is then generated by the CAD Sign-On application and sent to the FAC On-Duty Shift Officer alerting them that a radio has been assigned to a unit, position and member that is not listed in the valid radio dropdown list.
- The FAC On-Duty Shift Officer will follow up by adding the radio to the list or contacting the member for more information.

7.0 ERROR MESSAGE SOLUTION NUMBER 5 FOR FAC

7.1 This resolution is for DISPATCHERS with access to the VisiCAD application.

(a) In the VisiCAD Unit Queue, right click and from the menu select, “Roster System.”

(b) Highlight the person under “Assigned Personnel” and select the “Temporary Portable Radios” tab.

(c) Select “Delete” and you will be presented with a box that asks if you are sure you want to remove XXXX from this shift?

(d) Select “Yes”

(e) Next, you will be presented with a box that states who the radio is assigned to. It will state that, “Deleting the radio would remove the assignment. Would you like to continue?”

(f) Select “Yes”

(g) Highlight the person and hit, “Off Duty.”

(h) Then, click the “Save” button and then click the “Exit” button. This will close out the Roster program.

(i) Note: Changes in the CAD system can take up to a minute to affect CAD SignOn and there is no visible notification that the changes have taken place except that the radio ID is now available for assignment.

(j) Test the solution by assigning the radio.

7.2 If none of the solutions resolve the problem, create a help desk ticket and make sure to include the following details:

(a) Which Unit and Person are trying to assign the radio?

(b) Which Radio ID is it?

(c) Which Unit and Person does the system tell you it belongs to?

(d) Verify you have the correct radio ID.

STANDARD OPERATING PROCEDURES

No. 505 SPECIAL EVENTS LOG IN

POLICY:

It shall be the policy of the Fire Alarm Center to adhere to the following procedures for Special Event log in.

SEE ALSO: SFD Dispatch #18-10, New CAD Sign-On Application
SOP No. 511 (Task Force Log-On/Log-Off)
SOP No. 502 (CAD Sign-On)

1.0 GENERAL

1.1 The Fire Alarm Center will receive the Event Action Plan for the Event:

(a) The location or Command Post Address must be given.

(b) The event must be named such as "**SAFECO FIELD**"

(c) Units will be named as follows: *EVENT1, EVENT2, E384, A83*, etc.

2.0 LOGGING APPROPRIATE EVENT UNITS INTO CAD

2.1 Use Powerline to log-on the appropriate EVENT units and apparatus into CAD.

(a) Locate above logged unit(s) using the following procedures:

(1) Poke yourself in the eye
(2) Select "**All**"
(3) Scroll down to appropriate unit
(4) Right click on located unit
(5) From the drop down menu, select "**Roster System**"
(6) Ensure the "**Extended Shift**" box is checked
(7) Save the changes

2.2 Open the Call Taking Screen:

(a) Enter the address of the event location or command post
(b) Enter the event name in the location field, i.e. "**Safeco Field**"
(c) Choose the "**EVENT – Special Event**" type code.
(d) Expand the call taking screen (Vente Tab)
(e) Choose the Additional Information tab

(f) Change the Division to "**ADVISED**"
(g) Save and exit out of this screen

2.3 Poke yourself in the eye and select the "**ADVISED**" division to view incident.

3.0 FOLLOW-UP PROCEDURES

3.1 Coordinate with the Event Lead to ensure all people have logged onto the appropriate event/events and/or apparatus.

4.0 DISPATCHING SPECIAL EVENTS

4.1 From Powerline, dispatch the required units and put them on scene, as appropriate. *For example, "**D_EVENT1 ###**" (the Incident Number is (###).*

5.0 CHANGE OF EVENT PERSONNEL

5.1 If personnel are changed or added on a selected EVENT unit, they must be removed from the EVENT and then reassigned. After the EVENT has been reassigned, the changes will be represented in CADView.

5.2 Once changes are made, they should be confirmed in CADView:

(a) Click on the "**CADView**" icon on the desktop
(b) Under "Incidents," go to "**Advanced Incident Search**"
(c) Choose "EVENT – Special Event" under the "**Final Incident Type**"
(d) Make sure the "**Active Incidents**" box is checked.
(e) Click on the "**Show**" box.
(f) Confirm that appropriate personnel are logged into assigned event

6.0 EVENT CLOSURE/LOGGING OFF EVENT

6.1 When the EVENT is completed and goes off the air, OPS personnel should remove themselves from the incident using the following procedures:

(a) Click on the "**CAD Sign On**" icon on the desktop
(b) Choose the appropriate EVENT
(c) Clear Employees and Clear Radios
(d) Submit request

7.0 RADIO SIGN-ON ASSISTANCE FOR OPERATIONS

7.1 In order to maintain proper software communication and integrity, signing on to units and radios shall be done through CAD Sign-On (and not by VisiCAD).

7.2 Operations personnel are responsible for using CAD Sign-On to assign themselves to

the appropriate Special Event.

7.3 The following procedures should be implemented in case the FAC must assist OPS personnel when they are having difficulty using CAD Sign-On and assigning portable radios.

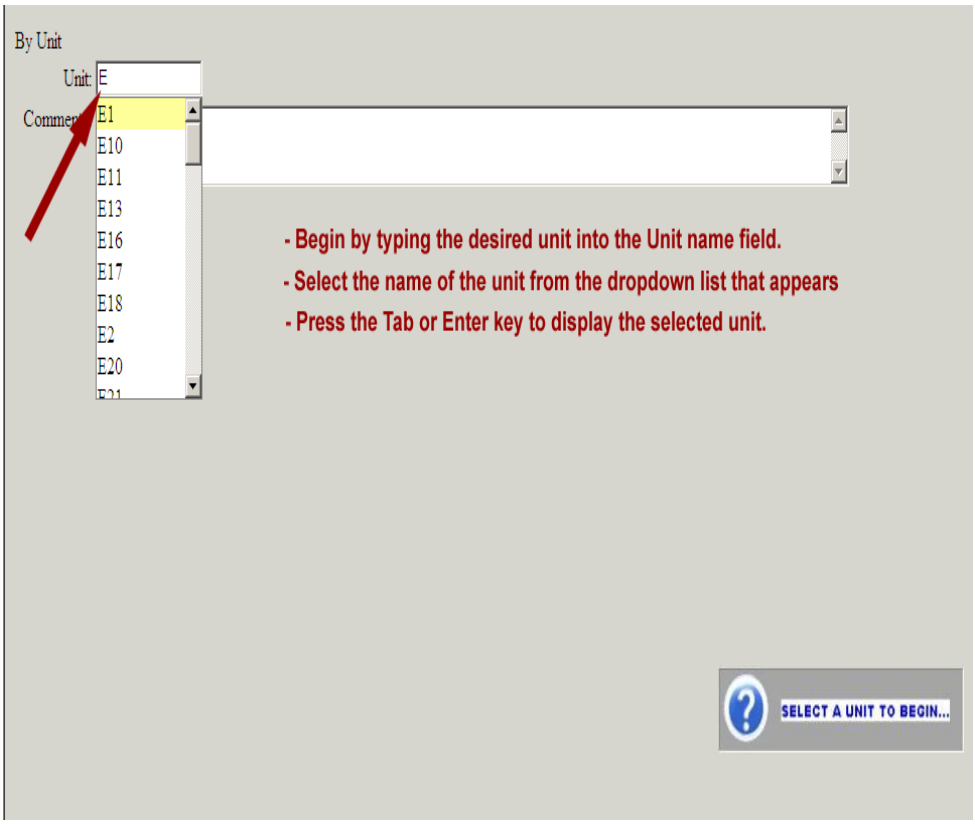
(a) USING CAD SIGN-ON

(1) Double click on the CAD Sign-On icon located on the desktop.

(2) CAD Sign-On no longer requires the user to login with a username and password.

(3) Begin by typing the name of the unit you will be logging on to *(See Figure 1)*. Select the desired unit and hit the *Tab* or *Enter* key to display the selected unit.

FIGURE 1

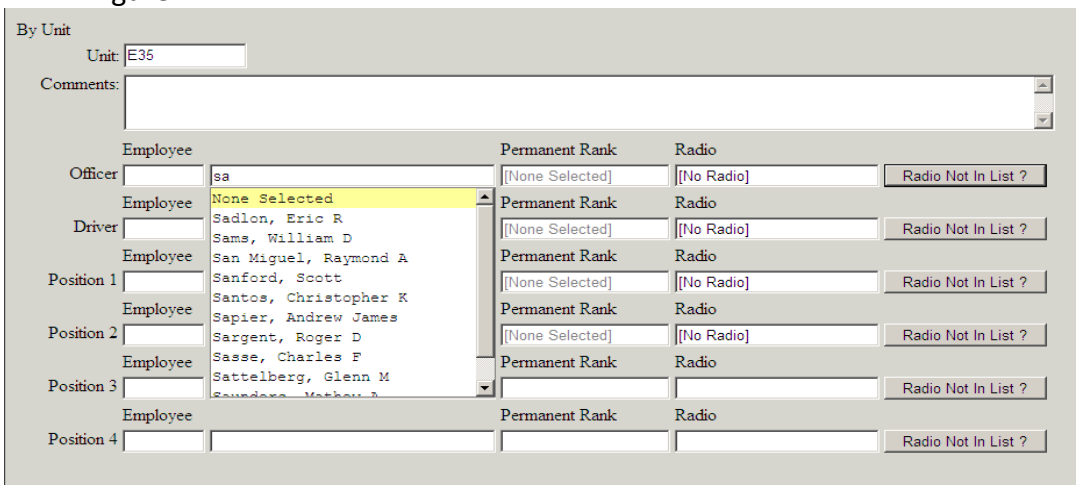


(b) ENTERING CREW MEMBERS INTO UNIT POSITIONS

(1) Enter shift officer or crew members into the appropriate unit positions on the selected unit in the same manner that was used in the previous version of CAD Sign-On.

(2) Unit positions can be filled by entering a member's Injury/Illness number or by beginning to type the member's last name and then selecting the appropriate name from the dropdown list that appears. (*See Figure 2)*

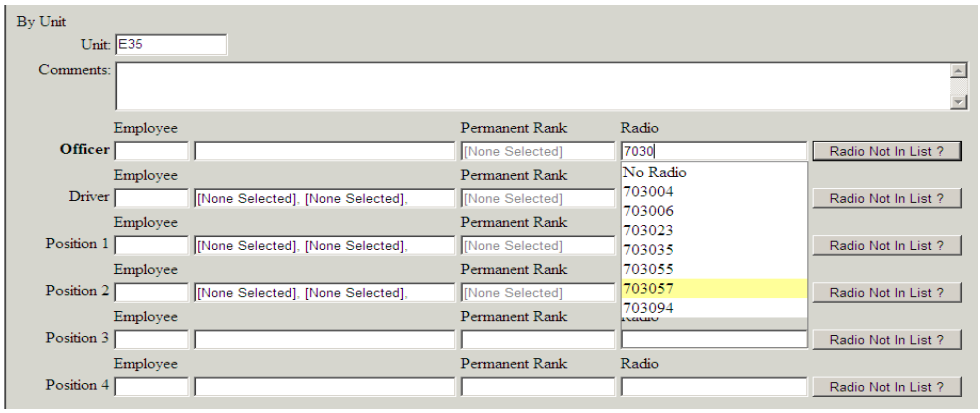
Figure 2



(c) ENTERING RADIOS INTO UNIT POSITIONS

(1) Enter radio numbers into each unit position in the same manner as the previous version of CAD Sign-On. Begin typing the radio number and a dropdown list will appear with all possible matches. Select the desired radio from the list. *(See Figure 3)*

Figure 3


By Unit
Unit: E35
Comments:
Employee
Permanent Rank
Radio
Officer
[None Selected]
7030
Radio Not In List ?
Driver
[None Selected], [None Selected],
Position 1
Position 2
Position 3
Position 4
No Radio
703004
703006
703023
703035
703055
703057
703094

(d) ASSIGNING RADIO(S) TO A UNIT WITHOUT A MEMBER

(1) There are times when it is necessary to assign a radio to a position on a unit without assigning a Member to that position. Follow these steps:

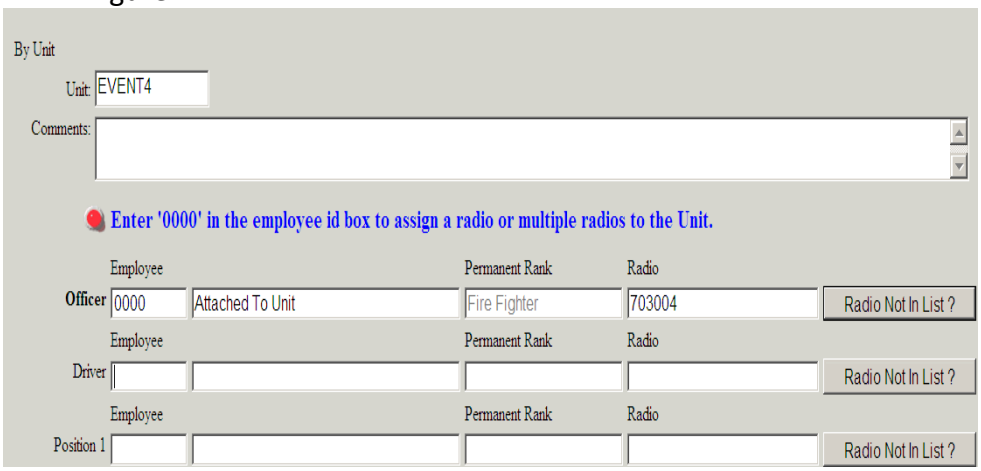
a. In the position you want to assign a radio to, type "0000" as the Employee ID number and press the tab key.

b. In the Employee Name field the words "Attached to Unit" will appear.

c. Tab over to the Radio ID field and enter the radio you wish to assign.

d. Submit your changes. *(See Figure 4)*

Figure 4



8.0 ERROR MESSAGE SOLUTION <u>NUMBER 1</u> FOR OPERATIONS

8.1 A radio cannot be assigned to more than one apparatus position as CAD Sign-On only allows a radio to be assigned to one position on one unit. .

(a) When you click the submit button to send your sign-on information to CAD, <u>if any of the radio numbers</u> you are trying to submit are already currently assigned to a position on a different unit, you will see a message appear in the message box area at the bottom of the screen informing you which radio number is the problem and which unit, position and member the radio is currently assigned to.

8.2 If Operations personnel are attempting to assign a radio to a position in an EVENT and they find the error message, *"The selected radio (XXXX, EVENT) is already assigned to a position on the current apparatus*. Either pick another radio or un-assign the radio from Position first if you want to assign this radio, direct Operations personnel as follows:

(e) Verify that this member is no longer using the radio. **THIS IS VERY IMPORTANT.**

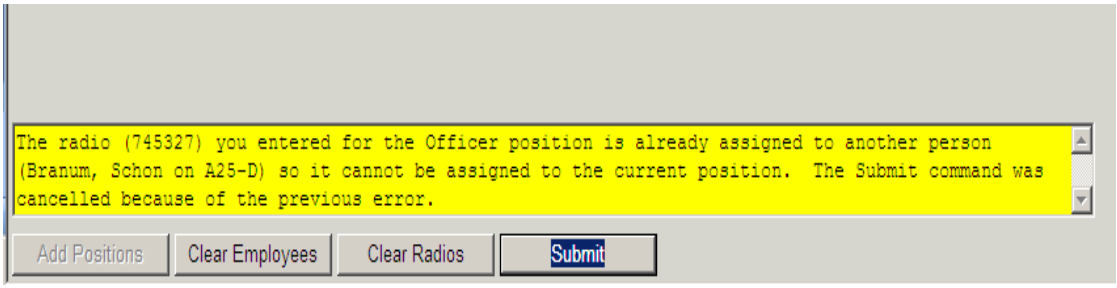
(f) Select the Unit from the "**Unit**" pull-down menu on the FDM Sign-On screen.

(g) At the position listed in the error noted above, set the radio to "**No Radio**" and press **SUBMIT** at the bottom. The "No Radio" selection is at the top of the radio list.

(h) Test the solution by trying to use the radio for the place or person where you would like it to be assigned.

9.0 ERROR MESSAGE SOLUTION NUMBER 2 FOR OPERATIONS

9.1 If Operations personnel are still attempting to assign a radio to a position in an EVENT and the following error message appears:



(a) Re-submit or call SFD MIS Help Desk with the exact error message, direct Operations personnel as follows:

(1) Verify that this person is no longer using the radio. **THIS IS VERY IMPORTANT**.

(2) Select the Unit from the "**Unit**" pulldown menu on the FDM Sign-On screen.

(3) At the position listed in error noted above, sign onto using your injury/illness number and using the radio listed in the error message.

- Press the **SUBMIT** button.
  - After submitting, return to that position and set the radio to "No Radio." The "No Radio" selection is at the top of the radio list.
- Hit the **SUBMIT** button.

(4) Test the solution by trying to use the radio for the place or person where you would like it to be assigned.

(5) If the radio is still not assigning to the proper position, see 10.0 below.

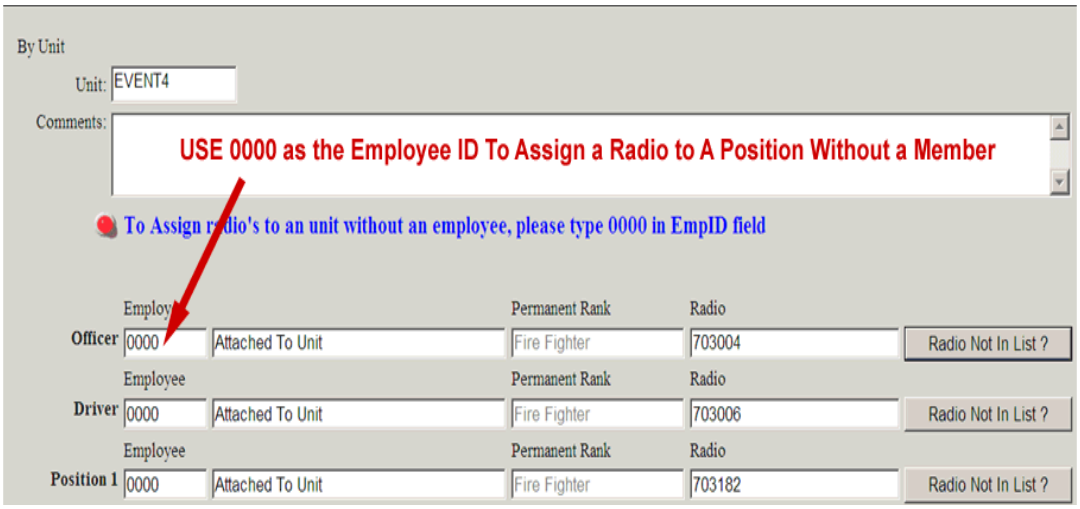
10.0 ERROR MESSAGE SOLUTION NUMBER 3 FOR OPERATIONS

10.1 Radio disappears when a member is NOT assigned to the Position

(a) If a radio is assigned to a position on a unit but a member is not also assigned to that position, the selected radio will disappear from the unit. Sign-On does not allow a radio to be assigned to a position on a unit without an Employee ID assigned.

(b) To assign a radio to a position without a Member, enter "0000" as the Employee ID and hit the tab key. The words "**Spare Radio**" previously listed as "Attached to Unit" will appear in the Employee Name field. Next,

enter the desired Radio ID. Submit the changes. The radio is now assigned to the desired position without an Employee assigned to the position. (See Figure 6B)



(c) It is acceptable though to assign a member to a position on a unit and not assign that member a radio. This happens very infrequently when the member is a recruit/trainee, FAC, or other who is on a rig but doesn't have a radio.

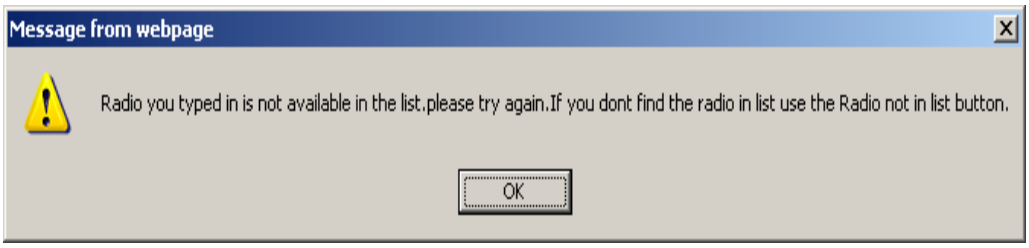
11.0 ERROR MESSAGE SOLUTION NUMBER 4 FOR OPERATIONS

11.1 Radio number does not appear in the Radio Dropdown list:

(a) The Radio Dropdown list is populated with valid portable radio numbers from the Department's inventory tracking system. A valid portable radio is a radio that begins with the prefix of 703 or 745 and falls within a minimum and maximum range for each of those prefixes per valid radio ranges recorded into the CAD system itself.

(b) It is possible, although a rare occurrence, that a member can have physical possession of a radio does not appear in the radio dropdown list.

(c) In this case, CAD Sign-On will recognize that the radio number the member is entering is invalid and will display a pop-up message to the user informing them that the radio is not in the valid radio list.


Message from webpage
Radio you typed in is not available in the list.please try again.If you dont find the radio in list use the Radio not in list button.
OK

(d) Click the OK button to clear the message and then do the following:

(1) Double check that you are correctly typing in the radio number of the radio you physically have in your possession. If you are sure you're trying to enter the correct number then go to step 2.

(2) Click the *Radio Not In List?* Button. An input box will appear as shown in Figures 8A, 8B and 8C below.

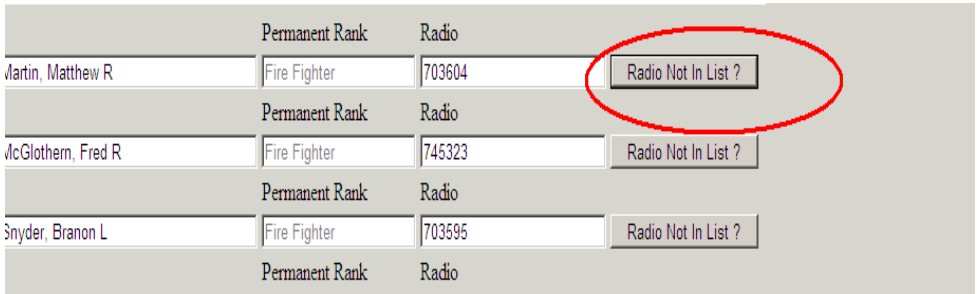
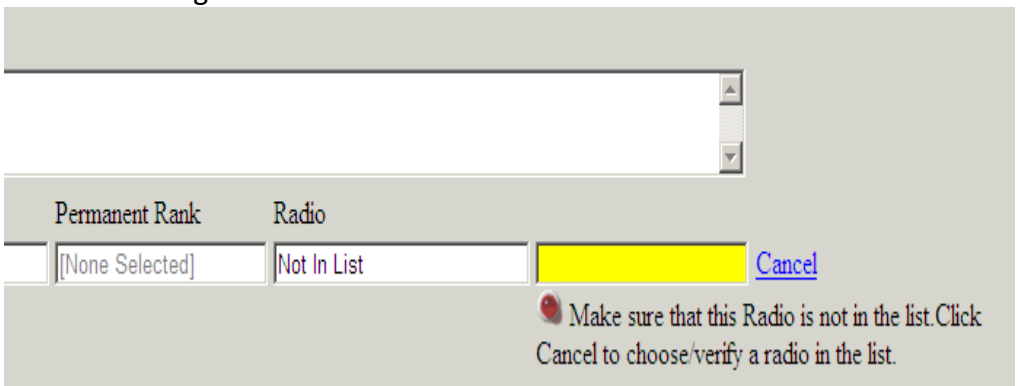
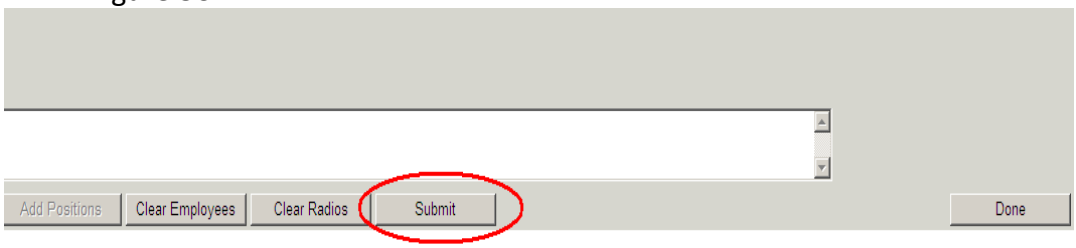


Figure 8B



(e) Type the radio number into the radio input box. When finished filling out the Sign-On form for the selected unit, click the Submit button to submit the sign-on(s).

Figure 8C



(f) Clicking the Submit button at this point will allow the user to assign the radio to the desired position and member.

- An email is then generated by the CAD Sign-On application and sent to the FAC On-Duty Shift Officer alerting them that a radio has been assigned to a unit, position and member that is not listed in the valid radio dropdown list.

- The FAC On-Duty Shift Officer will follow up by adding the radio to the list or contacting the member for more information.

12.0 ERROR MESSAGE SOLUTION NUMBER 5 FOR FAC

12.1 This resolution is for DISPATCHERS with access to the VisiCAD application.

(k) In the VisiCAD Unit Queue, right click and from the menu select, "Roster System."

(l) Highlight the person under "Assigned Personnel" and select the "Temporary Portable Radios" tab.

(m) Select "Delete" and you will be presented with a box that asks if you are sure you want to remove XXXX from this shift?

(n) Select "Yes."

(o) Next, you will be presented with a box that states who the radio is assigned to. It will state that, "Deleting the radio would remove the assignment. Would you like to continue?"

(p) Select "Yes."

(q) Highlight the person and hit, "Off Duty."

(r) Then, click the "Save" button and then click the "Exit" button. This will close out the Roster program.

(s) Note: Changes in the CAD system can take up to a minute to affect CAD Sign-On and there is no visible notification that the changes have taken place except that the radio ID is now available for assignment.

(t) Test the solution by assigning the radio.

12.2 If none of the solutions resolve the problem, create a help desk ticket and make sure to include the following details:

(a) Which Unit and Person are trying to assign the radio?

(b) Which Radio ID is it?

(c) Which Unit and Person does the system tell you it belongs to?

(d) Verify you have the correct radio ID.

STANDARD OPERATING PROCEDURES

No. 509 RIG SWAP – CHANGE OF APPARATUS

POLICY:
It shall be the policy of the Fire Alarm Center to adhere to the following procedure when putting spare units on and off duty.

SEE ALSO: SOP No. 511 (Task Force Log On/Log Off)

1.0 RIG SWAP – CHANGE OF APPARATUS

1.1 Use the following procedure for a Rig Swap:

(a) **Step 1**

(1) Obtain the apparatus number (Vehicle ID#) that the unit is going to be swapping into (e.g., E5404, M3760).

(b) **Step 2**

(1) Within the **POWERLINE** place the unit **AIQ** (e.g., AIQ_E10).

(c) **Step 3**

(1) R-click on the unit in the **UNIT STATUS** queue and choose **CHANGE VEHICLE** from the drop-down menu.

(2) Enter the new apparatus number (Vehicle ID#) in the **NEW VEHICLE ID** field, (e.g., E5404, M3760).

- Write down the old apparatus number from the top of the Change Vehicle page then tab off.

(3) Select **OK**.

(d) **Step 4**

(1) Within the **UNIT STATUS** queue place the unit **AOR**, then **AIQ** (e.g., AOR_E10). *Note: If the unit was available on air at the time of the rig swap, place the unit AOR again.*

(2) Verify in the Unit Status queue that the unit is AIQ in the proper

station. Sometimes the system may pick the station nearest to their location at the time of the swap.

1.2 After completion of the Change Vehicle:

(a) Open the tool box and open the vehicle manager. At the bottom left of the page in the Name box, enter the old apparatus number then click the search box.

(b) The old apparatus Number should appear in the box next to the Name box. *Double click the old number and the box with the Vehicle ID will open.* The old number should be at the top under Vehicle ID.

(c) Now type in or select from the drop down in the Unit Name box the old number and click the Save button at the bottom of the page.

(d) Now the Vehicle ID and the Unit Name should match.

(e) Never change the Vehicle ID. You are now finished.

STANDARD OPERATING PROCEDURES

No. 510 CREATING NEW UNITS IN CAD

POLICY:

It shall be the policy of the Fire Alarm Center to adhere to the following procedures when creating new units in CAD

SEE ALSO: SOP No. 511 (Task Force Log On/Log Off)

1.0 GENERAL

1.1 Administrator privileges are needed to create new units in CAD. All FAC floor officers have administrative privileges, providing access to all utilities and other programs in the toolbox.

1.2 Members creating new units should refer to units already existing in CAD to see which fields need to be completed.

2.0 PROCEDURE

2.1 Use the following procedure to create a new unit in CAD:

(1) Open the Tools menu

(2) Open the Pop Up Utility List

(3) Open the Units Names Utility

(4) Add the Unit Name (code and name are the same)-(example, **HAZVAN, E34**)

(5) Add the Unit ID (code and name are the same)-(example, **3360, E5310, M3645**)

(6) Open Vehicle Manager

(7) Click Add

(8) Enter Vehicle Id (**E5310, M3770**…)

(9) Enter Unit Name (**HAZVAN, E34**…)

(10) Complete all the other fields including Sharing

(11) Click on SAVE before exiting

(12) From Powerline, change units division to correct division
(13) Put unit AOR then AIQ

STANDARD OPERATING PROCEDURES

No. 511 TASK FORCE LOG-ON/LOG-OFF

POLICY:

It shall be the policy of the Fire Alarm Center to adhere to the following procedures when logging task forces on or off in CAD

SEE ALSO: SOP No. 512 (Putting Spare Units On Duty)

1.0 TASK FORCE LOG ON PROCEDURE

1.1 Use the following procedure to log on a task force in CAD:

(1) Open vehicle manager.
(2) Search for "TF". This will return a list of Task Force units 1-10
(3) Double click on the unit you want to use.
(4) Change the Home station to the station where the Task for unit will be located.
(5) Change the Primary Resource Type to the correct type *(Engine, Ladder, Aid, Medic)*
(6) Change the Secondary Resource Type to the correct type *(EMS RES ENG LAD and EMS RES ENG LAD AID for engines and ladders, EMS RES ENG LAD AID for aid cars, nothing for other units)*
(7) Save your changes and Exit vehicle manager.
(8) From the Powerline, Log On the unit (L_TF1)
(9) From the Powerline, AOR then AIQ the unit.

1.2 CAD will recommend the correct units for responses. Task force units have NO AVL's so you need to put them AIQ after each response.

2.0 TASK FORCE LOG OFF PROCEDURE

2.1 Use the following procedure to log off a task force in CAD:

(1) Put the unit AIQ.
(2) Open vehicle manager and search for the unit you want to log off.

(3) Double click on the unit name.
(4) Change the Home station back to “Vehicle”.
(5) Change the Primary resource type back to “Non Unit”.
(6) Remove all the secondary resource types.
(7) Save your changes and Exit vehicle manager.
(8) From the Powerline, put the unit AOR then AIQ.
(9) From the Powerline, Log Off the unit. (LO TF1)

STANDARD OPERATING PROCEDURES

No. 512 PUTTING SPARE UNITS ON/OFF DUTY

POLICY:

It shall be the policy of the Fire Alarm Center to adhere to the following procedure when putting spare units on and off duty.

SEE ALSO: SOP No. 511 (Task Force Log On/Log Off)

1.0 PUTTING SPARE UNITS ON DUTY

1.1 Use the following procedure put a spare unit on duty in CAD:

(a) **Step 1**

(1) Obtain the Vehicle ID# for the apparatus that is going to be used (e.g., E5404, M3760).

(2) Obtain the radio designator (Unit Name) that the unit is going to use (e.g., E80, A85).

(b) **Step 2**

(1) Within the Vehicle Manager tool, search for and select the appropriate vehicle (e.g., E5404, M3760).

(2) From the Vehicle Information and Assignments (tab 1*)*, change the Home Station to the appropriate one.

(3) Change the **UNIT NAME** to the appropriate radio designator (e.g., E80, A85).

(4) Verify the unit's Primary Resource Type is correct (e.g., Engine, Aid Car, etc.).

(5) Verify the unit's Secondary Resource Type is correct:

- Engine & Ladder – EMS RES ENG LAD & EMS RES ENG LAD AID
- Aid Car – EMS RES ENG LAD AID

- Medics – (none)

(6) Select the Capabilities and Staffing (tab 2), verify that engine and ladder Capabilities indicate Fire Unit-Engine or Ladder.

(7) Select the Sharing (tab 4), and verify all Jurisdictions and all Divisions are selected.

(8) Select the Paging (tab 5), and add any Pagers and Paging Groups if necessary.

(9) Save changes and Exit.

(c) **Step 3**

(1) **Log-On** the unit (e.g., "L_E80").

(d) **Step 4**

(1) Within the Unit Status queue, R-click on the unit and place it both AOR, then AIQ.

(2) Within the Unit Status queue, R-click on the unit and select Roster System from the drop down menu. Check ☑ the Extended Shift box.

(3) Notify the company to roster on to the unit with their appropriate radio numbers.

2.0 PUTTING SPARE UNITS OFF DUTY

2.1 Use the following procedure to put a spare unit off duty in CAD:

(a) **Step 1**

(1) Place the unit **AIQ** (e.g., AIQ_E80).

(2) **Log Off** the unit (e.g., "LO E80, A85").

(b) **Step 2**

(1) Within the Vehicle Manager tool, search for and select the unit (e.g., E80, A85).

(2) From the Vehicle Information & Assignments (tab 1), change the unit's Home Station back to Vehicle.

(3) Change the Unit Name back to match the Vehicle ID# (e.g., E5404, M3760).

(4) Change the unit's Primary Resource Type to Non-Unit.

(5) Select the Paging (tab 5), remove any Pagers and Paging Groups.

(6) Save changes and Exit.

STANDARD OPERATING PROCEDURES

No. 513 ROAD NETWORK MANAGEMENT UTILITY

POLICY:

It shall be the policy of the Fire Alarm Center to adhere to the following procedures when altering the CAD road network to reflect street and bridge closures.

1.0 CLOSING A ROAD SEGMENT

1.1 Use the following procedure to create a Road Impedance for travel re-routing:

(1) In VisiCAD Tools, select **Road Network Management Utility**

(2) Click Add.

(3) Enter a designator in the Name field (**Use the street name**)

(4) Enter 0 or 1 mph in the Edited Speed field (**0 for bridges and 1 for everything else**.)

(5) Enter a Start Date and Time in the appropriate field (**time must be in the future**.)

(6) Enter an End Date and Time in the appropriate field if appropriate.

(7) Locate and zoom in on the map to the section of roadway to be closed **Ctrl+Left click** on the section of road way to be closed (this will highlight it in yellow)

(8) Select Save.

1.2 Verify that the re-routing is working properly by using the following procedure:

(1) In VisiCAD Explorer, select: **Tools, Show Directions**

(2) Locate and zoom in on the map to the section of roadway that has been closed

(3) Left click on a section of street on opposite sides of the section of closed

roadway and the long/lat will show in the Routing Directions window.

(4) Select: Directions

(5) A window of Directions will pop up. Read through the directions and verify that the route of travel bypasses the closed section of roadway.

2.0 RE-OPENING A ROAD SEGMENT

2.1 To delete a Road Impedance closure, use the following procedure:

(1) In VisiCAD Tools, select **Road Network Management Utility**

(2) Select: **Edit**

(3) Enter an * in the Search String field and select Search

(4) A list of created road impedances will show in the window. Left click to highlight the desired one and select OK

(5) Select the Delete (if an End date was entered it will delete on its own)

STANDARD OPERATING PROCEDURES

No. 520 CREATING A NEW TYPE CODE

POLICY:
It shall be the policy of the Fire Alarm Center to adhere to the following procedures when creating new type codes in CAD.

1.0 GENERAL

1.1 You must have Administrator Privileges to create type codes in CAD.

1.2 It would be a very unusual circumstance in which a type code would need to be created by someone who does not normally do so. In most cases, it is best to put off creating a new type code until an experience CAD administrator is available.

2.0 TYPE CODE CREATION PROCEDURE

2.1 Use the following procedures to create a new type code in CAD:

(a) Open the Tools menu.

(b) Open the Popup List Utility.

(c) Select “Incident Types”.

(d) Click “ADD’.

(e) Enter the new code. (HAZRA) - (5 char. Max, all caps)

(f) Enter a description. (HAZRAD – Hazmat Radiation)

(g) Click “SAVE” and “EXIT”.

(h) Open the Tools menu.

(i) Open the Response Plan Manager.

(j) Under “‘Plans on File”, Select plus next to Seattle, Seattle.

(k) Click “ADD” plan.

(l) Enter the new plan name. (HAZRAD – Hazmat Radiation, use new incident type-description)

(m) Select Dispatch Level of (Normal).

(n) Tab off dispatch level and click SAVE.

(o) Under 'Plans on file-Seattle', select the new incident type, click the '+' next to the incident type and select alarm level 1.

(p) Click Add detail.

(q) Select the resource or capability you want to use.(select order)

(r) Tab off and click SAVE.

(s) Click Add detail and repeat 17 & 18 if you want more units.

(t) Exit Response Plan Manager

(u) Open the Tools menu.

(v) Open the Problem Incident Subtype Utility.

(w) Click ADD.

(x) Enter the code. (HAZRAD) - (same as the new incident type)

(y) Enter the description, (HAZRAD – Hazmat Radiation) - (same as response plan. "Code-description")

(z) Select Priority.

(aa) Select Cert. Assignment.(You need to select the blank field)

(bb) Select Incident Type Description.

(cc) Check the Radius Search box and enter radius in the gray box if needed. (.5 for Hazmat)

(dd) Click SAVE & EXIT

(ee) Open the Tools Menu.

(ff) Open the Response Area Builder.

(gg) Select the plus next to Seattle, Battalion 2, Battalion 2, Battalion 2.

(hh) Select Response Plan Tab.

(ii) Click ADD.

(jj) Select new Incident type.

(kk) Select the associated plan.

(ll) Click SAVE.

(mm) Select the Area List.

(nn) Repeat steps 32 – 38 for each battalion.

(oo) Exit Response Area Builder.

(pp) Restart CAD

(qq) Open the Response Area Builder.

(rr) Select the plus next to Seattle, Seattle.

(ss) Select the plus next to Battalion 2, Battalion 2 then Battalion 2 folder

(tt) Click on the Response Plans tab

(uu) Scroll down to the new type code and make sure there is a "Plus" next to the new type code in the list. (If not you need to repeat steps 31- 38 again for each missing code.

(vv) Click the Area List and repeat steps 42 -45 for each battalion.

(ww) Exit Response area builder.

(xx) Create a test incident in each battalion to make sure the proper units are recommended.

(yy) Notify MIS that you have created a new Incident Type and Response Plan.

STANDARD OPERATING PROCEDURES

No. 521 STATION UNIT ROTATION

POLICY:
It shall be the policy of the Fire Alarm Center to adhere to the following procedures when rotationing units at the same station in CAD

1.0 GENERAL

1.1 This procedure shall be used anytime upstaffing occurs in Operations and the same type of unit at the same station is placed into service. For example: Aid 14 and Aid 84.

2.0 STATION UNIT ROTATION PROCEDURE

2.1 Use the following procedure to rotate units in CAD:

(1) Open Vehicle Manager in Tool Box menu.

(2) Go to Dispatcher Rules setup utility.

(3) Click Unit Selection Modifier tab

(4) Click station of rotating unit.

(5) Click Enable Altering Unit order

(6) Click responding.

(7) Click SAVE

STANDARD OPERATING PROCEDURES

No. 530 UPGRADES TO CAD

POLICY:
It shall be the policy of the Fire Alarm Center to adhere to the following procedures following upgrades to CAD.

1.0 GENERAL

1.1 Following any upgrade to CAD (new version, service pack, patch, etc.), the floor officer shall ensure that the Post Upgrade Check Off list is completed as soon as possible and forwarded to **ALARM2**.

2.0 REFERENCE:

DISPATCHER CHECK OFF LIST "After up grades"	
1. Check Locution interface _____ a. Dispatch a run and make sure location fires. Radio ____ b. Station ____	**8. Check Polygone Look-Up_____** a. Verify we get a map page number ___
2. Check PTT interface _____ a. Try different radios from PTT ____	**9. Check Address validation_____** a. Verify caution notes ____ b. Verify address history ____
3. Check Paging interface _____ a. Personnel ____ b. Unit ____ c. Incident ____	**10. Check MUM _____** a. Verify MUM receives CAD updates ____
4. Check AVL interface _____ a. Verify unit position is updating ____ b. Verify we receive unit status changes ___	**11. Check CAD View application_____**
5. Check MDC interface _____ a. Verify unit receives incident data ____ b. Verify MDC emergency button works ____	**12. Check EMD application _____** a. Verify application works ____ b. Verify type code is transferred over to CAD ____
6. Check Emergency Button_____ a. Verify a portable radio emergency button works ____	**13. Check closed record download ___** a. Check with MIS to verify incident transfer ____
7. Check Ani /Ali interface_____ a. Verify we transfer ani/ali over to CAD ____	**14. Check history search _____**

STANDARD OPERATING PROCEDURES

No. 535 CAD COMMANDS

POLICY:

It shall be the policy of the Fire Alarm Center to adhere to the following procedures when using Powerline Commands.

1.0 GENERAL

command	*description*	*example*	*explanation*
A	Assist unit to incident	A_L3_123	Add unit to an Incident (same as "D" command)
AIQ	Available in Quarters		
AORA	AOR All	AORA_E6_E6/L3/B5 or AORA_.123_E6/L3	Separate units remaining on the run with slashes
AR	Add Resource	AR_A5_L AR_.123_L	Recommends closest avail resource
AUT	Activate User Timer	AUT_DEP1_1500	Sets user timer (1500 = 15 min)
BALB	Balance a bunch	BALB_E6_2L/1E BALB_.123_2L/1E	Add resource(s) with the recall screen. ***Use when IC requests multiple units***
BALT	Balance Incident by Type Code	BALT_E6_MED BALT_.123_MED	Function key F9 inserts "BALT" on the powerline. Reconfigures response units.
BROST	Shows Battalion Roster	BROST_BAT5	This command brings up the Battalion roster. It looks confusing because of the way we do unit rosters but active personnel are the listed with assigned positions, i.e., P1, P2, D, O
CAN	Incident Cancellation		Use this command to cancel incident when response is cancelled prior to arrival
CARD	Cardfile Search	CARD_ANIMAL CONTROL	Search rolodex card file for any text

CIM	Critical Incident Mode	CIM_E5_M	Dedicates powerline to the incident. The "M" allows you to type comments that go directly into the call mask. ***Use for fire & rescue incidents.***
CUT	Clear User Timer	CUT_DEP1	Clears user timer

command	description	example	explanation
D	Dispatches Unit to Active Incident	D_E6,L3_123	Same as "A" command
DE	Dispatch Unit Enroute	DE_E6_123 (No Locution)	This command lets you dispatch a unit On-Scene to an ACTIVE incident. This command does not fire Locution or the Pagers Use when an AOR aid car offers to take a run for the engine
DL	Set Dispatch Level		In a situation where resources are scarce (wind storm, earthquake, multiple alarm fire, etc.), the officer may change the dispatch level to reduce the # of resources required.
DO	Dispatch Unit On Scene	DO_E6_123 (no Locution)	This command lets you dispatch a unit On-Scene to an ACTIVE incident. This command does not fire Locution or the Pagers. ***Use when a unit accidentally takes themselves off an incident -- places them back on the incident WITHOUT Locution or pagers going off.***
DU	Dispatch unit	DU_E6_123	This command lets you dispatch a unit to an ACTIVE incident with locution.
ER	Enroute	ER_MAR5	Unit Responding. ***Use for units without MDC's (i.e. MAR5, AIR9)***
ETP	Enroute to post. Places unit Enroute to station after move ups.	ETP_E6	This command places the unit Enroute to Post after you do a move up, if they forget to do it or they don't have a MDC.
FMP	Find members page by name	FMP_Smith	This command will tell you what pagers are assigned to a member by their name.
FP	Find pager by pager ID	FP_345	This command will let you look to see who has a pager using the pager ID.
FPG	Find pager group members by page group ID	FPG_01	This command will let you see who is in a certain page group. You have to use the page group code, i.e., STAFF.

command	*description*	*example*	*explanation*
FR	Find Radio	FR_70###	
FU	Find Unit	FU_E6	Use to highlight unit on the unit status queue. ***Use when company asks for their status.***
IH	Incident History by unit ID	IH_A5	Opens call mask for active incident for selected unit.
IN	Removes all out of service reasons	IN_B6	
L	Log unit onto CAD		***Use when placing spare units and/or task forces in service.*** See SOP 511 & 512 for procedures.
LO	Log Unit off CAD		***Use when placing spare units and/or task forces in service.*** See SOP 511 & 512 for procedures
M	Add Comments	M_123_A5	Use to add comments to an incident
MAPI	Map Displays Incident	MAPI_123	Zooms map to Incident Location
MAPU	Map will display unit	MAPU_E6	Zooms map to unit location
MOV	Move-up Companies	MOV_E6/25, L3/14,E5/10	
MOVD	Recall Move-Up Unit(s)	MOVD	Lists all moved up companies
MOVX	Cancel Move-Up Units	MOVX_E6,L3,E10	
MU	Add comments to Unit activity log	MU_E6_Test comment	This command lets you add comments to a Unit Activity log. It is not incident related.
OS	Unit On-Scene		
OUT	Unit Out of Service		Out of Service/Conditional Availability
PGT	Page Units		
PS	Powerline Search	PS_CIM	Search Powerline for limited CAD Command information
R	Recall Incident	R_A5	Brings up Incident Recall screen

command	*description*	*example*	*explanation*
RA	Re-assign a unit to a different incident or re-assign an incident	RA_.123 (to replace all units…drops it back into the pending queue for reassignment)	If you send a response with the wrong units, this command will clear all the units and place the incident back in the waiting incident window. *Use for a corrected address in a different part of the city or if a freeway response changes from NB to SB*
RADIO	VisiCAD, show default SOP	RADIO	Displays portable radio template
RD	Recall incident data and time stamps.	RD_E5 RD_.123	This command will Recall the Data fields and Time stamps for an incident in a Recall window.
RI	Resource Information. (Show available(A) Units by resource type): **E**- Engines **L**- Ladders **A**-Aid Cars **M**-Medics	RI_,A,E	This command lets you see all the available units by type of unit. Don't forget to use the commas in the right places as shown. The "A" stands for Available units.
RLINK	Removes incident links	RLINK_123_ 345	This command removes links that were created between incidents. *Use if you linked incidents that are then determined to be unrelated.*
ROST	Recall unit roster	ROST_E6	This command looks confusing because of the way we do unit rosters but active personnel are the listed with assigned positions, i.e., P1, P2, D, O.
RUT	Reset Unit Timer	RUT_DEP1_1500	This example puts an additional 15 min on the timer for DEP1.
SM	Send message by user ID	SM 1139 H,N,Subject, message (H = High, N=Normal)	This command let you send a mail message to someone using their injury/illness number. The "H" signifies High priority message and the "N" is for Normal sensitivity

command	*description*	*example*	*explanation*
SMW	Send message by workstation	SMW D101 H,N,Subject, message (H = High, N=Normal)	This command allows you to send a mail message to someone using the dispatch workstation number. Use a "D" and the position number. They all start with 10. SO position 4 would be D104. The "H" signifies High priority message and the "N" is for Normal sensitivity
ST	Puts unit in the Staged status.	ST_E6	This command places the unit in the Staged status. This command is used when a unit tells you they are "Standing By" for SPD.
STACK	Stacks a waiting incident for a unit for later dispatch	STACK_E6_ 123	This command will Stack incidents for a unit. *This would be handy during a storm when you want a unit to handle several incidents in their area.* The command places the incident in the Active incident queue with an "S" next to the incident ID. When the unit that the incident is stacked for goes in service, a high priority messages is sent to all positions telling them the unit is available for the next incident. The dispatch has to dispatch them on the next incident.
TR	Transporting	TR_Unit/Hospital	See Rolodex or flip cards for hospital codes (or use cmd "CARD HOSPITAL")
TRC	Transport Complete	TRC_M1	End of medical transport, Unit at destination
UH	View Unit History	UH_A5	Shows unit history
XCIM	Cancel Critical Incident Mode	XCIM	*Use when a fire or rescue is complete*

Fire Department

Probationary Firefighter Development Guidebook

XREF	Cross reference two incidents and **CLOSES FIRST INCIDENT**	XREF_123_345	This command is only used to cross reference an incident to an incident you want to CLOSE. The first incident in the command will be closed when you use this command. *A good time to use this command is when you dispatch a second incident to the same location by accident.*

Seattle Fire Department

Probationary Firefighter Development Guidebook

Seattle Fire Department

Probationary Firefighter Development GuidebookFOR THE PROBATIONARY FIREFIGHTER

You are responsible for ensuring that all of your Probationary requirements are completed and received by Training Division by the 12th month of your Probationary Year. Upon successful completion of Recruit School you will be assigned to an Operations Division company and will begin the second phase of your training, which will consist of a nine month "self-study" program. Monthly tests on both District & required readings will be given to ensure that assigned material has been learned and retained.

In conjunction with the "self-study program, you will participate in a manipulative skills program that will expand on the hose and ladder training you received in Recruit School. This program will be conducted by your assigned Company Officer and monitored by your Battalion Chief, with results logged in the Drill Competency sign off sheets.

DISTRICT STUDY

You will be required to learn a significant amount of material in regards to city wide routes of travel and facility locations. Each month will have elements of the City of Seattle that you will be required to learn. It is recommended, but not required, that you drive these routes in order to familiarize yourself with the physical nature of the roadways and facilities. Your final district exam will be based on your monthly district study in months four through nine.

DRIVER'S TRAINING

You received Driver Training in both classroom and on the track during Drill School. The last week of Drill School, you had a road check from an instructor.

During your engine company assignment of your Probationary year, you will do a driving drill on the assigned engine once each shift under the guidance of the regular driver and/or the company officer. This will consist of driving the assigned apparatus through the District while demonstrating good judgment and good driving technique.For the probationary firefighter

Skills and techniques include, but are not limited to:

- Driving in traffic
- Driving on narrow streets
- Entering and leaving the freeway
- Adhering to speed limits
- Backing and navigating residential traffic circles

Your company officer may allow you to drive Code Red, provided that you have been drilled by the Officer in Response Rules and have, in prior driving drills, demonstrated good control of the apparatus.

In the 10th or 11th month, you will receive a one hour check ride with a member of the Driver Training

Faculty. You will drive your Company's EVIP Road Course and will be expected to demonstrate all the above listed skills. You will be responsible for knowing the Response Rules, and will be instructed to drive Code Red to any aid response that comes in during your check ride. You will **NOT** be expected to drive Code Red to any rescue or fire response.

All documents for the Probationary Firefighter Development Guidebook can be found on Share Point under Training/Probationary Firefighter Guidebook

Engine Company Monthly Manipulative Drills

Engine Monthly Drills are #1-#6 They need to be accomplished in sequential month order, but the probationary firefighter does not needed to accomplish all Monthly Engine Drills prior to starting the Monthly Ladder Drills

Truck Company Monthly Manipulative Drills

Truck Monthly Drills are #1-#3 They need to be accomplished in sequential month order, but the probationary firefighter does not needed to accomplish all Monthly Truck Drills prior to starting the Monthly Engine Drills

Example:

Probationary firefighter Davis was assigned to E17D and completed Month 1, Month 2, & Month 3 engine drills. He was then detailed to Ladder 9 and completed Month 1, Month 2, & Month 3 of the truck drills. Upon rotating back to the engine the Month 4, Month 5, and Month 6 drills would need to be accomplished.http://www.ergometricsonline.com/markNoble/play.cfm

Local firefighter from Olympia, WA http://www.animatedknots.com/waterknotrescue/index.php

Animated knot video http://www.firefighterclosecalls.com/

Good training link

Sign up for the "Secret List" here

Month 4 Assignments Overview

Month 4 Probation Check-off

Self-Study Material

1. **Seattle Fire Department Policy & Operating Guidelines**
    - 1000 Authority
    - 3003 EEO
    - 3006 Injury/Illness
    - 3008 Personnel Rules & Regulations
    - 3016 Probationary Employees
    - 4003 Communications
    - 5010 Incident Accountability

- 5011 Incident Management System
- 5512 Incident Operations
- 5509 Watch Duties
- 6006 Personal Protective Equipment

2. **Emergency Care & Transportation of the Sick & Injured** 8th edition
   - Chapter 8

3. **King County Protocols** - all

4. **Training Guides**
   - 14-11
   - 14-12

5. **SFD Memo**
   - 186-05 D
   - 186-05 E

6. **Occupancy Based Firefighting**
   - Ventilation Supplement
   - Pre-Study Question

Month 4 Assignments Overview

7. **District Study**
   - Name & outline the boundary of all of the directional designation areas within the city of Seattle
   - Describe the address numbering system within the city of Seattle
   - Describe the difference between avenues & streets
   - Give the location by street intersection of all stations within your battalion

(List each station by nearest intersection)

   - Give the route of travel from your station to all of the other

stations within your battalion. (The easiest or shortest route on a map or the route in your car may not be the best route of travel for your fire apparatus. Ask if you're unsure.)

- Give the location & route of travel from your station to the following facilities
  - Headquarters
  - Fire Marshal's Office
  - Radio Shop
  - Fire Garage
  - Utility Shop/Commissary
  - Fire Alarm Center/Resource Management Center
  - Joint Training Facility
  - Local 27 Office

8. Supplemental Materials

- 4-6 SFD Pride & History
- 4-7 FF Heart Attacks
- 4-8 Hydrogen Cyanide (Power Point)
- 4-9 What's In Your Area (Power Point)
- 4-10 Four Story Tilt-ups
- 4-11 Window Size-up

	#1 Occupancy Based Firefighting (Share Point)	
1.1	The firefighter shall **read** the Occupancy Based Firefighting - Ventilation Document & complete the Ventilation pre-study questions	
1.2	The firefighter shall **demonstrate** understanding of the "SFD Ventilation Practices" through a discussion with their officer	
	#2 Equipment Operation/Safety	

2.1	The firefighter shall **define** procedures to be used in electrical emergencies, including proper procedures for shutting off the utility services to a building	
2.2	The firefighter shall **define** safety procedures as they apply to emergency operations. The specific areas to be defined are**:** • Protective equipment • Team concept • Portable tools & equipment • Riding an apparatus • Haz-Mat incidents	
	#3 Disability/exposures(POG 3006)	
3.1	The firefighter will **identify** a minimum of three common types of accidents and/or injuries, & their causes, which occur in the following locations: • Fire ground • Non-fire emergencies • Responding & returning to quarters • Training • Other on-duty locations	
3.2	The firefighter will **obtain & describe** the appropriate use of the on-duty & off-duty injury/illness forms for given situations	
3.3	The firefighter shall **describe** the proper procedures to follow after a "reportable exposure"	

	#4 Communications(POG 4003 & POG 5012)	
4.1	The firefighter shall **demonstrate** receiving an alarm or a report of an emergency at the fire station, and initiate action	
4.2	The firefighter shall **identify** traffic control devices installed in the fire station to facilitate the response of apparatus	
4.3	The firefighter shall **identify** all alarm alerting devices that should activate on receipt of an alarm	

4.4	The firefighter shall **identify** the procedures required for receipt & processing of business & personal calls	
4.5	The firefighter will **identify** the use of each of the 16, zone 1 channels	
4.6	The firefighter will **demonstrate** the ability to use the portable radio in the following situations: • Moving between dispatch & response channels • Locating the SPD channels • Setting the scan feature • Locating the mutual aid channels • Showing two ways to get to the simplex channels • Locating the site-trunking channels	
4.7	The firefighter will **explain** the use of site-trunked channels vs simplex channels	
4.8	The firefighter shall **define** policy & procedures concerning the ordering & transmitting of multiple alarms for fires & calls for special assistance from the emergency scene(Mayday, code blue, help the firefighter)	
4.9	The firefighter shall **demonstrate** understanding of the process of two-way communication & the importance of message acknowledgement	
4.10	The firefighter shall **demonstrate** the proper technique & procedures for operation of the station, portable & apparatus radios	
4.11	The firefighter shall **demonstrate** the operation of tracking, menu and status changes on the MDT system	

4.12	The firefighter shall **demonstrate** the operation of the CAD system to include: • Signing onto CAD • Verifying radio log-on • Unit history search function • Paging units	
	#5 Passport accountability (POG 5010)	

5.1	The firefighter shall **list & describe** all accountability system equipment(hardware) & show and understanding of its use	
5.2	The firefighter shall **describe** the elements of a personal accountability system & demonstrate the application of the system at an incident	
	#6 Watch Duty(POG 5509)	
6.1	The firefighter will **explain** which watch desk journal entries are in black ink and which are in red ink	
6.2	The firefighter will **identify** the different response type abbreviations that are recorded in the watch desk journal	
6.3	The firefighter will **demonstrate** the proper procedure to taking a lay-off and confirming a lay-off	
	#7 Personal Protective Equipment(POG 6006, King Co. CBT Infectious Diseases, & Exposure packet)	
7.1	The firefighter shall **identify** the function & limitations of the following articles of PPE • Protective coat, trousers, helmet, & goggles • SCBA • PASS device • Boots, gloves, hood & hearing protection • Nitrile gloves, EMS eye protection, HEPA mask, gowns	
7.2	The firefighter shall **demonstrate** the proper donning & doffing of the protective equipment from of EMS PPE (gown, gloves, goggles, & mask)	
7.3	The firefighter shall **describe** the proper care & cleaning/decontamination of PPE from above	

7.4	The firefighter shall **describe** the appropriate level of PPE for the following: • Any patient contact • Patient with a fever & cough • Patient contact where obvious body fluid exposure is possible • Auto extrication with visible blood present	

	#8 EMS(Emergency Care of the Sick & Injured & K.C. Protocols & Training Guides 14-11, 14-12, SFD Memo #186-05)	
8.1	The firefighter shall **demonstrate** CPR skills during station drills or actual cardiac arrests including • Continuous compressions • Airway management & ventilation with bag valve mask • Use of AED	
8.2	The firefighter shall **demonstrate** knowledge of the current standing orders for cardiac arrest in adults & pediatric patients by correctly performing the expected tasks during the monthly drills or during actual cardiac arrests	
8.3	The firefighter shall **demonstrate** daily & monthly checks of the LP500	
8.4	The firefighter shall **demonstrate** the procedures to take after a cardiac arrest to include filling out the questionnaire, calling the LP500 message line & following the download procedures	
8.5	The firefighter shall **demonstrate** the proper use of the aid car/medic unit stretcher including • Unloading the unit & loading the unit • Raising & lowering • Shortening the head end • Raising the foot end for trendelenberg position • Safely carrying a patient up & down stairs on a stretcher	
8.6	The firefighter shall **identify** the appropriate combination of large or small administrations sets & fluids (D5W, ringers lactate, bicarb bottle, & hypertonic saline/study fluid)	
8.7	The firefighter shall **demonstrate** setting up an IV bag & administration set	
8.8	The firefighter shall **demonstrate** setting up a ringers lactate in a pressure bag	
8.9	The firefighter shall **demonstrate** the proper placement of the LP12 “limb	
	leads” to assist the medic unit with patient monitoring	

8.10	The firefighter shall **demonstrate** a familiarity of a SFD medic unity by locating on demand: • BP Cuff & stethoscope • Nasal cannula or non-rebreather mask • Tape from drawer • Warm ringers, large ad set & pressure bag • Restraints • ABC kit • Resuscitation Pak (blue soft pack of resuscitation medications) • Doppler • Backboard & cervical collar • MCI kit • Spare oxygen bottle • Bag valve mask • Suction unit & how to remove it	
8.11	The firefighter shall **explain** the appropriate use of the pediatric & adult EPI pens	
8.12	The firefighter shall **identify** the criteria for the use of oral glucose, & properly administer it to a patient or firefighter	
8.13	The firefighter shall **demonstrate** proper use of the Kendrick traction device(Memo 38-06 & DVD)	
8.14	The firefighter shall **identify** the criteria for a "sick" patient to include: • Physiological indicators • Nature of the injury • Mechanism of the injury	
8.15	The firefighter shall **demonstrate** the proper use of FASPLINTS	
8.16	The firefighter shall **demonstrate** proper use of restraints on a backboard &/or stretcher	
8.17	The firefighter shall **demonstrate** standard SFD techniques for safely removing a patient from an automobile onto a long backboard without using a short board.	

	#1 Equipment (Basic Skills)	

1.1	The firefighter will complete an apparatus inventory and for the equipment: **1**.Explain where, when and how the item is used 2**.** Demonstrate use in a proficient manner, including safety rules 3**.** Perform all prescribed maintenance prior to returning equipment to the rig	
	#2 Power equipment(Basic Skills)	
2.1	The firefighter will be able to inspect, start, & perform maintenance on all power equipment assigned to the company	
	#3 Self Contained Breathing Apparatus(Basic Skills, POG 6007, Essentials)	
3.1	The firefighter shall **identify** the hazardous environments requiring the use of respiratory protection	
3.2	The firefighter shall **demonstrate** replacement of a 45 minute cylinder with a 60 minute cylinder on an SCBA assembly	
3.3	The firefighter shall **demonstrate** donning PPE within one minute	
3.4	The firefighter shall **demonstrate** donning the SCBA while wearing full PPE, within one minute	
	#4 Ladders (Basic Skills & Essentials)	
4.1	The firefighter shall **demonstrate** a high shoulder carry & raise of a 14’ roof ladder	
4.2	The firefighter shall **demonstrate** a low shoulder carry & raise of a 14’ roof ladder	
4.3	The firefighter shall **demonstrate** the deployment of a roof ladder to a peaked roof off a ground extension ladder	
4.4	The firefighter shall **demonstrate** a one person high shoulder carry/beam raise of a 24’/26’ ladder	
4.5	The firefighter shall **demonstrate** a one person low shoulder carry/beam raise of a 24’/26’ ladder	

4.6	The firefighter shall **demonstrate** a one person flat raise of a 24’/26’ ladder	

4.7	The firefighter shall **demonstrate** a one person pivot of a 24'/26' ladder	
4.8	The firefighter shall **demonstrate** a two person cradle carry/cradle raise of a 35' ladder	
4.9	The firefighter shall **demonstrate** a three person flat carry/raise of a 35' ladder with a roof package	
4.10	The firefighter shall **demonstrate** a two person beam carry/beam raise of a 35' ladder	
4.11	The firefighter shall **demonstrate** a four person flat raise of a 45' or greater ladder with tormentor poles	
4.12	The firefighter shall **demonstrate** the proper pivoting ladders up to 35'(in all positions) without hesitation or delays	
4.13	The firefighter shall climb the full length of a ground extension and **demonstrate** carrying fire fighting tools (rubbish hook & chainsaw)	
	#5 Ventilation: PPV/Vertical/Horizontal (Essentials, Building Construction)	
5.1	The firefighter will **describe** the potential benefits & potential hazards of the following types of ventilation: • Vertical • Horizontal • Trench/strip • Negative pressure • Positive pressure • Hydraulic	
5.2	The firefighter will **establish** horizontal ventilation (JTF burn bldg w/smoke prop available)	
5.3	The firefighter will **establish** PPV (JTF burn bldg w/smoke prop available)	
5.4	The firefighter will **establish** ventilation on a pitched roof (JTF has 3 props)	

	#6 Chief's Drill	
6.1	Drill of Chief's choosing	

Seattle Fire Department

Probationary Firefighter Development Guidebook

Monthly Assignment Check-off Sheet

Monthly, during your probation, you should read the required materials, study your district and complete the required tests. Tests should be graded and documented on your Form 50. As you complete each item log it below. When all items are complete, **send the POG Test and District Test, the Check-offs along with this form to Training Division – Attention Recruit Captain. The Form 50 should be sent up the chain-of-command.**

Probationary Firefighter_____**I/I#**_____**Month**_____

Signature_____

	Send to:	**Date Completed**	**Score**
Monthly Check-off	Training - Recruit Cpt.		**NA**
Manipulative Check-off	Training – Recruit Cpt.		**NA**
POG Test	Training - Recruit Cpt.		
District Test	Training - Recruit Cpt.		
Forms 50 & 50A	Chain of Command		**NA**

Any questions about tests or reasons why any items above will not be received on time should be listed in the comments section.

Comments:

_____

_____

_____

_____

_____

_____

Month 5 Assignments Overview

1. **Month 5**

Probation Check-off

Self-Study Material

2. **Seattle Fire Department Policy & Operating Guidelines**
    - 5001 Aid & Medic Units
    - 5002 Aircraft Operations
    - 5004 Carbon Monoxide
    - 5005 Civil Disturbances
    - 5007 Disaster Management
    - 5008 Hazardous Materials Operations
    - 5009 High Rise Operations
    - 6007 Respiratory Protection Program
    - 7002 Equipment
    - 7006 Repairs & maintenance

3. **District Study**
    - Give the location by street intersection of all stations in Battalion Two
    - **List each station by nearest intersection**
    - Give the route of travel to all stations in Battalion Two from your station
    - Give the location & route of travel from your station to the **emergency room entrances** of all hospitals in the city:
        - Harborview Medical Center
        - University of Washington
        - Swedish Cherry Hill
        - Swedish First Hill

- Swedish Ballard
- Veterans Administration
- Northwest Hospital
- Children's Regional Medical Center
- Virginia Mason

Month 5 Assignments Overview

3. Supplemental Materials

- 5-3 JTF Drills
- 5-4 SFD Pride and History
- 5-5 Handcuff Knot
- 5-6 RIT Drill FF Down at the Window
- 5-7 RIT Drill FF Out of Air
- 5-8 RIT Drill No Exit
- 5-9 RIT 1st Due Assignments

	#1 Carbon Monoxide Alarms (POG 5004)	
1.1	The firefighter shall be able to **describe** the concerns to be address at a response for a carbon monoxide alarm activation	
1.2	The firefighter shall be able to **describe** the three phases of a CO response (Search & Rescue, Investigation, & Re-occupancy)	
1.3	The firefighter shall be able to **describe** the concerns and required actions with 10ppm CO, greater than 10 ppm CO but less than 35ppm of CO, & 35ppm or greater of CO	
	#2 Hazardous Materials Operations (POG 5008)	
2.1	The firefighter shall **describe** the initial company operations at a HazMat incident, including the actions they would accomplish	
2.2	The firefighter shall **demonstrate** two ways of setting up emergency decontamination	
	#3 High Rise Operations (POG 5009)	

3.1	The firefighter shall **describe** the initial actions of the 1st due engine & truck at a high rise fire	
3.2	The firefighter shall **describe** their role if assigned to elevator operations	
3.3	The firefighter shall **describe** their role if assigned to ventilation	
3.4	The firefighter shall **describe** their role if assigned to evacuation	
3.5	The firefighter shall **explain** the difference between Phase I & Phase II firefighter elevator control	
3.6	The firefighter shall **demonstrate** the safety procedures to properly place the elevator into Phase II firefighter control & prior to moving the car for use	
3.7	The firefighter shall **describe** the minimum equipment required for the elevator operator	

	#4 Repairs & maintenance (7006)	
4.1	The firefighter shall **demonstrate** the ability to properly fill out a F130 online	
4.2	The firefighter shall **demonstrate** signing off repaired equipment that has been returned to the station.	
4.3	The firefighter shall **demonstrate** properly placing completed F130's in the company files	
4.4	The firefighter shall **describe** the situations that would place an apparatus out of service	
4.5	The firefighter shall **describe** the steps to placing an apparatus out of service	

	#1 Forcible Entry(Essentials)	
1.1	The firefighter shall **describe** how to force entry through the following: (*The JTF has these props continuously ** has these props occasionally, call)	

	*Inward swinging wood door in a wood jam	
	*Outward swinging wood door in a wood jam	
	*Inward swinging steel door with a steel jam	
	*Outward swinging steel door with a steel jam	
	**Sectional overhead door	
	**Roll up door	
	**Scissor gates	
	Padlocks	
	Chain driven parking gate	
	Traction wheel driven parking gate	
	#2 Salvage(Basic Skills)	
2.1	The firefighter shall **describe** the application for **& demonstrate** the accordion fold & the donut roll for salvage	
2.2	The firefighter shall **demonstrate** laying & throwing tarps as a method of deploying salvage covers to cover property	
2.3	The firefighter shall **demonstrate** the construction & use of a ladder catch-all	
2.4	The firefighter shall **demonstrate** the construction & use of a tarp catch-all	
2.5	The firefighter shall **demonstrate** the construction & use of the stairway water chute	

	#3 Sprinklers(Essentials)	

3.1	The firefighter shall **identify** a fire department sprinkler connection & water motor alarm	
3.2	The firefighter shall **explain** how the automatic sprinkler head activates & releases water	
3.3	The firefighter shall **demonstrate** how to stop the flow from a sprinkler head using a wedge	
3.4	The fire fighter shall **identify**, on site, during an inspection the main control valve on an automatic sprinkler system, & **explain** how to "open" & "close" the valve	
3.5	The firefighter shall **identify** the control & operating valves of a sprinkler system including: • Outside screw & yoke(OS&Y) • Post indicator • Wall post indicator	
3.6	The firefighter shall **identify**, on site, during an inspection the main drain valve on an automatic sprinkler system	
3.7	The firefighter shall **identify & describe** the following sprinkler systems: • Wet • Dry • Deluge • Pre-action • Residential	
3.8	The firefighter shall **identify** all pressure gauges on wet & dry systems	
3.9	The firefighter shall **explain** how to identify a dry system gone wet	

	#4 Aerial Ladders Operations (IFSTA Aerial Operations)	
4.1	The firefighter shall **describe** aerial positioning for the assigned ladder truck	
4.2	The firefighter shall **demonstrate** satisfactory knowledge & performance of the following ladder operations: • Set the ladder jacks • Position apparatus for using the aerial for rescues • Position the apparatus for access	
4.3	The firefighter shall **identify** the load chart & describe the load limits for the assigned ladder truck	
4.4	The firefighter shall **identify & describe** the use of the high idle	
4.5	The firefighter shall **locate & explain** the function of the rung alignment light	
4.6	The firefighter shall **demonstrate** satisfactory knowledge & performance of the following ladder operations: • Operating the controls to raise the ladder from bed • Operating the controls to lower into a building • Operating the controls to retract the flys & rotate simultaneously • Operating the controls to rotate & extend the fly(s) simultaneously • Operating the controls to bed the ladder	
4.7	The firefighter shall **demonstrate** satisfactory knowledge & performance of the Aerial Ladder Pipe Evolution (all positions)	
4.8	The firefighter shall **demonstrate** satisfactory knowledge & performance of the Aerial Stokes Rescue Evolution (all positions)	
	#5 Elevator Rescue(Essentials & Company library)	
5.1	The firefighter shall **locate** the elevator rescue reference materials in the company library	
5.2	The firefighter shall **describe** the difference between hydraulic & traction elevators	
5.3	The firefighter shall **describe** the proper procedures for the response to passengers stuck in an elevator	

Operations Study Program Standard		Initials/date
5.4	The firefighter shall **locate** the elevator hoistway keys on the apparatus	

5.5	The firefighter shall **access** an elevator key box	
5.6	The firefighter shall **demonstrate** opening a hoistway door in a rescue situation or simulated situation (JTF drill tower elevator available)	
	#6 Chief's Drill	
6.1	Drill of Chief's choice	

Seattle Fire Department

Probationary Firefighter Development Guidebook

Monthly Assignment Check-off Sheet

Monthly, during your probation, you should read the required materials, study your district and complete the required tests. Tests should be graded and documented on your Form 50. As you complete each item log it below. When all items are complete, **send the POG Test and District Test, the Check-offs along with this form to Training Division – Attention Recruit Captain. The Form 50 should be sent up the chain-of-command.**

Probationary Firefighter_____**I/I#**_____**Month**_____

Signature_____

	Send to:	**Date Completed**	**Score**
Monthly Check-off	Training - Recruit Cpt.		**NA**
Manipulative Check-off	Training – Recruit Cpt.		**NA**
POG Test	Training - Recruit Cpt.		
District Test	Training - Recruit Cpt.		
Forms 50 & 50A	Chain of Command		**NA**

Any questions about tests or reasons why any items above will not be received on time should be

listed in the comments section.

Comments:

Month 6 Assignments Overview

1. **Month 6 Probation Check-off**

Self-Study Material

2. **Seattle Fire Department Policy & Operating Guidelines**
    - 4004 Response Guidelines
    - 5013 Marine Operations
    - 5014 MCI (Multiple Casualty Incidents)
    - 5015 Mutual Aid
    - 5016 Post Incident Procedures
    - 5018 Technical Rescue
    - 5019 Wildland/Urban Firefighting
    - 5501 Adverse Weather
    - 5506 Flag Customs
    - 5507 House Dues
    - 5508 Mail Run

3. **District Study**
    - Give the location by street intersection of all fire stations in the Fourth Battalion. **List stations by nearest intersection**

    - Give the route of travel to all stations in the Fourth Battalion

from your station

- List in order, by street names, the on-ramps and off-ramps of Northbound I-5 between Boeing Access Road & NE 145 Street

- List in order, by street names, the on-ramps and off-ramps of Southbound I-5 between Boeing Access Road & NE 145 Street

- List in order the street names, the on-ramps & off-ramps of I-5 Express Lanes (south to north)

Month 6 Assignments Overview

4. Supplemental Materials

- 6-3 JTF Drills
- 6-4 SFD Pride and History
- 6-5 The Art of Reading Smoke (Power Point)
- 6-6 Enclosed Structure Dangers (Power Point)
- 6-7 Truck Co. 1st Due Assignments

	#1 Response Guidelines (POG 4004 & LAR Training Guide)	
1.1	The firefighter shall explain what it means to be "available for response" on an engine & on a truck	
1.2	The firefighter shall explain the required actions when a multiple alarm is dispatched & the actions required to "move-up"	
1.3	The firefighter shall demonstrate the required actions during a freeway response (in all positions)	
	#2 Company Records (POG 5505)	
2.1	The firefighter shall locate the following without hesitation: • Watch desk journal • Inspection file index (hard copy & computer) • Re-inspection tickler • Hydrant inspection cards (hard copy & computer) • Special inspection files • Time roll –F84 • Requests – F87	
2.2	The firefighter shall demonstrate completing inspection paperwork on the computer	
2.3	The firefighter shall locate a re-inspection in the tickler for their shift	
2.4	The firefighter shall demonstrate filling in the Time Roll	
	#3 Flag Customs (POG 5506)	
3.1	The firefighter shall demonstrate folding the Flag following proper flag folding customs	
3.2	The firefighter shall describe the proper flag etiquette for placing flags at half-mast	

3.3	The firefighter shall describe when & why it is acceptable for flags to be flown at night	

	#4 Knots(Basic Skills)	
4.1	The firefighter shall **demonstrate** the procedures for inspecting, maintaining, & storing rope	
4.2	The firefighter shall **identify** the reasons to place rope out of service	
4.3	The firefighter shall **explain** the use and **demonstrate** tying the following knots, Bends and Hitches:	
	• Square bend	
	• Round turn & two half hitches	
	• Hose knot	
	• Rolling hitch pulling left	
	• Rolling hitch pulling right	
	• Fisherman's bend	
	• Prussik hitch	
	• Water "knot" or ring bend	
	• Figure "8" follow-through	
	• In-Line Figure "8" Towards	
	• In-Line Figure "8" Away	
	• Figure "8" on a bight	
	• Bowline with a Yosemite finish	
	• Long-tail bowline	
	• Running bowline	

	#1 Confined Space (Training Guides & computer)	
1.1	The firefighter shall **locate** the reference materials in the company library & on the computer	
1.2	The firefighter shall **explain** the operating functions of the 5 gas detector	

DRAFT

1.3	The firefighter shall **demonstrate** conducting daily checks of the 5 gas detector	
1.4	The firefighter shall **demonstrate** the packaging of a patient in the Sked Stretcher for a vertical evacuation	
	#2 TIC/RAK (Training Guides & computer)	
2.1	The firefighter shall **demonstrate** conducting an oriented search without a TIC	
2.2	The firefighter shall **demonstrate** conducting an oriented search with a TIC	
2.3	The firefighter shall **locate** a downed firefighter with an activated PASS device	
	The firefighter shall **demonstrate** the procedure to follow to transmit a mayday report	
2.4	The firefighter shall **demonstrate** the transfilling of a downed firefighter from a RAK	
2.5	The firefighter shall **demonstrate** placing the RAK facepiece on a downed firefighter	
	#3 Rope Rescue (Training Guides & computer)	
3.1	The firefighter shall **locate** the reference materials in the company library & on the computer	
3.2	The firefighter shall **demonstrate** the set up a raising & a lowering system	
	#4 Vehicle Extrication (Training Guides & computer)	
4.1	The firefighter shall **locate** the reference materials in the company library & on the computer	

4.2	The firefighter shall **demonstrate** stabilizing a vehicle	
4.3	The firefighter shall **demonstrate** securing the power on a vehicle	
4.4	The firefighter shall **demonstrate** removing the roof on a vehicle	
4.5	The firefighter shall **demonstrate** removing all doors from the vehicle	
4.6	The firefighter shall **demonstrate** displacing the dash in a vehicle	

DRAFT

	#5 Heavy Rescue (Training Guides & computer)	
5.1	The firefighter shall **locate** the reference materials in the company library & on the computer	
5.2	The firefighter shall **explain** all operating functions of the airbag lift system	
5.3	The firefighter shall **explain** the load limits of a crib box	
5.4	The firefighter shall **build** a crib box	
	#6 Chief's Drill	
6.1	Drill of Chief's Choice	

Seattle Fire Department

Probationary Firefighter Development Guidebook

Monthly Assignment Check-off Sheet

Monthly, during your probation, you should read the required materials, study your district and complete the required tests. Tests should be graded and documented on your Form 50. As you complete each item log it below. When all items are complete, **send the POG Test and District Test, the Check-offs along with this form to Training Division – Attention Recruit Captain. The Form 50 should be sent up the chain-of-command.**

Probationary Firefighter_____**I/I#**_____**Month**
_____

Signature_____

	Send to:	**Date Completed**	**Score**
Monthly Check-off	Training - Recruit Cpt.		**NA**
Manipulative Check-off	Training – Recruit Cpt.		**NA**
POG Test	Training - Recruit Cpt.		
District Test	Training - Recruit Cpt.		
Forms 50 & 50A	Chain of Command		**NA**

Any questions about tests or reasons why any items above will not be received on time should be

DRAFT

listed in the comments section.

Comments:

Month 7 Assignments Overview

1. **Month 7 Probation Check-**

off Self-Study Material

2. **Seattle Fire Department Policy & Operating Guidelines**
    - 3004 Ethics
    - 3005 Employee Suggestions
    - 3007 Awards
    - 3010 Serious Injury or Death
    - 6001 Accident Prevention
    - 6002 Chemical Hazard Communication
    - 6003 Dangerous Buildings
    - 6004 Safety

6005 Infection Control Plan

3. **District Study**
    - Give the location by street intersection of all fire stations in the Fifth Battalion. **List stations by nearest intersection**

    - Give the route of travel to all stations in the Fifth Battalion from your station

    - List in order, by street names, the on-ramps and off-ramps of Northbound State Route 99 between East Marginal Way South

DRAFT

and Bridge Way North

- List in order, by street names, the on-ramps and off-ramps of Southbound State Route 99 between Bridge Way North and East Marginal Way South

4. **King County Patient Care Protocols –** Entire document

Month 7 Assignments Overview

5. **Seattle Fire Department Policy & Operating Guidelines**
    - 7-3 JTF Drills
    - 7-4 SFD Pride and History
    - 7-5 Chimney Fires
    - 7-6 Backdraft
    - 7-7 Backdraft (video)

Month 7 – Probation Check-off

DRAFT

Instructor

Operations Study Program Standard Initials/date

	#1 Firefighter II Skills	
1.1	The firefighter shall **demonstrate** completing a NFIRS report	
1.2	The firefighter shall **demonstrate** changing unit status via MDC (Mobile Data Computer)	
1.3	The firefighter shall **demonstrate** changing status via radio	
1.4	The firefighter shall **demonstrate** conducting a station tour	
	#2 Accident Prevention (POG 6001)	
2.1	The firefighter shall **locate** the accident report kit & **explain** when it is used	
	#3 Safety (POG 6004)	
3.1	The firefighter shall **explain** who is responsible for safety at an incident	
3.2	The firefighter shall **explain** what the ISO (incident safety officer) focus is on during an incident	
	#4 Infection Control Plan (POG 6005)	
4.1	The firefighter shall **demonstrate** that they have the required items in their fanny pack	
4.2	The firefighter shall **explain** the proper procedure for decontamination of: • PPE (fire) • Aid kits • Station uniform/boots (EMS) • Rig	
4.3	The firefighter shall **explain** the difference between a reportable exposure & a hospital reportable exposure	
4.4	The firefighter shall **explain** the purpose of the Situation Found program	

Seattle Fire Department

DRAFT

Probationary Firefighter Development Guidebook

Monthly Assignment Check-off Sheet

Monthly, during your probation, you should read the required materials, study your district and complete the required tests. Tests should be graded and documented on your Form 50. As you complete each item log it below. When all items are complete, **send the POG Test and District Test, the Check-offs along with this form to Training Division – Attention Recruit Captain. The Form 50 should be sent up the chain-of-command.**

Probationary Firefighter_____**I/I#**_____**Month**
_____

Signature_____

	Send to:	**Date Completed**	**Score**
Monthly Check-off	Training - Recruit Cpt.		**NA**
Manipulative Check-off	Training – Recruit Cpt.		**NA**
POG Test	Training - Recruit Cpt.		
District Test	Training - Recruit Cpt.		
Forms 50 & 50A	Chain of Command		**NA**

Any questions about tests or reasons why any items above will not be received on time should be listed in the comments section.

Comments:
_____
_____
_____
_____
_____
_____
_____
_____
_____

Seattle Fire Department

DRAFT

Month 8 Assignments Overview

1. **Month 8 Probation Check-**

off Self-Study Material

2. **Seattle Fire Department Policy & Operating Guidelines**
    - 1001 Correspondence
    - 1005 Media Relations
    - 2001 Inspections *only through page 87*
    - 2002 Smoke Alarms
    - 3011 Discipline
    - 3012 Drugs & Alcohol
    - 7008 Uniforms

3. **District Study**
    - Give the location by street intersection of all fire stations in the Sixth Battalion. **List stations by nearest intersection**

    - Give the route of travel to all stations in the Fourth Battalion from your station

4. **Supplemental Materials**
    - 8-3 JTF Drills
    - 8-4 SFD Pride and History
    - 8-5 Attic Fires

	#1 Firefighter II Skills	
1.1	The firefighter shall demonstrate conducting a building inspection	
1.2	The firefighter shall demonstrate completing a NOV	
1.3	The firefighter shall demonstrate completing a F-6	

DRAFT

	#2 **Correspondence** (POG 1001)	
2.1	The firefighter shall **explain** the difference between Type I memos, Type II memos, & dispatches	
2.2	The firefighter shall **demonstrate** creating a Type II memorandum	
2.3	The firefighter shall **demonstrate** creating a Department letter to the Chief	
	#3 **Inspections** (POG 2001)	
3.1	The firefighter shall **explain** the purpose of the regular inspection program	
3.2	The firefighter shall **explain** the different general occupancy classifications: (A,B,E, I, R, U etc..)	
3.3	The firefighter shall **explain** the process in conducting a regular inspection (i.e.: starting pt, finishing pt. ,route of travel)	
3.4	The firefighter shall **explain** inspection criteria during a regular inspection (those things that areas of concern)	
3.5	The firefighter shall **demonstrate** the process for taking a complaint: • Filling out the form • Documentation • Forwarding • Filing	

	#4 **Discipline** (POG 3011)	
4.1	The firefighter shall **explain** the purpose of discipline	
4.2	The firefighter shall **explain** the progression of discipline	
4.3	The firefighter shall **explain** the checks & balances in place to protect firefighters in regards to discipline	

DRAFT

	#1 Driver Drills (Basic Skills)	
1.1	The firefighter shall **demonstrate** LDH to the front	
1.2	The firefighter shall **demonstrate** LDH to the rear	
1.3	The firefighter shall **demonstrate** laying forward dry	
	#2 Tailboard Drills (Basic Skills)	
2.1	The firefighter shall **demonstrate** taking a hydrant as a tailboard member on a forward lay dry	
2.2	The firefighter shall **demonstrate** advancing an 1 ¾" hose for a fire attack at grade level	
2.3	The firefighter shall **demonstrate** advancing an 1 ¾" hose for a fire attack to below grade	
2.4	The firefighter shall **demonstrate** advancing an 1 ¾" hose for a fire attack to above grade	
	#3 Engine Company Drills (Basic Skills, Memo 96-09, & Tng Guide 9-2)	
3.1	The firefighter shall **demonstrate** (in all positions) a monitor manifold • #2 Unload the wye section, lay reverse, supply, & 2nd supply • #3/#4 Monitor, 2 ½", & set-up monitor	
3.2	The firefighter shall **demonstrate** drafting or complete the annual pump test	
	#4 Apparatus Driving	
4.1	Shift 1	
4.2	Shift 2	
4.3	Shift 3	
4.4	Shift 4	
4.5	Shift 5	

DRAFT

4.6	Shift 6	
4.7	Shift 7	
4.8	Shift 8	
	#9 Chief's Drill	
9.1	Drill of Chief's choosing	

Seattle Fire Department

Probationary Firefighter Development Guidebook

Monthly Assignment Check-off Sheet

Monthly, during your probation, you should read the required materials, study your district and complete the required tests. Tests should be graded and documented on your Form 50. As you complete each item log it below. When all items are complete, **send the POG Test and District Test, the Check-offs along with this form to Training Division – Attention Recruit Captain. The Form 50 should be sent up the chain-of-command.**

Probationary Firefighter_____**I/I#**_____**Month**
_____

Signature_____

	Send to:	**Date Completed**	**Score**
Monthly Check-off	Training - Recruit Cpt.		**NA**
Manipulative Check-off	Training – Recruit Cpt.		**NA**
POG Test	Training - Recruit Cpt.		
District Test	Training - Recruit Cpt.		
Forms 50 & 50A	Chain of Command		**NA**

Any questions about tests or reasons why any items above will not be received on time should be listed in the comments section.

Comments:
_____
_____
_____

DRAFT

Seattle Fire Department

Probationary Firefighter Development Guidebook

Month 9 Assignments Overview

1. **Month 9 Probation Check-**

off Self-Study Material

2. **Seattle Fire Code**
    - Chapter 2 – Occupancy classification definitions only
    - Section 504 - 509
    - Section 902 – Standpipe system classes and types only
    - Section 905

3. **Training Guide #1-1** Firefighting Foam Operations, Apparatus, & Equipment

4. **District Study**
    - Give the location by street intersection of all fire stations in the Seventh Battalion. **List stations by nearest intersection**

    - Give the route of travel to all stations in the Seventh Battalion from your station

5. **Supplemental Materials**
    - 9-3 JTF Drills
    - 9-4 SFD Pride and History
    - 9-5 Standpipe Operations
    - 9-6 Standpipe Operations Multi-Family

DRAFT

Month 9 – Probation Check-off

	#1 Firefighter II Skills	
1.1	The firefighter shall **demonstrate** completing a F-20B	
1.2	The firefighter shall **demonstrate** requesting AMR by both radio & phone	
	#2 Seattle Fire Code	
2.1	The firefighter shall **explain** when building are required to have stair access to the roof	
2.2	The firefighter shall **explain** where elevator key boxes should be located & what should be found in each box	
2.3	The firefighter shall **explain** the building hazards that could be encountered in a building & how they should be marked	
2.4	The firefighter shall **explain** hydrant inspection frequency, protection, & markings	
2.5	The firefighter shall **explain** the classes of standpipes	
2.6	The firefighter shall **explain** the possible problems associated with each type of standpipe	
2.7	The firefighter shall **explain** which building require standpipes	
2.8	The firefighter shall **explain** when a building is allowed to have a dry standpipe	
2.9	The firefighter shall **explain** when standpipes are required to be interconnected and the benefit & problems associated with this	
2.10	The firefighter shall **explain** what buildings are not required to have standpipes even when they are greater than 3 stories from the lowest fire department access point	

	#1 Driver Drills (Basic Skills)	

DRAFT

1.1	The firefighter shall **demonstrate** setting the appropriate discharge pressures while simultaneously flowing water to a 2 1/2" smoothbore nozzle and 2 ½" TFT nozzle	
1.2	The firefighter shall **demonstrate** setting the appropriate discharge pressures for flowing foam from a FoamPro rig, Elkhart In-Line Eductor, and a Pro Pak	
1.3	The firefighter shall **explain** when it is appropriate to use foam	
1.4	The firefighter shall **explain** at what proportions foam is typically set for the FoamPro, Elkhart In-Line Eductor, & the Pro Pak	
	#2 Tailboard Drills (Basic Skills)	
2.1	The firefighter shall **demonstrate** advancing a charged 2 ½" hoseline for a fire attack at grade level	
2.2	The firefighter shall **demonstrate** advancing a charged 2 ½" hoseline for a fire attack above grade level	
2.3	The firefighter shall **demonstrate** advancing a charged 2 ½" hoseline for a fire attack below grade level	
2.4	The firefighter shall **demonstrate** advance a charged 1 ¾" hoseline from a standpipe for a fire attack	
	#3 Engine Company Skills (Basic Skills)	
3.1	The firefighter shall **demonstrate** (in all positions) advancing a 2 ½" hoseline up a ground extension ladder & making a fire attack	
3.2	The firefighter shall **demonstrate** (in all positions) taking a standpipe and deploying a 1 ¾ " hoseline for fire attack	
	#4 Apparatus Driving	
4.1	Shift 1	
4.2	Shift 2	

4.3	Shift 3	
4.4	Shift 4	

DRAFT

4.5	Shift 5	
4.6	Shift 6	
4.7	Shift 7	
4.8	Shift 8	
	#7 Chief's Drill	
7.1	Drill of Chief's choosing	

Probationary Firefighter Development Guidebook

Monthly Assignment Check-off Sheet

Monthly, during your probation, you should read the required materials, study your district and complete the required tests. Tests should be graded and documented on your Form 50. As you complete each item log it below. When all items are complete, **send the POG Test and District Test, the Check-offs along with this form to Training Division – Attention Recruit Captain. The Form 50 should be sent up the chain-of-command.**

Probationary Firefighter_____**I/I#**_____**Month**
_____

Signature_____

	Send to:	**Date Completed**	**Score**
Monthly Check-off	Training - Recruit Cpt.		**NA**
Manipulative Check-off	Training – Recruit Cpt.		**NA**
POG Test	Training - Recruit Cpt.		
District Test	Training - Recruit Cpt.		
Forms 50 & 50A	Chain of Command		**NA**

Any questions about tests or reasons why any items above will not be received on time should be listed in the comments section.

Comments:
_____
_____
_____
_____
_____
_____
_____
_____

DRAFT

Seattle Fire Department

Probationary Firefighter Development Guidebook

Month 10 Assignments Overview

1. **Month 10 Probation Check-**

off Self-Study Material

2. **ICS 100 & 200 Certification**
    - Go online to the address below & complete the study & test for FEMA ICS 100 & ICS 200 Certification. You may use your home address to receive your certificates.

    - Immediately forward a copy of the e-mail notification you receive for completing the two courses to the Assistant Training & Education Coordinator at Training Division.

    - Copies of the ICS 100 & ICS 200 Certificates must be forwarded to the Training Division In-Service Coordinator.

    - Web Addresses to be used

ICS 100 – http://training.fema.gov/emiweb/is/is100.asp ICS 200 – http://training.fema.gov/emiweb/is/is200.asp

3. **District Study**
    - District Final Exam

4. **Supplemental Materials**
    - 10-3 JFT Drills
    - 10-4 SFD Pride and History
    - 10-5 Garage Fires
    - 10-6 Coos Bay NIOSH Report
    - 10-7 Coos Bay Fatality (Power Point)
    - 10-8 Dehydration
    - 10-9 Dehydration (Power Point)

DRAFT

Month 10 – Probation Check-off

DRAFT

Instructor

Operations Study Program Standard Initials/date

	#1 ICS Certification	
1.1	The firefighter shall complete the ICS 100 certification	
1.1	The firefighter shall complete the ICS 200certification	
	#2 EMS Drill	
2.1	The firefighter shall **conduct** a company drill on pediatric triangle & child patient assessment	

	#1 Driver Drills	
1.1	The firefighter shall **demonstrate** the ability to transition from LDH to 2 ½" as required when performing greater than 600 ft. lay (Parallel 2 ½" with proper orientation of Siamese)	
1.2	The firefighter shall **demonstrate** the ability to charge the standpipe when the FDC is not accessible (charging the standpipe from an outlet)	
1.3	The firefighter shall **demonstrate** the proper set-up for a low pressure hydrant	
1.4	The firefighter shall **demonstrate** LDH to the rear (see drill sheet 10-10)	
1.5	The firefighter shall **demonstrate** LDH to the front (see drill sheet 10-11)	
1.6	The firefighter shall **demonstrate** reverse pump hook-up(see drill sheet 10-12)	
1.7	The firefighter shall **demonstrate** 24'/26' ladder throw from the engine brackets (see drill sheets 10-13 & 10-14)	
	#2 Engine Company Drills	
2.1	The firefighter shall **describe** the benefits to tandem pumping & the situations where it would be appropriate to use	
2.2	The firefighter shall **demonstrate** the ability to tandem pump	

DRAFT

2.3	The firefighter shall **demonstrate** transfilling a downed firefighter in a no-visibility situation	
	#3 Apparatus Driving	
4.1	The firefighter shall **explain** the response rules for driving code red	
4.2	The firefighter shall **demonstrate** good control of the apparatus while driving	
4.3	The firefighter shall **demonstrate** driving the Company's EVIP Road Course after completing 4.1 & 4.2	
4.4	Shift 1	
4.5	Shift 2	

4.6	Shift 3	
4.7	Shift 4	
4.8	Shift 5	
4.9	Shift 6	
4.10	Shift 7	
4.11	Shift 8	
	#5 Chief's Drill	
5.1	Drill of Chief's choosing	

DRAFT

Seattle Fire Department

Probationary Firefighter Development Guidebook

Monthly Assignment Check-off Sheet

Monthly, during your probation, you should read the required materials, study your district and complete the required tests. Tests should be graded and documented on your Form 50. As you

complete each item log it below. When all items are complete, **send the POG Test and District Test, the Check-offs along with this form to Training Division – Attention Recruit Captain. The Form 50 should be sent up the chain-of-command.**

Probationary Firefighter_____I/I#_____Month _____

Signature_____

	Send to:	Date Completed	Score
Monthly Check-off	Training - Recruit Cpt.		**NA**
Manipulative Check-off	Training – Recruit Cpt.		**NA**
POG Test	Training - Recruit Cpt.		
District Test	Training - Recruit Cpt.		
Forms 50 & 50A	Chain of Command		**NA**

Any questions about tests or reasons why any items above will not be received on time should be listed in the comments section.

Comments:

_____
_____
_____
_____
_____
_____
_____
_____
_____

Seattle Fire Department

Probationary Firefighter Development Guidebook

Month 11 Assignments Overview

1. **Month 11 Probation Check-off Self-Study Material**

2. **Driving Check Ride**
   - Final driving evaluation with be scheduled through the Training Division

DRAFT

3. **Occupancy Based Firefighting**
    - Chapter 1

4. **Supplemental Materials**
    - 11-4 SFD Pride and History
    - 11-5 First Due Assignments – Engine Company
    - 11-6 Contra Costa NIOSH Report
    - 11-7 Contra Costa Investigative Report

11-8 Contra Costa Case Study QuestionsMonth 11 – Probation Check-off

DRAFT

Instructor
Operations Study Program Standard Initials/date

	#1 Deaths in the line of duty…	
1.1	The firefighter shall **read** the(NIOSH) Case study – Contra Costa County, CA located on Share Point	
1.2	The firefighter shall **discuss** the Contra Costa County, CA case study with their officer using the discussion points on the worksheet located on Share Point	
	#2 Occupancy Based Firefighting	
2.1	The firefighter shall **read** the Occupancy Based Firefighting document Chpt. 1	
2.2	The firefighter shall **explain** to the officer SFD's best practices for single family dwelling	

#5 Engine Manipulative Drills - Check-off

Instructor
Operations Study Program Standard Initials/date

	#1 Tailboard Drills	
1.1	The firefighter shall **demonstrate** tying the following knots: • Square knot • Clove hitch • Double fisherman's knot • Figure 8 on a bite • Bowline with a Yosemite finish	
1.2	The firefighter shall **demonstrate** replacing a burst section with two 2 ½" lines on supply side of the pump	
1.3	The firefighter shall **demonstrate** replacing a burst section with two 2 ½" lines on discharge side of the pump	
	#2 Apparatus Driving	

DRAFT

2.1	Shift 1	
2.2	Shift 2	
2.3	Shift 3	
2.4	Shift 4	
2.5	Shift 5	
2.6	Shift 6	
2.7	Shift 7	
	#3 Chief's Drill	
3.1	Drill of Chief's choosing	

Seattle Fire Department

Probationary Firefighter Development Guidebook

Monthly Assignment Check-off Sheet

Monthly, during your probation, you should read the required materials, study your district and complete the required tests. Tests should be graded and documented on your Form 50. As you complete each item log it below. When all items are complete, **send the POG Test and District Test, the Check-offs along with this form to Training Division – Attention Recruit Captain. The Form 50 should be sent up the chain-of-command.**

Probationary Firefighter_____**I/I#**_____**Month** _____

Signature_____

	Send to:	**Date Completed**	**Score**
Monthly Check-off	Training - Recruit Cpt.		**NA**
Manipulative Check-off	Training – Recruit Cpt.		**NA**
POG Test	Training - Recruit Cpt.		
District Test	Training - Recruit Cpt.		
Forms 50 & 50A	Chain of Command		**NA**

DRAFT

Any questions about tests or reasons why any items above will not be received on time should be listed in the comments section.

Comments:

_____
_____
_____
_____
_____
_____
_____
_____
_____

Month 12 Assignments Overview

1. **Month 12 Probation Check-off Self-Study Material**

2. **ICS 800 Certification**
   - Go online to the address below & complete the study & test for FEMA ICS Certification. You may use your home address to receive your certificates.
   - Immediately forward a copy of the e-mail notification you receive for completing the course to the Assistant Training & Education Coordinator at Training Division.
   - A copy of the ICS 800 Certificates must be forwarded to the Training Division In-Service Coordinator.
   - Web Addresses to be used

ICS 800 – http://training.fema.gov/emiweb/is/is800.asp

3. **Occupancy Based Firefighting**
   - Chapter 2
   - Chapter 3

DRAFT

4. **How We Decide** (article)

5. **65th Street Incident of June 5, 2008** (report)

6. **Final Written Exam**
    - Answer questions from all assigned reading materials: achieve a grade of 80% or more on a final written exam. **Exam will be given at the Training Division**

Month 12 Assignments Overview

7.

- 12-5 How We Decide
- 12-6 65Th Street Final Report
- 12-7 65th Street Questions
- 12-8 SFD Pride and History
- 12-9 Sacramento Roof Collapse (video)
- 12-10 Firefighter Safety (Power Point)

Month 12 – Probation Check-off

DRAFT

Instructor

	Operations Study Program Standard	Initials/date
	#1 Occupancy Based Firefighting	
1.1	The firefighter shall **read** Occupancy Based Firefighting Chpt. 2 & 3	
1.2	The firefighter shall **explain** to the officer SFD's best practices for high density town homes and for low/mid rise multi-family dwellings	
1.3	The firefighter shall **read** How We Decide	
1.4	The firefighter shall **read** The 65th Street Incident of June 5, 2008 and **discuss** the follow-up with their officer	

#6 Engine Manipulative Drills - Check-off

	Operations Study Program Standard	Instructor Initials/date
	#1 Driver Drills	
1.1	The firefighter shall **demonstrate** completing a blind alley lay as the 1st engine	
1.2	The firefighter shall **demonstrate** completing a blind alley lay as the 2nd engine	
1.3	The firefighter shall **demonstrate** pumping to a ladder pipe	
	#2 Tailboard Drills	
2.1	The firefighter shall **demonstrate** the proper use of restraints on a patient	
2.2	The firefighter shall **demonstrate** a firefighter down emergency transfill in zero visibility	
	#3 Apparatus Driving	
3.1	Shift 1	
3.2	Shift 2	
3.3	Shift 3	
3.4	Shift 4	

DRAFT

3.5	Shift 5	
3.6	Shift 6	
3.7	Shift 7	
3.8	Shift 8	
	#4 Chief's Drill	
4.1	Drill of Chief's choosing	

Seattle Fire Department

Probationary Firefighter Development Guidebook

Monthly Assignment Check-off Sheet

Monthly, during your probation, you should read the required materials, study your district and complete the required tests. Tests should be graded and documented on your Form 50. As you complete each item log it below. When all items are complete, **send the POG Test and District Test, the Check-offs along with this form to Training Division – Attention Recruit Captain. The Form 50 should be sent up the chain-of-command.**

Probationary Firefighter_____**I/I#**_____**Month**
_____

Signature_____

	Send to:	**Date Completed**	**Score**
Monthly Check-off	Training - Recruit Cpt.		**NA**
Manipulative Check-off	Training – Recruit Cpt.		**NA**
POG Test	Training - Recruit Cpt.		
District Test	Training - Recruit Cpt.		
Forms 50 & 50A	Chain of Command		**NA**

Any questions about tests or reasons why any items above will not be received on time should be listed in the comments section.

Comments:
_____

DRAFT

SUBJECT:	**COMMUNICATIONS EQUIPMENT**
REVISED: SEE ALSO:	12/3/18
PAGE(S):	(Policy Section). OG-4004 Radio Language Protocols. OG-4005 Radio Procedures. OG 4006 Radio Channels, Zones, and Usage.
	10

DRAFT

GENERAL INFORMATION

This section provides information and guidelines for communications equipment in the SFD. Portable radios, pagers, base stations, Computer Aided Dispatching (CAD), telephones (wired/cellular/satellite), and Mobile Data Computers (MDC) are discussed in this section as communications equipment.

PORTABLE RADIOS

Portable radios are emergency equipment and should be considered as vital as other personal protective equipment.

A portable radio is assigned to all operations personnel at the beginning of each work shift. This radio assignment remains in effect for as long as the member is assigned to that unit during the shift. Each member is responsible for the radio assigned to him or her during the work shift.

Members assigned to a position on a unit that responds to emergencies must sign onto the CAD system. When signing on to CAD, members must visually check the radio number of the portable radio assigned to them to ensure that the correct radio number is logged into the CAD system. After signing on, members must check CAD View to see if CAD received the correct information. If CAD does not accept the sign on information, contact the Help Desk immediately at 386-9770.

Not all SFD portable radios are intrinsically safe. Radios that are intrinsi- cally safe are marked with a

green dot on the bottom of the radio and/or a label under the battery with green writing. Intrinsically safe radios are "Factory Mutual" approved for specific hazardous atmospheres where ignitable concentrations of flammable gases or vapors exist. Radios that are not intrinsically safe could cause or become a source of ignition. If a person is operating in an area that has ignitable concentrations of flam- mable gases or vapors, do not operate a radio that is not marked intrin- sically safe.

RADIO PROCEDURES

Portable radios will be carried by all Operations Division personnel when at the scene of emergency responses.

Radios must be monitored at all times while the unit is on-the-air and it is advised that all members carry their assigned radio during such times.

Carrying radios in back pockets may cause damage to the LCD screen when the member sits down.

A portable radio battery's life is limited. Radios should be turned off when the user is in their assigned station or the radio is stored on the apparatus. To ensure proper operation, portable radio batteries should be changed twice a day or after extensive use.

The radios for Operations units, when in-service, will be switched to the primary dispatch channel, Zone 1 Channel 4. Portable radio tones will always be active and should not be muted.

FEEDBACK Feedback can be an inherent problem with multiple radios in close proximity. Feedback is caused by the 'looping' of a transmission between radios where it becomes amplified. Members should be aware that they can reduce feedback by:

- Reducing the volume.
- Covering the speaker/microphone.
- Creating some distance between the radios.

RADIO TESTS The Fire Alarm Center (FAC) periodically conducts a number of different radio tests that all members should be aware of and understand. They are as follows:

- The May Day Tone is tested/transmitted every Sunday.
- The Abandon Building Tone is tested/transmitted every Sunday.
- Interoperable communications links/patches between SFD and other jurisdictions (e.g., USCG)

are established and tested every Sunday fol- lowing the Abandon Building Tone.

- The emergency marker tone is tested/transmitted after the Abandon Building Tone once a month.
- Portable radio emergency buttons for specified units (on a rotating basis) are tested on Sundays.

DISTRIBUTING PORTABLE RADIOS

DRAFT

In the event of a portable radio problem, the Company Officer should:

- If necessary, redistribute portable radios to the company members most likely to need them (e.g., team leaders and nozzle-person).
- The Officer should attempt to obtain a replacement radio from the Incident Commander (IC).

During emergency incidents, when a member is assigned a replacement radio, the FAC may be requested to change the CAD Sign-on informa- tion for that member as soon as possible.

COMMUNICATIONS EQUIPMENT

At all other times, members will change their own designated portable radio number by accessing CAD Sign-on (located on the station com- puter).

SITE TRUNKING The SFD is a part of a county wide trunked - 800MHz system. Over 95% percent of Seattle is covered by 4 towers (sites) out of a total of 28 in the greater King County region. The system is designed so these 4 sites con- tinue to interoperate, even if the rest of the regional system fails.

The normal manner in which the radio system works is that radio trans- missions on designated talkgroups are routed through what is called the Zone Controller which assigns the talkgroup to one of several available frequencies. This main 'brain' simply makes sure transmitted messages are received and broadcast for anyone who can see a system site. Our radios are programmed to search for the site that provides the strongest signal. This is not always a Seattle site.

The possibility exists that the system may occasionally malfunction. One or more parts of the overall system may be unavailable, preventing the Zone Controller from properly routing a signal (transmission). In these situations we go into what is termed site trunking. Notification of this on the radio will be indicated in two ways:

- You will hear an audible tone at 7 second intervals.
- The LED screen on the radio will show, “Site Trunking.”

When this situation happens, our ‘fall back’ procedure is to switch our radios to Zone 9 (Zone 9 channels are identical to Zone 1). This, via the radio programming, directs the radio to search and use only the four Seattle sites. Our radios therefore ignore the Zone Controller and instead use our own Seattle simulcast site controller for the routing of transmissions.

However, there are two different types of site trunking, localized and county-wide. Dependent on which type, our procedures will vary slightly.

Localized (Seattle-wide) – Localized site trunking means that the prob- lem may be limited to a single site. For whatever reason, an individual radio or unit may, because of its location, require the use of a site that has lost contact with the Zone Controller. In these instances, the unit will probably be the first to identify the problem and should use the follow- ing procedures:

DRAFT

- Switch portable/mobile radio(s) to Zone 9 and the designated channel that you're currently assigned to; Keep one portable on Zone 1.
- Contact the FAC to notify that you're in site trunking; If you need to use a phone, dial 386-1498.
- Consider yourself on Radio Dispatching; You will be dispatched on Zone 9 Channel 4.
- When the portable on Zone 1 no longer displays "Site Trunking," the unit can secure from Radio Dispatching and switch all radios back to Zone 1.

DRAFT

TRUNKED CHANNEL

- Notify the FAC that you are clear from site trunking.

County-Wide – County-wide site trunking means that the problem is with the entire system and the whole county is probably affected. In this instance the FAC will be the first to identify the problem and will make a Department-wide announcement. The announcement will instruct all units to:

- Switch portable and mobile radios to Zone 9 and monitor the channel currently assigned to.
- Radio Dispatching will be in effect; Units will be dispatched on Zone 9 Channel 4.
- Return to quarters if not on an emergency response.
- The FAC may initiate a radio test of all units.
- The FAC will notify when the problem is resolved and when to switch radios back to Zone 1 and return to CAD Dispatching.

Units at an incident location that cannot communicate with the IC or FAC on the assigned channel should switch to the associated direct channel (e.g., Zone 2, Channel 1, for fire responses).

When in site trunking the station's base radio does not need to be switched to Zone 9 for it is programmed to always be in site trunking mode and searching for just the Seattle zone sites.

A trunked channel is one that is routed through the trunked system and is controlled by the system's main Zone Controller (also may be called the Master Site). It is a mode of communication in which conversations over the radio utilize multiple frequencies, and possibly multiple sites. These conversations are on "talkgroups" which are carried on one or more trunked channels (the talkgroup is selected on the radio whereas the channel is assigned by the Zone Controller). The Zone Controller, or 'brain' determines the proper routing of the signal and chooses between multiple available frequencies and sites, and broadcasts the message for everyone tohear.

Members should use the appropriate trunked talkgroup when possible, as these talkgroups are monitored by the FAC. This also allows the mem- ber to take full advantage of the radio's features such as the emergency button. The SFD talkgroups we use are on trunked channels (e.g., Zones 1, 3, and 9).

Members that experience poor radio reception or transmission at an incident should switch to the appropriate direct channel to establish communication. This action stresses the importance that someone on the exterior (command post) monitor the direct channel associated with the incident.

DIRECT CHANNEL A direct channel is one that is not routed through the trunked system and is not controlled by the system's Zone Controller. It is a mode of communication in which the sender transmits and receives a message at separate times on an assigned frequency. In essence it is similar to a walkie-talkie in that communication is directly from radio to radio.

DRAFT

Direct channels have a limited range; therefore, if needing to communi- cate over a greater distance such as during disaster operations, use of apparatus mobile radios would be advantageous due to having greater power and range.

These channels are not monitored by the FAC and the emergency but- ton does not function.

Members, therefore should use the appropriate trunked talkgroups whenever possible. This will allow the FAC to monitor communications and keep trunked radio features available to the members.

IC's should avoid having all units switch to a direct channel as a routine procedure.

IC's should monitor or assign a member to monitor the appropriate direct channel as soon as possible after command has been established.

Examples of when members should switch to a direct channel:

- In areas of known poor radio reception or transmission.
- When radios "bonk" indicating they are out of range.
- When they cannot communicate with anyone on the trunked talk- group.

Members should use the direct channels that correspond to the assigned incident trunked channel on the Zone 1 bank, Channels 1, 2 or 3.

Example: When the incident is assigned to Zone 1 Channel 1, the direct channel is Zone 2 Channel 1 (ST OPS 1). The same for Zone 1 Channel 2 (ST OPS 4), and Zone 1 Channel 3 (ST OPS 3).

Members that experience poor radio reception or transmission on either a trunked or direct channel should change their location, use a cell or landline phone, use runners, etc. to establish communication.

ZONE & CHANNEL ASSIGNMENTS

ZONE ASSIGNMENTS

SFD radios have zones, or channel banks, programmed into them, six of which receive the most use.

Zone 1 contains the SFD's main day-to-day working channels. Units should always monitor Zone 1 Channel 4 when in-service unless directed otherwise.

Zone 2 is utilized for SFD tactical channel communication and King County mutual aid zones such as:

- Channel 1, 2, and 3 are the tactical/direct channels.

DRAFT

- Channels 11 is the mutual aid zone channel for NORCOM (Bellevue, Mercer Island and Shoreline Fire), and Channel 12 is the mutual aid zone channel for ValleyCOM (South King County Fire).

Zone 3 contains the SFD Emergency channels and is used during Level 1 Operations (e.g., a catastrophic event where Battalion dispatching is implemented). During normal daily operations this zone may be used for drilling purposes.

Zone 6 contains the Seattle Police channels and can be scanned for obtaining information relating to an ongoing incident involving both SFD and Seattle Police.

Zone 8 contains a number of SFD Administration channels (i.e., Chan- nels 11-15). This zone was created so that Channels 11-15 could be used (e.g., a special event) and if a response was required, the normal assigned SFD channels could be turned to without having to change zones. Zone 8 Channels 1-10 and 16 operate the same as their respec- tive channels on Zone 1 including transmitting over Zone 1.

Zone 9 contains the same channels as Zone 1, but is used during site trunking.

ZONE 1 (Z1)	SFD main
ZONE 2 (Z2)	SFD direct channels and other County mutual aid
ZONE 3 (Z3)	SFD Emergency Battalion
ZONE 4 (Z4)	State Operations
ZONE 5 (Z5)	City mutual aid
ZONE 6 (Z6)	Seattle Police
ZONE 7 (Z7)	Events
ZONE 8 (Z8)	SFD Administration
ZONE 9 (Z9)	Site Trunking

DRAFT

NOTE

Depending upon a radio's programming, any base, mobile or portable radios may show an additional zone above Zone 9. These zones may be displayed as Zone 10, 12, Zone 71 or 72. These are future inter-operability zones currently used as nationwide talk groups. These additional zones currently are not used by the SFD.

CHANNEL ASSIGNMENTS

Each zone contains 16 different channels, or talk groups. Appendix 1 lists all channels for each zone within our radio system. Unless otherwise directed by the FAC, designated channels are to be used for operations as they are defined.

OTHER COMMUNICATION EQUIPMENT

MOBILE RADIO

DRAFT

All fire department apparatus mobile radios have Zone 1 Channel 4 pro- grammed as the priority channel which can be selected at any point by pressing the *Home* button.

When out-of-quarters and in-service, the scanning function should be activated. When dispatched on an alarm and directed to switch to another channel by the FAC, units should cancel this feature.

Desktop Radio

Desktop radios have Zone 1 Channel 4 programmed as the priority channel and must be left on Channel 4 with the scanning feature turned on. These radios, unlike portable and mobile radios, are always in site trunking mode which means they only search for one of the four Seattle sites and never need to be switched to Zone 9.

When directed to switch to another channel, units should turn off the scanning feature.

The scanning feature may also be turned off between the hours of 2200 and 0700.

Pager

CADView Paging

DRAFT

All Operations units are assigned one or two pagers dependant on the type of unit. The pager is primarily for alarm notification purposes and may also be used to contact a unit for non-emergency, Department business when unable to make contact via telephone or radio.

If assigned a pager it should be carried or kept in a place that will allow the member to be immediately alerted if the pager activates.

Administrative personnel are only required to carry their pagers when on duty or in a potential call back status.

Internal Department paging is available on CADView. CADView paging has the following capabilities:

- Single messages can be sent to multiple individuals, units and/or groups.
- A character counter helps prevent messages from being cut-off when sent.
- Contains a Group Paging Directory that lists all group members.

High usage of the CADView paging system has an impact on dispatch pages from the FAC. Department members need to utilize discretion when using the paging system. CADView paging therefore should pri- marily be used for critical and emergency messages. When possible, members should use the telephone, radio, or E-mail for routine commu- nications.

STATION ALERTER SYSTEM

The station alerting system is typically located in the watch office and activates the station lights, bells and/or tones, printer and PA system. This system is activated by the FAC to notify unit(s) within a specified station of an emergency alarm or special notice. The alerting system may also be activated by the station itself when needed (e.g., still alarm).

At 0700 daily, the FAC activates all fire station's alerting systems followed by a voice announcement, "0700 hours, hitch." If the daily alerter test is not received properly, notification should be made to the FAC of the test failure.

DEPARTMENT TELEPHONE/FAX

DRAFT

All SFD phones are programmed to allow abbreviated five digit dialing within the City Phone network as well as general access outside the City system.

Fire station main/business lines are set to allow local calls and in-state long distance access. Fire station fax lines are set to allow national long distance access, as are the Chief's business phones. All other SFD busi- ness phones have the level of long distance access set according to spe- cific business needs.

In the event that a station needs to make an out-of-state fire prevention or other business related call, the call can be made from a Chief's phone. Another option is to call the Department of Information Tech- nology (DoIT) Telephone Services at (206) 386-1111 and request assis- tance in making the call.

CELLULAR PHONE

All apparatus are assigned a Department cell phone that should be stored in the cab. Officers are responsible for the cellular phones assigned to the unit(s) under their supervision.

Operations personnel should be alert to use the cell phones in situations where they would be of benefit at an emergency scene (e.g., need to be discrete when transmitting confidential information).

Cell phones should also be used to report non-emergency incidents by dialing 911 and contacting the desired agency directly (e.g., SPD, Detoxification Van (through SPD), Washington State Patrol, etc.).

Often the contacted agency will ask specific questions that can be better answered first hand by the calling member vs. attempting to have the FAC relay information. This provides more accurate transfer of informa- tion and guarantees the appropriate response.

SATELLITE PHONE

Satellite phones are to be utilized during City wide emergencies when other forms of communication havefailed.

Satellite phones are located at the FAC, Resource Management Center (RMC), Operations Deputy Chief's office, and all Battalion Headquar- ters. The Fire Chief, Assistant Chiefs, and Administrative Deputy Chiefs have satellite phones in their assigned vehicles.

MOBILE DATA COMPUTER

The Mobile Data Computer (MDC) is the primary means of managing status changes. It responds to barehanded touch on the screen fields and buttons. Pencils, pens, or gloved hands will not work on the touch screen.

DRAFT

The MDC in all front-line and reserve apparatus will be checked for updates daily at the beginning of each shift using the VisiNet Mobile Launch Application. The application appears as a button on the Task Bar at the bottom of the MCD screen. This ensures that the MDC has the most current information with regards to hazardous conditions at emer- gency sites and accurate routing and vehicle location information.

The MDC will be shut down and restarted every Saturday. The restarting process takes approximately two minutes and is outlined in the VisiNet Mobile Training Guide.

For the operation of the MDC (e.g., toolbar navigation, status button changes, etc.), refer to the "Documentation and User Manuals" on the SFD SharePoint Home page under the Department Library heading. It is suggested that Operation companies review this training guide at regular intervals to maintain the skills necessary to appropriately use the MDC.

Problems with the MDC should be handled by calling the Department's Help Desk at 386-9770.

DocuSign Envelope ID: B759EAB4-9EOE-4CF2-822E-C3EFC21AAD71

DRAFT

SUBSCRIPTION AGREEMENT

This Subscription Agreement (the ***"Agreement")*** is entered into this ***'J.Q*** day of

J ***t(***

,

20_1 /ie·Effective Date") by and between ESO SOLUTIONS, INC., a Texas corporation with its principal place of business at 9020 N Capital ofTexas Highway, Building 11-300, Austin, Texas 78759 ***("ESO"),*** and the City of Seattle on behalf of the Seattle Information Technology Department, with its principal place of business at 700 Fifth Avenue, Suite 2700, Seattle, WA 98124 ***("Customer")*** (each a ***"Party"*** and collectively the ***"Parties").***

WHEREAS, ESO is in the business of providing software services (the *"Services")* to businesses and municipalities; and

WHEREAS, Customer desires to obtain these Services from ESO, to be used by Seattle Fire Department, all upon the terms and conditions set forth herein;

NOW, THEREFORE, for and in consideration of the agreement made, and the payments to be made by Customer, the Parties mutually agree to the following:

1. **Services.** ESO agrees to provide Customer the Services selected by Customer on Exhibit A attached hereto and incorporated by reference herein. Customer agrees that Services purchased hereunder are neither contingent on the delivery of any future functionality or future features, nor dependent on any oral or written public comments made by ESQ regarding future functionality or future features.

2. **Term.** The Term of this Agreement shall commence on the Effective Date and shall terminate one year after

the Effective Dale ***("/11itial Term").*** THE AGREEMENT SHALL AUTOMATICALLY RENEW FOR SUCCESSIVE RENEWAL TERMS OF ONE YEAR , UNLESS ONE PARTY GIVES THE OTHER PARTY WRITTEN NOTICE THAT THE AGREEMENT WILL NOT RENEW, AT LEAST THIRTY (30) DAYS PRIOR TO THE END OF THE CURRENT TERM.

3. Subscription Fees, Invoices and Payment Terms.

a. Subscription Fees. King County, Washington, a home rule charter county and a political subdivision of the State of Washington, has offered, and Customer has agreed, to pay for select Customer Subscription Fees on Customer's behalf as indicated in Exhibit A (collectively, the ***"Subscriptio11 Fees").*** In the event King County does not pay select Subscription Fees on behalf of Customer, and Customer chooses to continue receiving those Services, then Customer shall be responsible for any outstanding fees. Provided, however, that Customer remains directly responsible for those Services listed on Exhibit A not being paid by King County or any additional Services requested by Customer not paid by King County. To the extent that the terms of Sections 3 and 4 of the Agreement apply to those Subscription Fees which King County has agreed to pay, ESO shall first seek to resolve those issues with King County directly.

b. Payment of Invoices. Customer shall pay the full amount of invoices within thirty (30) days of receipt (the ***"Due Date").*** Customer is responsible for providing complete and accurate billing and contact information to ESO and to notify ESQ of any changes to such information.

c. Disputed Invoices. If Customer in good faith disputes a portion of an invoice, Customer shall remit to ESO, by the Due Date, full payment of the undisputed portion of the invoice. In addition, Customer must submit written documentation: (i) identifying the disputed amount, (ii) an explanation as to why the Customer believes this amount is incorrect, (iii) what the correct amount should be, and (iv) written evidence supporting Customer's claim. If Customer does not notify ESO of a disputed invoice by the Due Date, Customer shall have waived its right to dispute that invoice. Any disputed amounts determJned by ESO to be payable shall be due within ten (I0) days of such determination.

4. Terminati on.

a. Termination by Customer for ESO Default. If ESO fails to perform a material obligation under this Agreement and does not remedy such failure within thirty (30) days following written notice from Customer ***("ESO Default"),*** Customer may terminate this Agreement without incurring further liability, except for the payment of all accrued but unpaid Subscription Fees. If ESO is unable to provide Service(s) for ninety (90) consecutive days due to a Force Majeure event as defined in Section 16a, *Force Majeure,* Customer may terminate the affected Service(s) without liability to ESO.

b. Termination by ESQ for Customer Default. ESO may terminate this Agreement with no further liability if(i) Customer fails to pay for Services as required by this Agreement and such failure remains uncorrected for five (5) days following written notice from ESO, or (ii) Customer fails to perform any other material obligation under this Agreement and does not remedy such failure within thirty
(30) days following written notice from ESO (collectively referred to *as* ***"Customer Default").*** In the event of a Customer Default,
ESO shall have the right to (i) terminate this Agreement; (ii) suspend all Services being provided to Customer; (iii) terminate the right to use the Software on the web and/or mobile devices; (iv) apply interest to the amount past due, at the rate of one and one-half percent (I Y:,%) (or the maximum legal rate, if less) of the unpaid amount per month; (v) offset any amounts that are owed to Customer by ESO against the past due amount then owed to ESO; and/or (vi) take any action in connection with any other right or remedy ESO may have under this Agreement, at law or in equity. If ESO terminates this Agreement due to a Customer Default, Customer shall remain liable for all accrued Subscription Fees and other charges. In addition, Customer agrees to pay ESO's reasonable expenses (including attorney and collection fees) incurred in enforcing ESO's rights in the event of a Customer Default.

5. Delivery of Data upon Expiration or Termination of Agreement. If Customer requests its data within thirty (30) days of expiration of this Agreement, or the termination of this Agreement pursuant to Section 4 above, ESO shall deliver to Customer its data. ESO shall make reasonable and good faith efforts to accommodate Customer's preference for the type of media for delivery. Customer shall reimburse ESO for the cost of the media on which Customer's data is delivered to Customer.

6. **System Maintenance.** In the event ESO determines that it is necessary lo interrupt the Services or that there is a potential for Services to be interrupted for the performance of system maintenance, ESO will use good-faith efforts to notify Customer prior to the performance of such maintenance and will schedule such maintenance during non-peak hours (midnight to 6 a.m. Central Standard Time). In no event shall interruption of Services for system maintenance constitute a failure of performance by ESO.

7. **Access to Internet.** Customer has sole responsibility for obtaining, maintaining, and securing its connections to the Internet, and ESO makes no representations to Customer regarding the reliability, performance or security of any particular network or provider.

8. **Mobile Software.** If Customer elects to use ESO's Mobile Software (the ***"Software"),*** the provisions of this Section shall apply.

a. Use of Software. Subject to the terms, conditions and restrictions in this Agreement and in exchange for the Mobile Software Interface Fees and/or Subscription Fees, ESO hereby grants to Customer a non-exclusive, world-wide, non-transferable rights, for the Term of this Agreement, to use and copy (for installation and backup purposes only) the Software to the units for which the Mobile Software Interface has been purchased.

b. Ownership and Restrictions. 'I11is Agreement does not convey any rights of ownership in or title lo the Software or any copies thereof All right, title and interest in the Software and any copies or derivative works thereof shall remain the property of ESO. Customer will not: (i) disassemble, reverse engineer or modify the Software; (ii) allow any third party to use the Software; (iii) use the Software as a component in any product or service provided by Customer to a third party; (iv) transfer, sell, assign, or otl1erwise convey the Software; (v) remove any proprietary notices placed on or contained within the Software; or (vi) copy the Software except for backup purposes. Customer agrees to keep the Software free and clear of all claims, liens, and encumbrances.

c. Mobile Software Interface Fee. The Mobile Software Interface Fee is non-refundable. The Software shall be deemed accepted upon delivery to Customer.

d. Title. ESO hereby represents and warrants to Customer that ESO is the owner of the Software or otherwise has the right to grant to Customer the rights set forth in this Agreement. In the event of a breach or threatened breach of the foregoing representation and warranty, Customer's sole remedy shall be to require ESO to either: (i) procure, at ESO's expense, the right to use the Software, or
(ii) replace the Software or any part thereof that is in breach and replace it with Software of comparable functionality that does not cause any breach.

9. **Support and Updates.** During the Term of this Agreement, ESO shall provide Customer the support services and will meet the service levels as set forth in Exhibit B attached hereto and incorporated herein. ESO will also provide Updates lo Customer, in accordance with Exhibit B.

_ **to. Other Services.** Upon request by Customer, ESQ may provide services related to the Software other than the standard support described above at ESO's then-current labor rates. This may include on-site consultation, configuration, and initial technical assistance and training for the purpose of installing the Software and training selected personnel on the use and support of the Software. ESO shall undertake reasonable efforts to accommodate any written request by Customer for such professional services.

11. **Indemnification by ESQ.** To the extent permitted by law, ESO shall protect, defend, indemnify and hold the Customer harmless from and against all claims, demands, danmges, costs, actions and causes of actions, liabilities, fines, penalties, judgments, expenses and attorney fees, resulting from the injury or death of any person or the damage to or destruction of property, caused by ESO's gross negligence or willful misconduct in performing this Agreement, except for damages resulting from the negligence of the Customer. As to the Customer, ESO waives any immunity it may have under RCW Title 51 or any other Worker's Compensation statute. The parties acknowledge that this waiver has been negotiated by them.

ESO will indemnify Customer from and against intellectual property infringement claims caused by the Customer accessing the Services. The obligations set forth in this section do not apply if the third party claim is caused by, or results from: (a) Customer's combination or use of the Services with software, services, or products developed by Customer or third parties, if the claim would have been avoided by the non-combined or independent use of the Services; or (b) Participant's continued

allegedly infringing activity after being notified thereof or after being provided modifications that would have avoided the alleged infringement or (c) Customer's misuse of the Services, including but not limited to uploading infringing content.

12. **Limitation of Liability.** EXCEPT FOR ESQ'S INDEMNITY OBLIGATION UNDER THE FOREGOING PROVISION, CUSTOMER HEREBY AGREES THAT ESO'S TOTAL LIABILITY TO CITY FOR ANY AND ALL LIABILITIES, CLAIMS OR DAMAGES ARISING OUT OF OR RELATING TO TI-IIS CONTRACT, HOWSOEVER CAUSED AND REGARDLESS OF THE LEGAL THEORY ASSERTED, INCLUDING BREACH OF CONTRACT OR WARRANTY, TORT, STRICT LIABILITY, STATUTORY

LIABILITY OR OTHERWISE, SHALL NOT, IN THE AGGREGATE, EXCEED TI-IE AGGREGATE AMOUNT OF FEES PAID BY CUSTOMER AND KING COUNTY AS IT RELATES TO THIS AGREEMENT. UNDER ESQ'S INDEMNITY OBLIGATION, ESO'S TOTAL LIABILITY SHALL BE TWO-HUNDRED THOUSAND DOLLARS ($200,000.00) IN ADDITION TO THE AGGREGATE AMOUNT OF FEES PAID BY CUSTOMER AND KING COUNTY AS IT RELATES TO THIS AGREEMENT. IN NO EVENT SHALL EITHER ESO OR CUSTOMER BE LIABLE TO THE OTHER FOR ANY PUNITIVE, EXEMPLARY, SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, LOST PROFITS, LOST BUSINESS OPPORTUNITIES, LOSS OF USE OR EQUIPMENT DOWN TIME, AND LOSS OF OR CORRUPTION TO DATA) ARISING OUT OF OR RELATING TO THIS AGREEMENT, REGARDLESS OF THE LEGAL THEORY UNDER WHICH SUCH DAMAGES ARE SOUGHT, AND EVEN IF THE PARTIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

13. **Acknowledgements and Disclaimer of Warranties.** Customer acknowledges that ESO cannot guarantee that there will never be any outages in ESO network and that no credits shall be given in the event Customer's access to ESO's network is interrupted. THE SERVICES ARE PROVIDED "AS IS." UNLESS OTHERWISE SPECIFIED HEREIN, ESO MAKES NO REPRESENTATION OR WARRANTY TO CUSTOMER OR ANY OTHER PERSON OR ENTITY, WHETHER EXPRESS, IMPLIED OR STATUTORY, AS TO THE DESCRIPTION, QUALITY, MERCHANTABILITY, COMPLETENESS OR FITNESS FOR A PARTICULAR PURPOSE, OF ANY SERVICE OR SOFTWARE PROVIDED HEREUNDER OR DESCRIBED HEREIN, OR AS TO ANY OTHER MATTER (INCLUDING WITHOUT LIMITATION THAT THERE WILL BE NO IMPAIRMENT OF DATA OR THAT SERVICES WILL BE UNINTERRUPTED OR ERROR FREE), ALL OF WHICH WARRANTIES BY ESO ARE HEREBY EXCLUDED AND DISCLAIMED, TOTI-IE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

14. **Confidential Information.** ***"Confidential Information"*** shall mean all information disclosed in writing by one Party lo the other Party that is clearly marked "CONFIDENTIAL" or "PROPRIETARY" by the disclosing Party at the time of disclosure or which reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Confidential Information does not include any information that (i) was already known by the receiving Party free of any obligation to keep it confidential at the time of its disclosure; (ii) becomes publicly known through no wrongful act of the receiving Party; (iii) is rightfully received from a third person without knowledge of any confidential obligation; (iv) is independently acquired or developed without violating any of the obligations under this Agreement; or (v) is approved for release by written authorization of the disclosing Party.

The State of Washington's Public Records Act (Release/Disclosure of Public Records), under Washington State Law (reference RCW Chapter 42.56, the Public Records Act), deems all materials received or created by Customer to be public records. These records include but are not limited to bid or proposal submittals, agreement documents, contract work product, or other bid material.

The State of Washington's Public Records Act requires that publie records must be promptly disclosed by Customer upon request unless that RCW or another Washington State statute specifically exempts records from disclosure. Exemptions are narrow and explicit and are listed in Washington State Law (Reference RCW 42.56 and RCW 19.108).

As mentioned above, Customer is required to promptly make public records available upon request. However, under Washington State Law some records or portions of records may be considered legally exempt from disclosure. A list and description of records identified as exempt by the Public Records Act can be found in RCW 42.56 and RCW 19.108.

DRAFT

If Customer receives a public disclosure request for any records or parts of records that ESO has specifically identified in this contract as proprietary or confidential, Customer will notify ESO in writing of the request without unreasonable delay and will postpone disclosure. While it is not a legal obligation, Customer, as a courtesy, will allow ESO up to ten business days lo obtain and serve Customer with a court injunction to prevent Customer from releasing the records (reference RCW 42.56.540). IfESO fails to obtain a Court order and serve Customer within the *ten* days, Customer may release the documents.

Customer will not assert an exemption from disclosure on ESO's behalf. IfESO believes that its records are exempt from disclosure, Vendor is obligated to seek an injunction under RCW 42.56.540. ESO acknowledges that Customer will have no obligation or liability to ESO if the records are disclosed.

15. General Provisions.

a. Force Majeure. Neither Party shall be liable lo the other, nor deemed in default under this Agreement if and to the extent that such Party's performance of this Agreement is delayed or prevented by reason of Force Majcurc, which is defined to mean an event that is beyond the reasonable control of the affected Party and occurs without such Party's fault or negligence.

b. Entire Agreement. This Agreement, including all schedules, exhibits, addenda and any Business Associate Agreement (as that term is used in the Health Insurance Portability and Accountability Act and related regulations) *(see* Exhibit C) are incorporated herein by reference, constitutes the entire agreement between the Parties and supersedes all prior and contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter. No modification, amendment, or waiver of any provision of this agreement shall be effective unless in writing and signed by the Party against whom the modification, amendment or waiver is asserted.

c. Governing Law. This Agreement shall be governed by the laws of the State of Washington without regard to choice or conflict of law rules.

d. Arbitration. Any controversy or claim arising out of or relating to this Agreement, or a breach of this Agreement, shall be finally settled by arbitration in Seatlle, Washington, and shall be resolved under the laws of the State of Washington. The arbitration shall be conducted before a single arbitrator, who may be a private arbitrator, in accordance with the commercial rules and practices of the American Arbitration Association then in effect. Any award, order or judgment pursuant to such arbitration shall be deemed final and binding and may be enforced in any court of competent jurisdiction. The arbitrator may, as part of the arbitration award, permit the substantially prevailing Party to recover all or part of its attorney's fees and other out-of-pocket costs incurred in connection with such arbitration. All arbitration proceedings shall be conducted on a confidential basis. The Parties knowingly, voluntarily, and irrevocably waive their right to a trial by jury.

c. No Press Releases without Consent. Neither Party may use the other Party's name or trademarks, nor issue any publicity or public statements concerning the other Party or the existence or content of this Agreement, without the other Party's prior written consent. Notwithstanding, Customer agrees that ESO may use Customer's name and logo in ESO sales presentations, without Customer's prior written consent, during the Term of this Agreement, but only for the purposes of identifying the Customer as a customer of ESO. Likewise, Customer may use ESO's name and logo to identify ESQ as a vendor of Customer.

g. Aggregate Data Reporting. Customer hereby grants ESQ the right to collect and store its data for aggregate reporting purposes, but in no event shall ESQ disclose Protected Health Information ***("PHI")*** unless permitted by law. Moreover, ESO will not identify Customer without Customer's consent.

h. Compliance with Laws. Both Parties shall comply with and give all notices required by all applicable federal, state and local Jaws, ordinances, rules, regulations and lawful orders of any public authority bearing on the performance of this Agreement.

i. Waiver. No failure or delay by either Party in exercising any right under this Agreement shall constitute a waiver of that right. If Customer has made any change to the Agreement that Customer did not bring to ESQ's attention in a way that is reasonably calculated to put ESO on notice of the change, the change shall not become part of the Agreement.

DRAFT

j. Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision shall be modified by the court and interpreted so as best to accomplish the objectives of the original provision to the fullest extent permitted by law, and the remaining provisions of this Agreement shall remain in effect.

k. Taxes and Fees. This Agreement is exclusive of all taxes and fees. Unless otherwise required by Jaw, Customer is responsible for and will remit (or will reimburse ESQ for) all taxes of any kind, including sales, use, duty, customs, withholding, property, value- added, and other similar federal, state or local taxes (other than taxes based on ESO's income) assessed in connection with the Services and/or Software provided lo Customer under this Agreement.

l. Independent Contractor. Nothing in this Agreement shall be construed to create: (i) a partnership,joint venture or other joint business relationship between the Parties or any of their affiliates; or (ii) a relationship of employer and employee between the Parties. ESO is an independent contractor and not an agent of Customer.

I. Counteq:,arts: Execution. This Agreement and any amendments hereto may be executed by the Parties individually or in any combination, in one or more counterparts, each of which shall be an original and all of which shall together constitute one and the same agreement. Execution and delivery of this Agreement and any amendments by the Parties shall be legally valid and effective through: (i) executing and delivering the paper copy of the document, (ii) transmitting the executed paper copy of the documents by facsimile transmission or electronic mail in "portable document format" ***(".pdf')*** or other electronically scanned format, or (iii) creating, generating, sending, receiving or storing by electronic means this Agreement and any amendments, the execution of which is accomplished through use of an electronic process and executed or adopted by a Patty with the intent to execute this Agreement (i.e. ***"electronic signature"*** through a process such as DocuSign®). In making proof of this Agreement, it shall not be necessary to produce or account for more than one such counterpart executed by the Party against whom enforcement of this Agreement is sought.

m. Notice. All notices, requests, demands and other communications required or permitted to be given or made under this Agreement shall be in writing, shall be efiective upon receipt or attempted delivery, and shall be sent by (i) personal delivery; (ii) certified or registered United States mail, return receipt requested; (iii) overnight delivery service with proof of delivery, or (iv) fax. Notices shall be sent to the addresses above. No Party to this Agreement shall refuse delivery of any notice hereunder.

[Signature Page Follows]

IN WITNESS WHEREOF, the undersigned expressly agree and warrant that they are authorized to sign and enter into this Agreement on behalf of the Party for which they sign and have executed this Agreement on the Effective Date first written above.

ESO: **CUSTOMER:**

DocuSigned by:
Chris Dillie
E749AB441C2F496...
[Signature]

Chris Dillie
[Printed Name]

President and CEO

DRAFT

|S

[redacted]

Harold D. Scoggins

[Printed Name]

[redacted] n;K

[Title]

9/27/2016

DRAFT

[Title]

[Date] 10/6/2016 *[Date]*

EXHIBIT A

SCHEDULE OF SUBSCRIPTION FEES

Customer has selected the following Services, at the fees indicated:

EHR Suite w/ Quality Management, 60,000 - 80,000 Incidents.
List Price: $80,500.00, annually recurring. Fees
paid by King County EMS.

PAYMENT TERMS AND PAYMENT MILESTONES

The subscription year for Services shall begin upon execution of the Subscription Agreement or upon the commencement of active work on software implementation, whichever date comes later. The Subscription Fees arc invoiced annually in advance commencing upon execution of this Agreement.

EXHIBITB

SUPPORT SERVICES AND SERVICE LEVELS

This Exhibit describes the software support services ***("Support Services")*** that ESO will provide and the service levels that ESO will meet.

1. **Definitions.** Unless defined otherwise herein, capitalized terms used in this Exhibit shall have the same meaning as set forth in the Agreement.

(a}***"Customer Service Representative"*** shall be the person or persons at ESO designated by ESO to receive notices of Errors encountered by Customer that Customer's Administrator has been unable to resolve.

(b)***"Error"*** means any failure of the Software to conform in any material respect with its published specifications.

(c) ***"Error Correction"*** means a bug fix, patch, or other modification or addition that brings the Software into material conformity with its published performance specifications.

(d) ***"Priority A Error"*** means an Error that renders the Software inoperable or causes a complete failure of the Software leading to a major disruption/impact on Customer's operations.

(e)***"Priority B Error"*** means an Error that substantially degrades the performance of the Software or materially restricts Customer's use of the Software and/or one or more features or functions of the Software.

(f) ***"Priority C Error"*** means an Error that causes only a minor impact on Customer's use of the Software for which a work around may or may not exist.

(g) ***"Update"*** means any new commercially available or deployable version of the Software, which may include Error Corrections, enhancements or other modifications, issued by ESO fro111 time to time to its Customers.

(h)***"Normal Business Hours"*** means 7:00 am to 7:00 pm Monday through Friday, Central Time Zone.

DRAFT

2. Customer Obligations.

Customer will provide at least one administrative employee (the ***"Administrator"*** or ***"Administrators")*** who will handle all requests for first- level support from Customer's employees with respect to the Software. Such support is intended to be the "front line" for support and information about the Software to Customer's employees. ESO will provide training, documentation, and materials to the Administrators to enable the Administrators to provide technical support to Customer's employees. The Administrators will refer any Errors to ESO's Customer Service Representative that the Administrators cannot resolve, pursuant to Section 3 below; and the Administrators will assist ESO in gathering information to enable ESO to identify problems with respect to reported Errors.

3. Support Services.

(a) *Scope.* As further described herein, the Support Services consist of: (i) Error Corrections that the Administrator is unable to resolve and {ii) periodic delivery of Error Corrections and Updates. The Support Services will be available to Customer during normal business hours, but Customers may submit requests for a support assistance 24 hours per day, 7 days per week. Priority A Errors encountered outside normal business hours may be communicated to the Customer Service Representative via telephone or email. Priority B and C Errors encountered outside normal business hours shall be communicated via email.

(b) Procedure.

(i) *Report of Error.* In reporting any Error, the Customer's Administrator will describe to ESO's Customer Service Representative the Error in reasonable detail and the circumstances under which the Error occurred or is occurring; the Administrator will initially classify the Error as a Priority A, B or C Error. ESO reserves the right to reasonably reclassify the Priority of the Error.

(ii) *Efforts Required.* ESO shall exercise commercially reasonable efforts to correct any Error reported by the Administrator in accordance with the priority level assigned to such Error by the Administrator. Errors shall be communicated to ESO's Customer Service Representative after hours as indicated below, depending on the priority level of the Error. In the event of an Error, ESO will within the time periods set forth below, depending upon the priority level of the Error, commence verification of the Error; and, upon verification, will commence Error Correction. ESO will work diligently to verify the Error and, once an Error has been verified, and until an Error Correction has been provided to the Administrator, shall use commercially reasonable, diligent efforts to provide a workaround for the Error as soon as reasonably practicable. ESO will provide the Administrator with periodic reports on the status of the Error Correction on the frequency as indicated below. ESO may use multiple forms of communication for purposes of submitting periodic reports to Customer, including but not limited to, messages in the Software or messages appearing upon login or other means of broadcasting error reporting to multiple customers affected by the same Error.

(iii) Qualifications of Staff. The support desk will be staffed with competent technical consultants who are trained in and thoroughly familiar with the Software and with the Customer's applicable configuration. Telephone support and all communications will be delivered in understandable English.

(c) *Support Services.* The parties acknowledge that from time-to-time ESO may update his support processes specifically addressed in this Exhibit by posting such updates to ESO's website or otherwise notifying Customer of such updates. Customer will accept updates to ESO's support procedures and any other terms in this Exhibit; provided however, that they do not materially decrease the level of Support Services that Customer will receive from ESO.

ESO Solutions, Inc.

Priority of Error	Communicating Error to ESO outside Normal Business Hours	Time in Which ESO Will Commence Verification	Frequency of Periodic Status Reports	Response Process
Priorit y A	Telephone or email	Within 4 hours of notification	Every 2 hours until resolved	Prompt and ongoing effort, w continuous reporting to Cust until a work-around or fix has provided. A work-around acceptable as an interim solu pending resolution of the issue. Root cause failure r on all tickets classified as Pric will be provided lo Customer

Priorit y B	Email	Within 8 business hours of notification	Every **8** business hours until resolved	Proceed with fix as med priority work, according schedule mutually agreed lo by ESO and Customer.
Priority C	Email	Within three business days of notification	Every week until resolved	Proceed with fix as low pric work.

4. ESO Server Administration.

ESO is responsible for maintenance of Server hardware. Server administration includes:

(a) Monitoring and Response
(b) Service Availability Monitoring
(c) Backups
(d) Maintenance

(i) Microsoft Patch Management
(ii) Security patches to supported applications and related components
(iii) Event Log Monitoring
(iv) Log File Maintenance
(v) Drive Space Monitoring

(c) Security
(t) Virus Definition & Prevention
(g) Firewall

DRAFT

ESO Solulions, Inc.

EXHIBITC

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ***("Agreeme11f')*** is entered into by and between ESO Solutions, Inc. ***("Ve11dor"),*** a Texas corporation, and Customer ***("Covered E11tity"),*** as of the Effective Date of the Subscription Agreement, for the purpose of setting forth Business Associate Agreement terms between Covered Entity and Vendor. Covered Entity and Vendor each are

referred to as a ***"Ptuty"*** and collectively as the ***"Parties."*** This Agreement shall commence on the Effective Date set forth above.

WHEREAS, Covered Entity, owns, operates, manages, performs services for, otherwise are affiliated with or are themselves a Covered Entity as defined in the federal regulations at 45 C.F.R. Parts 160 and 164 (the ***"Privacy Sta11dards")*** promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 ***("HIPAA")*** and the Health Information Technology for Economic and Clinical Health Act of2009 ***("HITECH');***

WHEREAS, pursuant to HIPAA and HITECH, the U.S. Department of Health & Human Services ***("HHS")*** promulgated the Privacy Standards and the security standards at 45 C.F.R. Parts 160 and 164 (the***"Security Sta11dards")*** requiring certain individuals and entities subject to the Privacy Standards and/or the Security Standards to protect the privacy and security of certain individually identifiable health information ***("Protected Health /11formatio11"*** or***"PHI"),*** including electronic protected health information ***("EPHf');***

WHEREAS, the Parties wish to comply with Privacy Standards and Security Standards as amended by the HHS regulations promulgated on January 25, 2013, entitled the "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act," as such may be revised or amended by HHS from time to time:

WHEREAS, in connection with Vendor's performance under its agreement(s) or other documented arrangements between Vendor and Covered Entity, whether in effect as of the Effective Date or which be,eome effective at any time during the term of this Agreement (collectively ***"Busi11ess Arra11geme11ts"),*** Vendor may provide services for, or on behalf of, Covered Entity that require Vendor to use, disclose, receive, access, create, maintain and/or transmit health information that is protected by state and/or federal law; and

WHEREAS, Vendor and Covered Entity desire that Vendor obtain access to PHI and EPHI in accordance with the terms specified
herein;

DRAFT

NOW, THEREFORE, in consideration of the mutual promises set forth in this Agreement and the Business Arrangements, and
other good and valuable consideration, the sufficiency and receipt of which are hereby severally acknowledged, the Parties agree as follows:

I. **Vendor Obligations.**

In accordance with this Agreement and the Business Arrangements, Vendor may use, disclose, access, create, maintain, transmit, and/or receive on behalf of Covered Entity health information that is protected under applicable state and/or federal law, including without limitation, PHI and EPHI. All capitalized terms not otherwise defined in this Agreement shall have the meanings set forth in the regulations promulgated by HHS in accordance with HIPAA and HITECH, including the Privacy Standards and Security Standards (collectively referred to hereinafter as the ***"Co11jide1ttiality Requireme11ts").*** All reference to PHI herein shall be construed to include EPHI. PHI shall mean only that PHI Vendor uses, discloses, accesses, creates, maintains, transmits and/or receives for or on behalf of Covered Entity pursuan·t to the Business Arrangements. The Parties hereby acknowledge that the definition of PHI includes **"Genetic Information"** as set forth at 45 C.F.R. §160.103. To the extent Vendor is to carry out an obligation of Covered Entity under the Confidentiality Requirements, Vendor shall comply with the provision(s) of the Confidentiality Requirements that would apply to Covered Entity (as applicable) in the performance of such obligations(s).

2. Use of PHI.

Except as otherwise required by law, Vendor shall use PHI in compliance with this Agreement and 45 C.F.R. §164.504(e). Vendor agrees not to use PHI in a manner that would violate the Confidentiality Requirements if the PHI were used by Covered Entity in the same manner. Furthermore, Vendor shall use PHI for the purpose of performing services for, or on behalf of, Covered Entity as such services are defined in the Business Arrangements. In addition, Vendor may use PHI (i) as necessary for the proper management and administration of Vendor or to carry out its legal responsibilities; provided that such uses are permitted under federal and applicable state law, and (ii) to provide data aggregation services relating to the health care operations of the Covered Entity as defined by 45 C.F.R. § 164.501. Covered Entity also authorizes Vendor to collect and store its data for aggregate reporting, but in no event shall Vendor disclose PHI unless permitted by law. Moreover, Vendor will not identify Covered Entity without consent. Covered Entity authorizes Vendor to de-identify PHI it receives from Covered Entity. All de-identification of PHI must be performed in accordance with the Confidentiality Requirements, specifically 45 C.F.R. § 164.514(b).

3. Disclosure of PHI.

ESO Solutions, Inc.

3. I Subject to any limitations in this Agreement, Vendor may disclose PHI to any third party as necessary lo perform its obligations under the Business Arrangements and as permitted or required by applicable law. Vendor agrees not to disclose PHI in a manner that would violate the Confidentiality Requirements if the PHI was disclosed by the Covered Entity in the same manner. Further, Vendor may disclose PHI for the proper management and administration of Vendor; provided that: (i) such disclosures arc required by law; or (ii) Vendor: (a) obtains reasonable assurances from any third party to whom the PHI is disclosed that the PHI will be held confidential and used and disclosed only as required by law or for the purpose for which it was disclosed to third party, and (b) requires the third party to agree to immediately notify Vendor of any instances of which it is aware that PHI is being used or disclosed for a purpose that is not otherwise provided for in this Agreement or for a purpose not expressly permitted by the Confidentiality Requirements. Vendor shall report to Covered Entity any use or disclosure of PHI not permitted by this Agreement of which it becomes aware. Such report shall be made within five (5) business days of Vendor becoming aware of such use or disclosure.

3.2 If Vendor uses or contracts with any agent, including a subcontractor (collectively ***"Subcontractors")*** that uses, discloses, accesses, creates, receives, maintains or transmits PHI on behalf of Vendor, Vendor shall require all Subcontractors to agree in writing to the same restrictions and conditions that apply to Vendor under this

Agreement. In addition to Vendor's obligations under Section 9, Vendor agrees to mitigate, to the extent practical and unless othetwise requested by the Covered Entity, any harmful effect that is known to Vendor and is the result of a use or disclosure of PHI by Vendor or any Subcontractor in violation of this Agreement. Additionally, Vendor shall ensure that all disclosures of PHI by Vendor and its Subcontractors comply with the principle **of"minimum necessary use and disclosure,"** (i.e., in accordance with 45 C.F.R. *§*164.502(b), only the minimum PHI that is necessary to accomplish the intended purpose may be disclosed).

4. <u>Individual Rights Regarding Designated Record Sets</u>.

If Vendor maintains a Designated Record Set on behalf of Covered Entity, Vendor shall: (i) provide access to and permit inspection and copying of PHI by Covered Entity under conditions and limitations required under 45 C.F.R. *§* 164.524, as it may be amended from time to time; and (ii) amend PHI maintained by Vendor as required by Covered Entity. Vendor shall respond to any request from Covered Entity for access by an individual within ten (10) business days of such request and shall make any amendment requested by Covered Entity within twenty (20) business days of such request. Any information requested under this **Section 4** shall be provided in a form or format requested, if it is readily producible in such form or format. Vendor may charge a reasonable fee based upon Vendor's labor costs in responding to a request for electronic information (or a cost-based fee for the production of non-electronic media copies). Vendor shall notify Covered Entity within ten (I0) business days ofreceipt of any request for access or amendment by an individual.

5. <u>Accounting of Disclosures</u>.

Vendor shall make available to Covered Entity within ten (I0) business days of a request by Covered Entity the information required for an accounting of disclosures of PHI in accordance with 45 C.F.R. *§* 164.528 (or such shorter time as may be required by state or federal law). Such accounting must be provided without cost if it is the first accounting requested within any twelve (12) month period. For subsequent accountings within the same twelve (12) month period, Vendor may charge a reasonable fee based upon Vendor's labor costs in responding to a request for electronic information (or a cost-based fee for the production of non-electronic media copies) only after Vendor informs Covered Entity and Covered Entity informs the individual in advance of the fee, and the individual is afforded an opportunity to withdraw or modify the request. Such accounting obligations shall survive termination or expiration of this Agreement and with respect to any disclosure, whether on or before the termination of this Agreement, shall continue for a minimum of seven (7) years following the date of such disclosure.

6. <u>Withdrawal of Authorization</u>.

If the use or disclosure of PHI under this Agreement is based upon an individual's specific authorization regarding the use of his or her PHI, and: (i) the individual revokes such authorization in writing; (ii) the effective date of such authorization has expired; or (iii) the authorization is found to be defective in any manner that renders it invalid for whatever reason, then Vendor agrees, if it has received notice from Covered Entity of such revocation or invalidity, to cease the use and disclosure of any such individual's PHI except to the extent Vendor has relied on such use or disclosure, or where an exception under the Confidentiality Requirements expressly applies.

7. <u>Records and Audit</u>.

Vendor shall make available to HHS or its agents its internal practices, books, and records relating to the compliance of Vendorand Covered Entity with the Confidentiality Requirements, such internal practices, books and records to be provided in the time and manner designated by HHS or its agents.

8. <u>Implementation of Security Standards; Notice of Security Incidents</u>.

Vendor will comply with the Security Standards and, by way of example and not limitation, use appropriate safeguards to prevent the use or disclosure of PHI other than as expressly permitted under this Agreement. In accordance with the Security Standards, Vendor will implement administrative, physical, and technical safeguards that protect the confidentiality, integrity and availability of the PHI that it uses, discloses, accesses, creates, receives, maintains or transmits. To the extent feasible, Vendor will use commercially reasonable efforts to ensure that the technology safeguards used by Vendor to secure PHI will render such PHI unusable, unreadable and indecipherable to individuals

unauthorized to acquire or otherwise have access to such PHI. Vendor will promptly report to Covered Entity any Security

Incident of which it becomes aware; provided, however, that Covered Entity acknowledges and shall be deemed to have received notice from Vendor that there are routine occurrences of: (i) unsuccessful attempts to penetrate computer networks or services maintained by Vendor; and (ii) immaterial incidents such as "pinging" or "denial of services" attacks. At the request of Covered Entity, Vendor shall identify: the date of the Security Incident, the scope of the Security Incident, Vendor's response to the Security Incident, and to the extent pennitted by law, the identification of the party responsible for causing the Security Incident, if known.

9. Data Breach Notification and Mitigation.

9.1 HIPAA Data Breach Notification and Mitigation. Vendor agrees to implement reasonable systems for the discovery and prompt reporting of any "breach" of "unsecured PHI" as those terms are defined by 45 C.F.R. *§*164.402 ***("HfPAA Breach").*** The Parties acknowledge and agree that *45* C.F.R. *§§*164.404 and 164.410, as describe below in this **Section 9.1,** govern the determination of the date of a HIPAA Breach. In the event of any conflict between this **Section 9.1** and the Confidentiality Requirements, the more stringent requirements shall govern. Following the discovery ofa HIPAA Breach, Vendor will notify Covered Entity immediately and in no event later than five (5) business days after Vendor discovers such HIPAA Breach unless Vendor is prevented from doing so by 45 C.F.R. §164.412 concerning law enforcement investigations. For purposes of reporting a HIPM Breach to Covered Entity, the discovery ofa HIPAA Breach shall occur as of the first day on which such HIPAA Breach is known to Vendor or, by exercising reasonable diligence, would have been known to Vendor. Vendor will be considered to have had knowledge ofa HIPAA Breach if the HIPAA Breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the HIPAA Breach) who is an employee, officer or other agent of Vendor. No later than ten (10) business days following a HIPM Breach, Vendor shall provide Covered Entity with sufficient information to permit Covered Entity to comply with the HIPAA Breach notification requirements set forth at *45* C.F.R. §164.400 *et. seq.* This **Section 9.1** shall survive the expiration or termination of this Agreement and shall remain in effect for so long as Vendor maintains PHI.

9.2 Data Breach Notification and Mitigation Under Other Laws. In addition to the requirements of **Section 9.1,** Vendor agrees to implement reasonable systems for the discovery and prompt reporting of any breach of individually identifiable information (including, but not limited to, PHI and referred to hereinafter as ***"Imlividual/y ltlentijiable Information")*** that, if misused, disclosed, lost or stolen would trigger an obligation under one or more State data breach notification laws (each a***"State Breaclt")*** to notify the individuals who are the subject of the information. Vendor agrees that in the event any Individually Identifiable Information is lost, stolen, used or disclosed in violation of one or more State data breach notification laws, Vendor shall promptly: (i) notify Covered Entity within five (5) business days of such misuse, disclosure, loss or theft; and (ii) cooperate and assist Covered Entity with any investigation into any State Breach or alleged State Breach. This **Section 9.2** shall survive the expiration or termination of this Agreement and shall remain in effect for so long as Vendor maintains PHI or Individually Identifiable Information.

l 0. **Obligations of Covered Entity.**

10.1 Notification Requirement. Covered Entity shall notify Vendor of:

a. Any limitation(s) in Covered Entity's notice of privacy practices in accordance with *45* CFR 164.520 to the extent that such changes may affect Vendor's use or disclosure of **PHI;**

b. Any changes in, or revocation of, permission by Individual to use or disclose PHI, to the extent that such changes may affect Vendor's use or disclosure of PHI; and

c. Any restriction to the use or disclosure if PHI that Covered Entity has agreed to in accordance with *45* CFR 164.522, to the extent tl1at such restriction may affect Vendor's use or disclosure of PHI.

10.2 Pennissible Requests. Covered Entity agrees that it will not request Vendor to use or disclose PHI in any manner that would not be permissible under the Confidentiality Requirements if done by Covered Entity.

11. Terms and Termination.

11.1 Termination. This Agreement shall remain in effect until terminated in accordance with the terms of this **Section 11;** provided, however, that termination shall not affect the respective obligations or rights of the Parties

arising under this Agreement prior to the effective date of termination, all of which shall continue in accordance with their terms.

11.2 Termination with Cause. Either Party may immediately terminate this Agreement if either of the following events have occurred and are continuing to occur:

a. Vendor or Covered Entity fails to observe or perform any material covenant or obligation contained in this Agreement for ten (I 0) business days after written notice of such failure has been given; or

b. Vendor or Covered Entity violates any provision of the Confidentiality Requirement or applicable federal or state privacy law relating to its obligations under this Agreement.

11.3 May Terminate Business Arrangements in Event of for Cause Termination. Termination of this Agreement for either of the two reasons set forth in **Section 11.2** above shall be cause for immediate termination of any Business Arrangement pursuant to which Vendor uses, discloses, accesses, receives, creates, or transmits PHI for or on behalf of Covered Entity.

11.4 Termination Upon Conclusion of Business Arrangements. Upon the expiration or termination of all Business Arrangements, either Covered Entity or Vendor may terminate this Agreement by providing written notice to the other Party.

11.5 Return of PHI Upon Termination. Upon termination of this Agreement for any reason, Vendor agrees either to return all PHI or to destroy all PHI received from Covered Entity that is in the possession or control of Vendor or its Subcontractors. In the case of PHI for which it is not feasible to return or destroy, Vendor shall extend the protection of this Agreement to such PHI and limit further uses and disclosure of such PHI. Vendor shall comply with other applicable state or federal law, which may require a specific period of retention, redaction, or other treatment of such PHI. This **Section 11.5** shall survive the expiration or termination of this Agreement and shall remain in effect for so long as Vendor maintains PHI.

12. No Warranty.

PHI IS PROVIDED SOLELY ON AN "AS IS" BASIS. THE PARTIES DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

13. Ineligible Persons.

Vendor represents and warrants to Covered Entity that its directors, officers, and key employees: (i) are not currently excluded, debarred, or otherwise ineligible to participate in the federal health care programs as defined in 42 U.S.C. § 1320a-7b(f) of any state healthcare program (collectively, the ***"Healtltcare Programs");*** (ii) have not been convicted of a criminal offense related to the provision of healthcare items or services but have not yet been excluded, debarred, or otherwise declared ineligible to participate in the 1-lealtheare Programs; and (iii) are not under investigation or otherwise aware of any circumstances which may result in Vendor being excluded from participation in the Healthcare Programs (collectively, the ***"Wtlrrtmfy of No11-e.xclusio11").*** Vendor representations and warranties underlying the Warranty of Non-exclusion shall be ongoing during the term, and Vendor shall immediately notify Covered Entity of any change in the status of the representations and warranties set forth in this **Section 13.** Any breach of this **Section 13** shall give Covered Entity the right to terminate this Agreement immediately.

14. Equitable Relief.

The Parties understand and acknowledge that any disclosure or misappropriation of any PHI in violation of this Agreement will cause irreparable harm, the amount of which may be difficult to ascertain, and therefore agree that either Party shall have the right to apply to a court of competent jurisdiction for specific performance and/or an order restraining and enjoining any such further disclosure or breach and for such other relief deemed appropriate. Such right shall be in addition to the remedies otherwise available at law or in equity.

15. Entire Agreement.

This Agreement constitutes the complete agreement between Vendor and Covered Entity relating to the matters specified in this Agreement and supersedes all prior representations or agreements, whether oral or written with respect to such matters. In the event of any conflict between the terms of this Agreement and the terms of the Business Arrangements or any such later agreement(s), the terms of this Agreement shall control unless the terms of such Business Arrangements are more strict with respect to PHI and comply with the Confidentiality Requirements, or the Parties specifically otherwise agree in writing. No oral modification or waiver of any of the provisions of this Agreement shall be binding on either Party to this Agreement; *provided, however* that upon the enactment of any law, regulation, court decision or relevant government publication and/or interpretive guidance or policy that a Party believes in good faith will adversely impact the use or disclosure of PHI under this Agreement, that Party may amend the Agreement to comply with such law, regulation, court decision or government publication, guidance or policy by delivering a written amendment to the other Party which shall be effective thirty (30) calendar days after receipt. No obligation on either Party to enter into any transaction is to be implied from the execution or delivery of this Agreement. This Agreement is for the benefit of, and shall be binding upon the Parties, their affiliates and respective successors and assigns.

EXHIBITD

Seattle Fire Department

With

ESQ Solutions Inc.

CONSULTANTAGREEMENT

Title: ePRC Software Services

AGREEMENT NUMBER: 160147

This Agreement is made and entered into by and between the City of Seattle ("the City"), a Washington municipal corporation, through its Fire department as represented by the Chief; and ESO Solutions Inc. ("Consultant"), a corporation of the State of Texas and authorized to do business in the State of Washington.

WHEREAS, Consultant and City have entered into a separate Subscription Agreement to which this Consultant Agreement is attached as an exhibit; and

WHEREAS, Consultant is performing additional development work on behalf of City which is further detailed in this Exhibit D.

DRAFT

The Parties agree that the terms and conditions of this Exhibit E are in addition to, not in lieu of, the terms and conditions contained in the Subscription Agreement to which this Exhibit E is attached. In the event of a conflict between the language of this Exhibit E and the Subscription Agreement, the Subscription Agreement shall control.

1. TERM OF AGREEMENT.

The term of this Agreement begins when fully executed by all parties, and ends upon the completion of the projects detailed under Attachment A to this Exhibit, unless amended by written agreement or terminated earlier under termination provisions.

2. TIME OF BEGINNING AND COMPLETION.

The Consultant shall begin the work outlined in the "Scope of Work" ('Work") included as Attachment A to this Exhibit D upon receipt of written notice to proceed from the City. The City will acknowledge in writing when the Work is complete. Time limits established under this Agreement shall not be extended because of delays for which the Consultant is responsible, but may be extended by the City, in writing, for the City's convenience or conditions beyond the Consultant's control.

3. SCOPE OF WORK.

The Scope of Work for this Agreement and the time schedule for completion of such Work are described in Attachment A, which is attached to and made a part of this Agreement.

The Work is subject to City review and approval. The Cons.ultant shall confer with the City periodically, and prepare and present information and materials (e.g. detailed outline of completed Work) requested by the City to determine the adequacy of the Work or Consultant's progress.

4. PAYMENT AND REIMBURSEMENT.

The Consultant shall be compensated at a firm fixed rate of $37,790.00. The parties agree that the rate includes all direct, indirect, and overhead costs, including travel and living expenses, incurred by the Consultant in performance of the Services. There is no guarantee of a minimum amount of work or payment under this Agreement.

5. PROMPT PAY.

Definitions

A. An invoice is considered received when it is date-stamped at point of entry into the department. If the invoice is not date-stamped or otherwise marked as received by a department, the date of the invoice will be considered the date the invoice is received.

B. A payment is considered made on the day it is mailed or is available.

C. Disputed items include, but are not restricted to, improperly prepared invoices, lack of appropriate supporting documentation, unapproved staff or staff rates on the invoice, and unsatisfactory work product or services.

Prompt Payment to Consultant

A. Timely Payment: Except as provided otherwise herein, payment for an invoice will be made to the Consultant within thirty (30) calendar days of receipt of the invoice.

B. Disputed Items: The City may withhold payment for disputed items. The City will promptly notify the Consultant in writing, outlining the disputed items, the amount withheld and actions the Consultant must take to resolve the disputed items. The City default is to delay payment until a revised invoice is submitted and approved. However, the Consultant may request partial payment for the approved amounts, if the unapproved amount represents a small share of the total invoice. The City shall pay the revised invoice within thirty (30) calendar days of receipt.

C. Interest Payment: The City will agree to pay one percent (1%) interest per month, for payments made after thirty (30) calendar days from receipt of an invoice, on undisputed invoice amounts.

D. Legal Fees: In any action brought to collect interest due under this Section, the prevailing party is entitled to an award of reasonable attorney fees.

Prompt Payment to Subconsultants

A. Cut-Off Date: Except as provided otherwise herein, payment for an invoice will be made to a subconsultant within thirty (30) calendar days of receipt by the Consultant. The Consultant may establish a monthly cut-off date of *(to be established by Prime)* that subconsultants must submit an invoice in order to assure 30-day payment.

B. Disputed Items: The Consultant may withhold payment for disputed items. The Consultant will promptly notify the subconsultant in writing, outlining disputed items, the amount withheld and actions the subconsultant must take to resolve the disputed item(s). Such withheld amounts are limited only to items in dispute. The subconsultant can request partial payment for the approved amounts, or that the Consultant delay their entire payment until a revised invoice is submitted to and accepted by the Consultant. The Consultant shall pay the revised invoice within thirty (30) calendar days of receipt.

D. Interest Payment: The Consultant will agree to pay one percent (1%) interest per month, for payments made after thirty (30) calendar days from receipt of an invoice, on undisputed invoice amounts.

E. Flow-Down Clauses: The Consultant shall require this provision in each subcontract of any tier.

6. PAYMENT PROCEDURES.

The Consultant shall submit an invoice after all deliverables have been approved and accepted by the City. Payment will be made within 30 days of receipt of a correct invoice.

The invoices should

be submitted to:

Seattle Fire

Department
Attn: Jim Hominiuk
PO Box 94729
Seattle, WA 98124-
4729
James.Hominiuk@sea
ttle.gov

See attached checklist for further instructions.

DRAFT

Invoices must clearly display the following (sub-consultants' invoices must also include this information):

- Invoice Date and Invoice Number
- City Project Manager Name: Rene LeBeau
  (Please do not put PM's name in the address)
- Department Contract No. 160136
- Contract Title: Implementation Services for Democracy Voucher Project
- Period covered by the invoice
- Task # and title
- Employee's name and classification
- Employee's all-inclusive hourly rate and # of hours worked
- Total labor costs per task
- Itemization of direct, non-salary costs (per task, if so allocated)
- The following Sub-Consultant payment information will be provided (attach Sub-Consultant invoices as backup):
  - Amount Paid to all Sub-Consultants for the invoice period (list separate totals for each Sub-Consultant).
  - Cumulative To-Date amount paid to all Sub-Consultants (list separate totals for each Sub-Consultant).
- Cumulative costs per task and for the total project

7. TAXES, FEES AND LICENSES.

A. Consultant shall pay and maintain in current status, all necessary licenses, fees, assessments, permit charges, etc. It the Consultant's sole responsibility to monitor and determine changes or the enactment of any subsequent requirements for said fees, assessments, or changes and to immediately comply.

B. Where required by state statute, ordinance or regulation, Consultant shall pay and maintain in current status all taxes necessary for performance. Consultant shall not charge the City for federal excise taxes. The City will furnish Consultant an exemption certificate where appropriate.

C. As authorized by SMC, the Director of Finance and Administrative Services may withhold payment pending satisfactory resolution of unpaid taxes and fees due the City.

8. ADDRESSES FOR NOTICES AND DELIVERABLE MATERIALS.

Deliver all official notices under this Agreement to:

If to the City: James Hominiuk Seattle Fire Department
Fire Station #10 - SFD Headquarters Seattle, WA
98104 James.Hominiuk@seattle.gov
206-386-1476

If to the Consultant: Scott Kelly
ESO Solutions Inc.
9020 N Capital of Texas Hwy Building 2 Suite 300
Austin, TX 78759 scott.kelly@esosolutions.com 512-308-6508

Deliver all deliverable materials under this Agreement to:

If to the City:

If to the Consultant:

DRAFT

James Hominiuk Seattle Fire Department
Fire Station #10 - SFD Headquarters Seattle, WA 98104
James.Hominiuk@seattle.gov
206-386-1476

Scott Kelly
ESO Solutions Inc.
9020 N Capital of Texas Hwy Building 2 Suite 300
Austin, TX 78759 scott.kelly@esosolutions.com
512-308-6508

9. SOCIAL EQUITYREQUIREMENTS.

Consultant shall not discriminate against any employee or applicant for employment because of race, color, age, sex, marital status, sexual orientation, gender identity, political ideology, creed, religion, ancestry, national origin, honorably discharged veteran or military status or the presence of any sensory, mental or physical handicap, unless based upon a bona fide occupational qualification. The Consultant shall affirmatively try to ensure applicants are employed, and employees are treated during employment, without regard to race, color, age, sex, marital status, sexual orientation, gender identify, political ideology, creed, religion, ancestry, national origin, honorably discharged veteran or military status or the presence of any sensory, mental or physical handicap. Such efforts include, but are not limited to employment, upgrading, demotion, transfer, recruitment, layoff, termination, rates of pay or other compensation, and training. Consultant shall seek inclusion of woman and minority business for subcontracting. A woman or minority business is one that self-identifies to be at least 51% owned by a woman and/or minority. Such firms do not have to be certified by the State of Washington but must be registered in the City Online Business Directory.

Inclusion efforts may include the use of solicitation lists, advertisements in publications directed to minority communities, breaking down total requirements into smaller tasks or quantities where economically feasible, making schedule or requirement modifications that assist WMBE businesses to compete, targeted recruitment, mentorships, using consultants or minority community organizations for outreach, and selection strategies that result in greater subconsultant diversity.

10. INDEMNIFICATION.

Omitted.

11. INSURANCE.

Insurance is required; however, insurance certification does not need to be submitted to the City. Consultant will maintain premises and vehicle liability insurance in force with coverages and limits of liability generally maintained by similarly situated consultants and workers compensation insurance as required by Washington State statutes.

12. AUDIT.

Omitted.

13. INDEPENDENT CONSULTANT.

DRAFT

A. The Consultant is an independent Consultant. This Agreement does not intend the Consultant to act as a City employee. The City has neither direct nor immediate control over the Consultant or the right to control the manner or means by which the Consultant works. Neither the Consultant nor any Consultant employee shall be an employee of the City. This Agreement prohibits the Consultant to act as an agent or legal representative of the City. The Consultant is not granted express or implied rights or authority to assume or create any obligation or responsibility for or in the name of the City, or to bind the City. The City is not liable for or obligated to pay sick leave, vacation pay, or any other benefit of employment, nor to pay social security or other tax that may arise from employment. The Consultant shall pay all income and other taxes as due. The Consultant may perform work for other parties; the City is not the exclusive user of the services that the Consultant provides.
B. If the City needs the Consultant to Work on City premises and/or with City equipment, the City may provide the necessary premises and equipment. Such premises and equipment are exclusively for the Work and not to be used for any otherpurpose.
C. If the Consultant works on the City premises using City equipment, the Consultant remains an independent Consultant and does not as a City employee. The Consultant will notify the City Project Manager ifs/he or any other Workers are within 90 days of a consecutive 36-month placement on City property. If the City determines using City premises or equipment is unnecessary to complete the Work, the Consultant will be required to work from its own office space or in the field. The City may negotiate a reduction in Consultant fees or charge a rental fee based on the actual costs to the City, for City premises or equipment.

14. KEY PERSONS.

Omitted.

15. ASSIGNMENT AND SUBCONTRACTING.

The Consultant shall not assign or subcontract its obligations under this Agreement without the City's written consent, which may be granted or withheld in the City's sole discretion. Any subcontract made by the Consultant shall incorporate by reference this Agreement, except as otherwise provided. The Consultant shall ensure that all subconsultants comply with the obligations and requirements of the subcontract. The City's consent to any assignment or subcontract does not release the consultant from liability or any obligation within this Agreement, whether before or after City consent, assignment or subcontract.

16. FEDERAL DEBARMENT.

The Consultant shall immediately notify the City of any suspension or debarment or other action that excludes the Consultant or any subconsultant from participation in Federal contracts. Consultant shall verify all subconsultants intended and/or used by the Consultant for performance of City Work are in good standing a.nd are not debarred, suspended or otherwise ineligible by the Federal Government. Debarment shall be verified at https://www.sam.gov. Consultant shall keep proof of such verification within the Consultant records.

17. CITY ETHICS CODE (SMC 4.16.010 TO .105).

A. Consultant shall promptly notify the City in writing of any person expected to be a Consultant Worker (including any Consultant employee, subconsultant, principal, or owner) and was a former City officer or employee within the past twelve (12) months.
B. Consultant shall ensure compliance with the City Ethics Code by any Consultant Worker when the Work or matter related to the Work is performed by a Consultant Worker who has been a City officer or employee within the past two years.

C. Consultant shall provide written notice to the City of any Consultant worker who shall or is expected to perform over 1,000 hours of contract work for the City within a rolling 12-month period. Such hours include those performed for the Consultant and other hours that the worker performed for the City under any other contract. Such workers are subject to the City Ethics Code, SMC 4.16. The Consultant shall advise their Consultant Workers.

D. Consultant shall not directly or indirectly offer anything of value (such as retainers, loans, entertainment, favors, gifts, tickets, trips, favors, bonl.lses, donations, special discounts, work or meals) to any City employee, volunteer or official that is intended, or may appear to a reasonable person to be intended, to obtain or give special consideration to the Consultant. Promotional items worth less than $25 may be distributed by the Consultant to City employees if the Consultant uses the items as routine and standard promotional materials. Any violation of this provision may cause termination of this Agreement. Nothing in this Agreement prohibits donations to campaigns for election to City office, so long as the donation is disclosed as required by the election campaign disclosure laws of the City and of the State.

18. NO CONFLICT OF INTEREST.

Consultant confirms that the Consultant or workers have no business interest or a closefamily relationship with any City officer or employee who was or will be involved in the consultant selection, negotiation, drafting, signing, administration or evaluation of the Consultant's work. As used in this Section, the term Consultant includes any worker of the Consultant who was, is, or will be, involved in negotiation, drafting, signing, administration or performance of the Agreement. The term "close family relationship" refers to: spouse or domestic partner, any dependent parent, parent-in-law, child, son-in-law, daughter-in-law; or any parent, parent in-law, sibling, uncle, aunt, cousin, niece or nephew residing in the household of a City officer or employee described above.

19. ERRORS AND OMMISSIONS, CORRECTIONS.

Consultant is responsible for professional quality, technical accuracy, and the coordination of all designs, drawings, specifications, and other services furnished by or on the behalf of the Consultant under this Agreement. Consultant, without additional compensation, shall correct or revise errors or mistakes in designs, drawings, specifications, and/or other consultant services immediately upon notification by the City. The obligation provided for in this Section regarding acts or omissions resulting from this Agreement survives Agreement termination or expiration.

20. INTELLECTUAL PROPERTY RIGHTS.

A. Omitted.

B. The City may make and retain copies of instructional or technical documents prepared by the Consultant for its information and reference with their use on the project. The Consultant does not represent or warrant that such documents are suitable for reuse by the City or others, on extensions of the project or on any other project.

21. PROPRIETARY AND CONFIDENTIALINFORMATION.

Omitted.

22. DISPUTES.

Any dispute or misunderstanding that may arise under this Agreement, concerning the Consultant's performance, shall first be through negotiations, if possible, between the Consultant's Project Manager and the City's Project Manager. It shall be referred to the Director and the Consultant's senior executive(s). If such officials do not agree upon a decision within a reasonable period of time, either party may decline or discontinue such discussions and may then pursue the legal means to resolve such disputes, including but not limited to alternative dispute resolution processes. Nothing in this dispute process shall mitigate the rights of the City to terminate the contract.

Notwithstanding all of the above, if the City believes in good faith that some portion of the Work has not

DRAFT

been completed satisfactorily, the City may require the Consultant to correct such work prior to the City payment. The City will provide to the Consultant an explanation of the concern and the remedy that the City expects. The City may withhold from any payment otherwise due, an amount that the City in good faith finds to be under dispute, or if the Consultant provides no sufficient remedy, the City may retain the amount equal to the cost to the City for otherwise correcting or remedying the work not properly completed.

23. TERMINATION.

A. For Cause: The City may terminate the Agreement if the Consultant is in material breach of this Agreement, and such breach has not been corrected to the City's reasonable satisfaction in a timely manner.
B. For Reasons Beyond Control of Parties: Either party may terminate this Agreement without recourse by the other where performance is rendered impossible or impracticable for reasons beyond such party's reasonable control, such as, but not limited to, an act of nature, war or warlike operation, civil commotion, riot, labor dispute including strike, walkout or lockout, except labor disputes involving the Consultant's own employees, sabotage, or superior governmental regulation or control.
C. For City's Convenience: The City may terminate this Agreement without cause and including the City's convenience, upon written notice to the Consultant.
D. Notice: Notice of termination under this Section shall be given by the party terminating this Agreement to the other, not fewer than five (5) business days prior to the effective date of termination.
E. Actions upon Termination: if termination occurs not the fault of the Consultant, the Consultant shall be paid for the services properly performed prior to termination, with any reimbursable expenses then due, but such compensation shall not exceed the maximum compensation to be paid under the Agreement. The Consultant agrees this payment shall fully and adequately compensate the Consultant and all subconsultants for all profits, costs, expenses, losses, liabilities, damages, taxes and charges of any kind (whether foreseen or unforeseen) attributable to the termination of this Agreement.
F. Omitted.

24. CONSULTANT PERFORMANCE EVALUATION.

The Consultant's performance will be evaluated by the City at the conclusion of the contract. The Evaluation template can be viewed http://www.seattle.gov/contracting/docs/ccPE.doc.

25. DEBARMENT.

Under SMC Chapter 20.70, the Director of City Purchasing and Contracting Services (CPCS), as hereby delegated by the Director of Finance and Administrative Services, may debar a and prevent a Consultant from contracting or subconsultant with the City for up to five years after determining the Consultant:

A. Received overall performance evaluations of deficient, inadequate, or substandard performance on three or more City contracts;
B. Failed to comply with City ordinances or contract terms, including but not limited to, ordinance or contract terms
related to woman and minority business utilization, discrimination, equal benefits, or other state, local or federal non-discrimination laws;
C. Abandoned, surrendered, or failed to complete or to perform work on or for a City contract;
D. Failed to comply with contract provisions, including but not limited to quality of workmanship, timeliness of performance, and safety standards;
E. Submitted false or intentionally misleading documents, reports, invoices, or other statements to the City in connection with a contract;
F. Colluded with another firm to restrain competition;
G. Committed fraud or a criminal offense in connection with obtaining, attempting to obtain, or performir:ig a contract for the City or any other government entity;
H. Failed to cooperate in a City debarment investigation.

The CPCS Director or designee may issue an Order of Debarment under the SMC 20.70.050. Rights and remedies of the City under these provisions are besides other rights and remedies provided by law or under the Agreement.

26. MISCELLANEOUS PROVISIONS.

A. Amendments: No modification of this Agreement shall be effective unless in writing and signed by an authorized representative of each of the parties hereto.
B. Background Checks and Immigrant Status: The City has strict policies regarding the use of Background checks, criminal checks and immigrant status for contract workers. The policies are incorporated into the contract and available for viewing on-line at http://www.seattle.gov/business/WithSeattle.htm
C. Binding Agreement: This Agreement shall not be binding until signed by both parties. The provisions, covenants and conditions in this Agreement shall bind the parties, their legal heirs, representatives, successors and assigns.
D. The Consultant, at no expense to the City, shall comply with all laws of the United States and Washington, the Charter and ordinances of the City of Seattle; and rules, regulations, orders and directives of their administrative agencies and officers. Without limiting the generality of this paragraph, the Consultant shall comply with the requirements of this Section.
E. Omitted.
F. Omitted.
G. Captions: The titles of sections or subsections are for convenience only and do not define or limit the contents.
H. Severability: If any term or provision is determined by a court of competent jurisdiction to be invalid or unenforceable, the remainder of this Agreement shall not be affected, and each term and provision shall be valid and enforceable to the fullest extent permitted by law.
I. Waiver: No covenant, term or condition or the breach shall be deemed waived, except by written consent of the party against whom the waiver is claimed, and any waiver of the breach of any covenant, term or condition shall not be deemed a waiver of any preceding or succeeding breach of the same or any other covenant, term of condition. Neither the acceptance by the City of any performance by the Consultant after the time the same shall have become due nor payment to the Consultant for any portion of the Work shall constitute a waiver by the City of the breach or default of any covenant, term or condition unless otherwise expressly agreed to by the City in writing.
J. Entire Agreement: Omitted.
K. Negotiated Agreement: The parties acknowledge this is a negotiated agreement, that they have had this Agreement reviewed by their respective legal counsel, and that the terms and conditions of this Agreement are not to be construed against any party on the basis of such party's draftsmanship.
L. No personal liability: No officer, agent or authorized employee of the City shall be personally responsible for any liability arising under this Contract, whether expressed or implied, nor for any statement or representation made or in any connection with this Agreement.

ATTACHMENT A TO EXHIBIT D STATEMENT OF WORK

This Statement of Work **("SOW")** is made and entered into as of the effective date of the Subscription Agreement to which this serves as Attachment A to Exhibit D **("SOW Effective Date")** by and between the City of Seattle **("Customer")** and ESO Solutions, Inc., a Texas corporation with a principal place of business at 9020 North Capital of Texas Highway, Building II-300, Austin, TX 78759 **("Company"),** and is subject to the terms and conditions of the Agreement.

I. Description of Services and Milestones

1. CAD Interface: One of ESO's experienced technicians will install ESO's CAD Interface onto Customer's system to allow the functional use of CAD data within ESO's software. ESO predicts that, with compliance from Customer's CAD vendor, ESO will be capable of completing installation of the CAD

Interface described herein within two weeks of project initiation.

2. Cardiac Monitor Interface: Customer shall install ESO's Cardiac Monitor Interface application onto Customer's devices. ESO shall assist Customer in the installation process as a part of its implementation process, but the installation process shall be undertaken by Customer at Customer's facilities. The time frame for completion is dependent on Customer efforts.
3. ESO's Mobile Software: Customer will install ESO's mobile application on Customer's laptops, tablets, or other compatible mobile devices. ESO shall assist Customer in the installation process as a part of its implementation process, but the installation process will be primarily undertaken by Customer at Customer's facilities. The time frame for completion is dependent on Customer efforts.

Deliverables

I. ESO's CAD Interface shall be installed by an ESO technician. The ESO CAD Interface is designed to bring CAD data into ESO's system for use by the end user as they document incidents.
2. ESO's Cardiac Monitor Interface transmits data from Customer's cardiac monitor to ESO's mobile software. The software will be made available to Customer, and installed by Customer with support from ESO.
3. ESO's Mobile application allows for the offline collection of patient health information while in a mobile usage setting, as well as cardiac monitor integration (described in point 2 of this section.)

Assumptions and Requirements

I. The method in which ESO's CAD Interface is designed is dependent on the CAD system being used and the preference of the CAD system host and agency requesting the interface. It is important to note that there is development required on the part of the CAD vendor (and potentially, additional costs from the CAD vendor to Customer.) ESO may be unable to provide Deliverable I should Customer CAD Vendor be non-compliant with the requirements of this project, in which case Customer shall receive a full refund of CAD Interface fees as further described on Attachment B to Exhibit D.
2. ESO's Cardiac Monitor Interface will not function if Customer's cardiac monitors are not capable of transmitting data through either a cable connection, Bluetooth, or Wi-Fi.
3. ESO Mobile Software will only function on devices capable of meeting its technical specifications, attached hereto as Attachment C to Exhibit D.

II. **Fees (indicate all that apply)**

X_ **Fixed Price of$37,790.00**

X_ The above Fixed Price includes Materials and Expenses.

_ The above Fixed Price does not include Materials and Expenses.

III. **Not-to-Exceed Amount**

Under no circumstances shall the amounts payable under this SOW (including fees, materials and expenses) exceed
$37,790.00 (the "not-to-exceed amount").

IV Additional Terms

The projects described in this SOW require Customer to complete ESO's ePCR implementation process before they can be undertaken. Projects may be delayed should ESO's ePCR implementation meet delays. All projects described herein require active Customer participation and may be subject to delays dependent on Customer's availability.

ATTACHMENT B TO EXHIBIT D
Statement of Work Pricing

Customer has selected the following Services, at the fees indicated:

Product	Quantity	List Price	Total Price	Line Item Description
EHR Mobile	40.00	$695.00	$27,800.00	One-time unlimited mobile fee

Intedaoe - CAO (ESO APO lie@ $5.995.00 OM-'I!I1'MI

!niedaoo - Monillor $3995.00 One-!iim@lie@

Grand Total $37.790

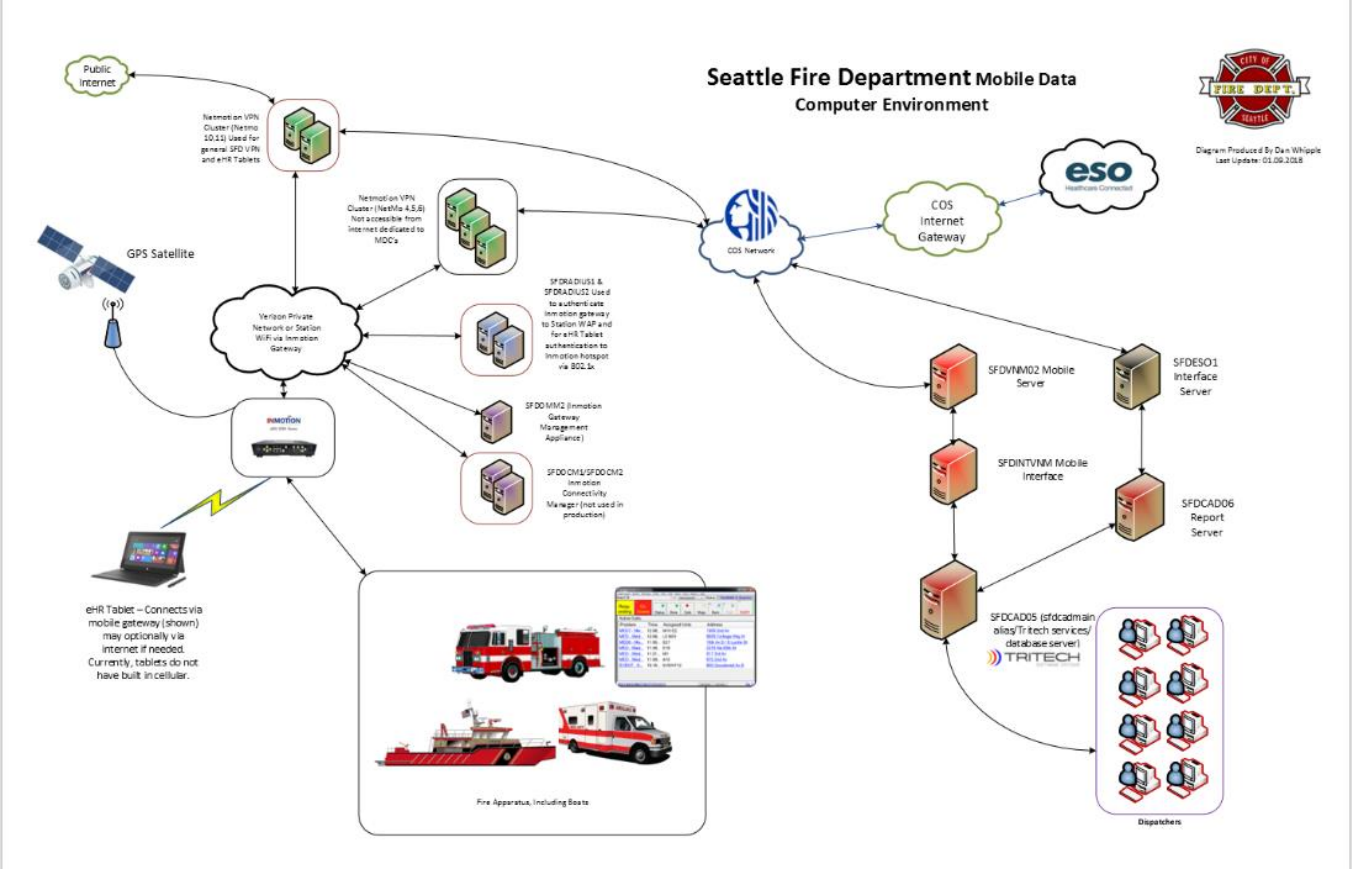
PAYMENT TERMS AND PAYMENT MILESTONES

The fees detailed above are invoiced in advance commencing upon execution of this Statement of Work.

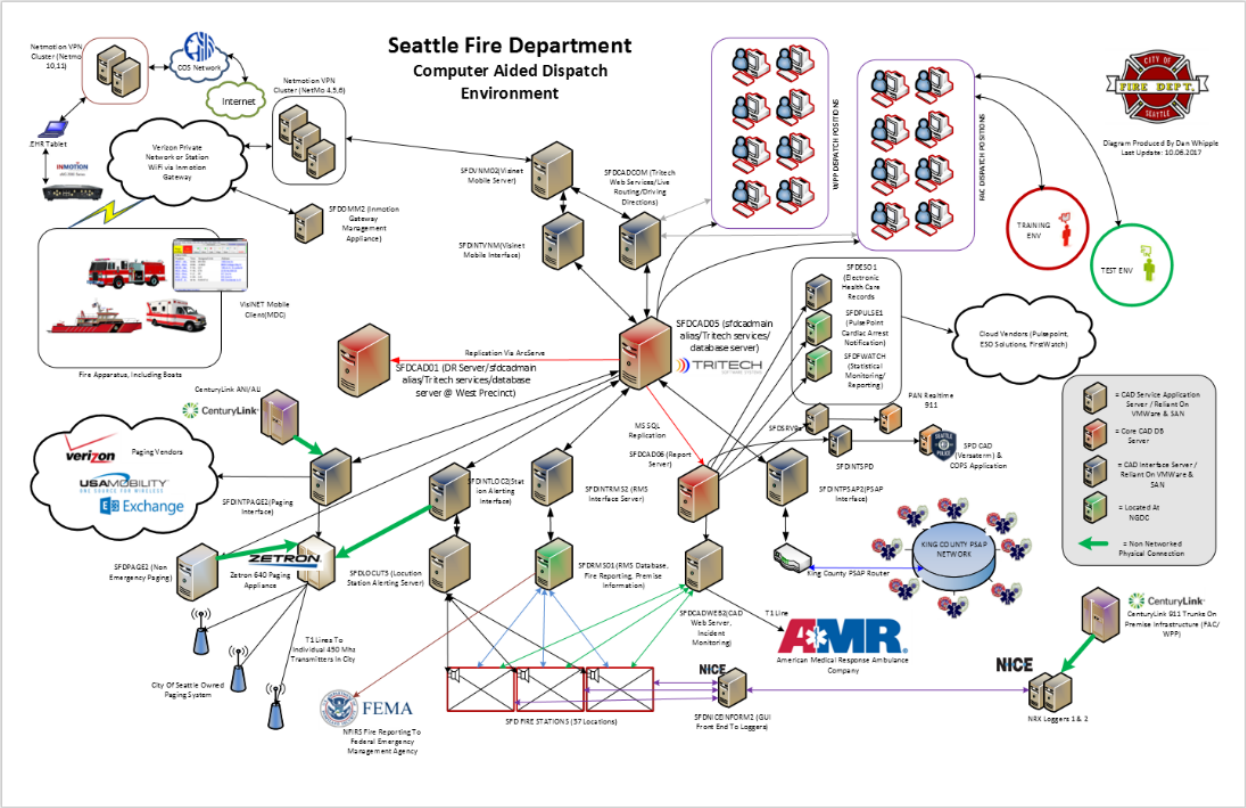
DRAFT

DRAFT

Seattle Fire Department: Mobile Data Computer Environment



Seattle Fire Department: Computer Aided Dispatch Environment



Training and Operational Resources

CAD Training Material: Incident Type Code

DRAFT

TYPE CODE	STANDARD RESPONSE	DESCRIPTION	USE	RELATED SOP
1RED	**1 Fire Unit**	**Nearest engine or ladder code red**	**Dispatcher discretion type codes, used for when dispatcher is unsure of which type code to use or wants to increase resources for the response.**	
3RED	**1 Engine, 1 Ladder, 1 BC**			
4RED	**2 Engines, 1 Ladder, 1 BC**			
ADV		**Advised**	**Type code used primarily for documentation purposes**	
AFA	**Per 5-Level Response Plan**	**Auto Fire Alarm**		
AFA4	**2 Engines, 1 Ladder, 1 BC**	**AFA with Waterflow indication**		
AFAF-Y	**1 Fire Unit (Code Yellow)**	**Auto Fire Alarm, False**		
AFAH	**2 Engines, 1 Ladder, 1 BC, Air 9, DEP1, SAFT2** **HazMat Group:** E10, L1, A10, HAZ1, STAF10	**Auto Fire Alarm, Hazardous Materials**		
AFAR	**1 Fire Unit**	**Auto Fire Alarm Residential**		
AFARF-Y	**1 Fire Unit (Code Yellow)**	**Auto Fire Alarm Residential False**		
AID	**1 Unit**	**Aid Response**		
AIDF	**2 Engines, 1 Aid Car**	**Freeway Aid Response**		840
AIDYEL-Y	**1 Unit (Code Yellow)**	**Code Yellow Aid Response**		

DRAFT

AIRCRASH	**5 Engines, 2 Ladders, 2 BCs, 1 Aid Car, 1 Medic Unit, Air 9, M44, DEP1, SAFT2, STAF10, REHAB1, RIG Engine, RIG Ladder**	**Aircraft Crash**		700

TYPE CODE	STANDARD RESPONSE	DESCRIPTION	USE	RELATED SOP
AIRSBY-y	**1 Fire Unit (Code Yellow)**	**Aircraft Standby**	**Mutual Aid to Boeing Field for Aircraft in Trouble**	
ALBELL	**1 Fire Unit**	**Alarm Bell Ringing**		
AMA	**1 Unit**	**Auto Medical Alarm**		
AMB	**Transfer to AMR**	**Transfer to AMR**		385
ANTIB-Y	**2 Chempack Engines**	**Respond to North Chempack site for Antibiotic Deployment**	**For bioterrorism event, prophylaxis for SFD, SPD, Airlift NW & immediate families**	605a
ASPD-Y	**1 Ladder (Code Yellow)**	**Assist Police**		
BARK-Y	**1 Fire Unit (Code Yellow)**	**Beauty Bark Fire**		
BRSH	**1 Engine**	**Brush Fire**		715
BRSHF	**3 Engines, 1 BC**	**Brush Fire on Freeway**		715

BRSHMJ	**5 Engines, 2 BCs, 2 Ladders,** **1 Medic Unit, Air 9, DEP1, REHAB1, SAFT2, STAF10**	**Brush Fire Major**	**Incidents involving large scale brush fire incidents including those in green belts, parks (Discovery, Carkeek, Seward, etc.) areas adjacent to freeways or significant brush fires in any other region of the City where substantial vegetation is prevalent.**	715
BRSHX	**2 Engines, 1 Ladder, 1 BC, SAFT2**	**Brush Fire With Exposures**		715
CAR	**1 Engine**	**Car Fire**		
CARF	**2 Engines**	**Car Fire on Freeway**		

TYPE CODE	STANDARD RESPONSE	DESCRIPTION	USE	RELATED SOP
CARX	**2 Engines, 1 Ladder, 1 BC, SAFT2**	**Car Fire with Exposures**		
CHEMP	**1 Chempack Engine**	**Chempack Engine**	**Used only in association with HAZMAT MCI**	605
CHIM	**1 Engine**	**Chimney Fire**		
CO-Y	**1 Ladder (Code Yellow)**	**Activated CO Detector**		
COMED	**1 Engine, 1 Ladder, 1 BC, 1 Medic Unit**	**Possible Patient**		
DUMP	**1 Engine**	**Dumpster Fire**		
DUMPX	2 Engines, 1 Ladder, 1 BC, SAFT2	**Dumpster Fire with Exposures**		

ELEC	**1 Engine**	**Electrical Problem**		
EVENT	**Event 10-15**	**Special Event (Mariners, Seahawks, Huskies, Seafair)**	**Sporting Events, concerts, fairs**	505
EXPMAJ	**5 Engines, 2 Ladders, 1 BC, DEP1, Medic Unit, Aid Car, Air 9, M44, SAFT2, STAF10, REHAB1, RIG Engine, RIG Ladder** **HazMat Group** **E10, L1, A10, HAZ1, STAF10**	**Major Explosion**		
EXPMIN	**2 Engines, 1 Ladder, 1 BC, M44**	**Minor Explosion**		
FALSE-Y	**1 Fire Unit (Code Yellow)**	**False Alarm**		
FASTB	**SAFT2 or 1 BC and SAFT2**	**Fast Back-up**		302
FIB	**5 Engines, 2 BCs, 2 Ladders, 1 Aid Car, 1 Medic Unit, Air 9, M44, DEP1, REHAB1, RIG Engine, RIG Ladder SAFT2, STAF10**	**Fire In Building**	**Requires RIG response**	
TYPE CODE	**STANDARD RESPONSE**	**DESCRIPTION**	**USE**	**RELATED SOP**
FIBHI	**8 Engines, 3 BCs, 3 Ladders, 1 Aid Car, 1 Medic Unit, Air 9, M44, DEP1, REHAB1, RIG Engine, RIG Ladder SAFT2, STAF10, MAR5**	**Fire In High-Rise Building**	**Requires RIG response**	

FIBRES	**4 Engines, 2 BCs, 2 Ladders, 1 Aid Car, 1 Medic Unit, Air 9, M44, DEP1, SAFT2, STAF10 – 2-11 or greater REHAB1**	**Fire in Single Family Residence**		
FIREF	**2 Engines**	**Rubbish Fires on Freeway**		
FIREWATCH	**1 Fire Unit (Code Yellow)**	**Firewatch**		
FOS	**1 Fire Unit**	**Food on Stove**		
FOSO-Y	**1 Fire Unit (Code Yellow)**	**Food on Stove, Out by Occupant**		
FUELSP-Y	**1 Fire Unit (Code Yellow)**	**Fuel Spill**		731 725
FURN-Y	**1 Fire Unit (Code Yellow)**	**Furnace Problem**		
GARAG	2 Engines, 1 Ladder, 1 BC, SAFT2	**Detached Garage Fire**		
HANGA	**1 Unit**	**Hang-up, Aid**		390
HANGF	**1 Fire Unit**	**Hang-up, Fire**		390
HAZ	**2 Engines, 1 Ladder, 2 BCs,** **1 Medic Unit, Air 9, DEP1, SAFT2** **HazMat Group** **E10, L1, A10, HAZ1, STAF10**	**Hazardous Material, Spill/Leak**		730 731 732
HAZADV	**(Alert HazMat Team: E10, L1, A10)**	Hazardous Material, Advised		

DRAFT

	HAZ1 (and E10 or L1) placed out of service			
TYPE CODE	STANDARD RESPONSE	DESCRIPTION	USE	RELATED SOP
HAZD	**2 Engines, 1 Ladder, 2 BCs,** **1 Medic Unit, DEP1, Air 9, SAFT2** **HazMat Group** E10, L1, A10, HAZ1, STAF10 **Decon Group** E27, L7, DECON1, A14	Hazardous Materials, Decontamination		730 606
HAZF	**5 Engines, 2 Ladders, 3 BCs, 1 Aid Car, 1 Medic Unit, DEP1, M44, SAFT2, DECON1, RIG Engine, RIG Ladder, Air 9,** **HazMat Group** **E10, L1, A10, HAZ1, STAF10** **Decon Group** **E27, L7, DECON1, A14**	**Hazardous Materials with Fire**		730

DRAFT

HAZMCI	**5 Engines, 2 Ladders, 2 BCs, 2 Aid Cars, 3 Medic Units, MCI1, DEP1, SAFT2, Air 9, M44, E21 or E35** **HazMat Group** E10, L1, A10, HAZ1, STAF10 **Decon Group** **E27, L7, DECON1, A14**	Hazardous Materials MCI	**Requires associated Chempak responses** ***(use CHEMP type code)***	735 605
HAZRAD	**1 Engine, Air 9, 1 BC** **HazMat Group** **E10, L1, A10, HAZ1, STAF10**	Hazardous Materials Radiation	**Radiation Detected**	734
HAZWHT	**1 Engine, 1 BC, Air 9** **HazMat Group** E10, L1, A10, HAZ1, STAF10	**Hazardous Materials Reduced Response**	**Use for White Powder reports or as HAZMAT reduced response**	733
HELPFF	**1 Chief, 1 Fire Unit, SPD**	HELP THE FIREFIGHTER		302

TYPE CODE	STANDARD RESPONSE	DESCRIPTION	USE	RELATED SOP
IAID	**1 Fire Unit, MSO, 1 BC, SAFT2**			

DRAFT

ILBURN-Y	**1 Fire Unit (Code Yellow)**	**Illegal Burn**		
IMED	**1 Fire Unit, 1 Medic Unit, MSO,** **1 BC, SAFT2**			
IMED7	**1 Fire Unit, 1 Unit, 1 Medic Unit, MSO, 1 BC, SAFT2**			
INVEOS-Y	**1 Fire Unit (Code Yellow)**	**Out of Service Investigation**		
LINK	**1 BC (to LCC 1263 6 Av S)**	**LINK Control Center (LCC)**		890
MARFIRES	**5 Engines, 2 Ladders, 2 BCs, 1 Aid Car, 1 Medic, Air 9, DEP1, M44, SAFT2, REHAB1, RIG Engine, RIG Ladder, STAF10, PATRL4** **Water RIG Group** **L7, A14, R1** **Marine Group** **E36, FIREBOAT, E5/FRB5, B7, MRN1**	**Marine Full Response on Shore**	**Fire in a marina, pier, boat, ship, or house boat and accessible from shore.**	740 613 1000

MARFIREW	**2 Engines, 1 Ladder, 1 BC, 1 Aid Car, 1 Medic, Air 9, DEP1, M44, SAFT2, REHAB1, RIG Engine, RIG Ladder STAF10, PATRL4** **Water RIG Group** **L7, A14, R1** **Marine Group** **E36, FIREBOAT, E5/FRB5, B7, MRN1**	**Marine Full Response on Water**	**Boat or ship fire on water; not accessible from shore at all.**	740 613 1000
TYPE CODE	**STANDARD RESPONSE**	**DESCRIPTION**	**USE**	**RELATED SOP**
MARSINKS	**1 Engine, 1 Ladder, 1 BC, DEP1, SAFT2, STAF10, PATRL4** **Water RIG Group** **L7, A14, R1** **Marine Group** **E36, FIREBOAT, E5/FRB5, B7, MRN1**	**Vessel Sinking on Shore**	**Boat or ship sinking and accessible from shore**	740 613 1000
MARSINKW	**1 Engine, 1 Ladder, 1 BC, DEP1, SAFT2, STAF10, PATRL4**	**Vessel Sinking on Water**	**Boat or ship sinking on the water; not accessible from shore at all.**	740 613 1000

	Water RIG Group **L7, A14, R1** **Marine Group** **E36, FIREBOAT, E5/FRB5, B7, MRN1**			
MARSERV	**PATRL4, FIREBOAT, E5/FRB5**	**Vessel Service Response**	**Service response for unit taking on water, mechanical issue, needs a tow.**	740 613 1000
MCI	**4 Engines, 2 Ladders, 2 BCs, 2 Aid Cars, 3 Medic Units, DEP1, SAFT2, M44, MCI1, E21 or E35, STAF10 & Air 9**	Multiple Casualty Incident		603
MED	**1 Unit, 1 Medic Unit**	**Medic Response**		
MED1	**1 Medic Unit**	**Single Medic Unit**		380
MED14	**2 Fire Units, 1 additional Unit,** **2 Medic Units, 1 BC, M44**	**MED14**		611
MED6	**1 Unit, 1 Fire Unit, 1 Medic Unit**	**MED6**		
MED7	**1 Fire Unit, 1 Unit, 1 Medic Unit**	**MED7**		
MEDF	**2 Engines, 1 Medic Unit**	Medic Response Freeway		840

TYPE CODE	STANDARD RESPONSE	DESCRIPTION	USE	RELATED SOP
MONOF	**5 Engines, 4 Ladders, 2 BCs,1 Aid Car, 1 Medic Unit, Air 9, DEP1,** **REHAB1, RIG Engine, RIG Ladder** **SAFT2, STAF10** **Technical Rescue Group** L7, A14, R1, B5	**Monorail Fire**		
MUAID	**1 Unit**	**Mutual Aid, Aid Response**		375
MUAIR	**AIR240/AIR260, 1 BC**	**Mutual Aid, Air Unit**		375
MUENG	**1 Engine and 1 BC**	**Mutual Aid, Engine**		375
MUHAZ	1 Medic Unit, 1 BC, Air 9 *HazMat Group* E10, L1, A10, HAZ1, STAF10	**Mutual Aid, Hazmat**		375
MULAD	**1 Ladder and 1 BC**	**Mutual Aid, Ladder**		375
MUMAR	**1 Medic Unit , Air 9** **Marine Group**	**Mutual Aid, Marine**		375

	.E36, FIREBOAT, E5, B7, MRN1			
MUMED	**1 Medic Unit**	**Mutual Aid Medic**		375
MUSTAL	**2 Medic Units & M44**	**Mutual Aid, ALS Strike Team**		375
MUSTBL	**5 Units, 1 BC and M44**	**Mutual Aid, BLS Strike Team**		375
MUSTE	**5 Units, 1 BC**			
MUSTL	**3 Ladders, 1 BC**	**Mutual Aid, Ladder Strike Team**		375
TYPE CODE	**STANDARD RESPONSE**	**DESCRIPTION**	**USE**	**RELATED SOP**
MUTF	**3 Engines, 1 Ladder, 1 BC**	**Mutual Aid, Structure Fire Task Force**		375
MUTFA	**2 Engines, 1 Ladder, 1 Medic, 1 BC**	**Mutual Aid, Aircraft Task Force**		375
MUTFBL	**2 Engines, 2 Aid Cars, M44, 1 BC**	**Mutual Aid, BLS Task Force**		375
MUTFTR	**1 Medic Unit** **Technical Rescue Group** **L7, A14, R1, B5**	**Confined Space, Water, Trench, Rope, or Heavy Rescue Mutual Aid Task Force**		375
MVI	**1 Unit**	**Motor Vehicle Incident**	*Formerly MVA*	
MVIF	**2 Engines, 1 Aid Car**	Motor Vehicle Incident Freeway	*Formerly MVAF*	840

MVIFM	**2 Engines, 1 Medic Unit, 1 Aid Car**	Motor Vehicle Incident Freeway Medic		
MVIM	**2 Units, 1 Medic Unit**	Motor Vehicle Incident Medic		840
NGL	**1 Engine, 1 Ladder, 1 BC**	**Natural Gas Leak**	**Broken line size less than 2" in diameter**	
NGLMJ	5 Engines, 2 Ladders, 2 BCs, DEP1, SAFT2, Medic Unit, Aid Car, Air 9 **HazMat Group** .E10, L1, A10, HAZ1, STAF10	**Major Natural Gas Leak**	**Broken line 2" or more in diameter or smaller line that is endangering multi-family residential**	850
NGO	**1 Ladder**	**Natural Gas, Odor**		
ODOR-y	**1 Fire Unit (Code Yellow)**	**Odor, Unknown**		
PAASPD-Y	**1 Fire Unit , 1 BC (Code Yellow)**	**Public Assembly, Assist SPD**	**Overcrowding complaint from CD or SPD**	766
TYPE CODE	**STANDARD RESPONSE**	**DESCRIPTION**	**USE**	**RELATED SOP**
RECONMAR	**Fire Unit**	**Fire or Marine**	**Dispatch on all water responses to either incident location or caller location; E5, E36, L7 are NOT the**	

			Recon Unit. Page to Marine Group, Technical Rescue, PTRL4	
RECONRES	**Fire Unit**	**Water Rescue**	**Dispatch on all water responses to either incident location or caller location; E5, E36, L7 are NOT the Recon Unit. Page to Marine Group, Technical Rescue, PTRL4**	
RESCAR	**2 Engines, 1 Ladder, 1 BC, 1 Medic Unit, 1 Aid Car, M44, SAFT2**	**Automobile Extrication**	**"One patient trapped inside, only one vehicle, that is on all four wheels"**	757
RESCS	**2 Engines, 1 Ladder, 1 BC, 1 Medic Unit, 1 Aid Car, Air 9, DEP1, SAFT2, STAF10, M44** **Confined Space Group** **E36, L7, B5, A14, R1, MRN1**	**Confined Space Rescue**		755
RESELV-Y	**1 Ladder (Code Yellow)**	**Elevator Rescue**		
TYPE CODE	**STANDARD RESPONSE**	**DESCRIPTION**	**USE**	**RELATED SOP**

TYPE CODE	STANDARD RESPONSE	DESCRIPTION	USE	RELATED SOP
RESHVY	**2 Engines, 1 Ladder, 1 BC, 1 Medic Unit, 1 Aid Car, DEP1, SAFT2, STAF10, M44** **Technical Rescue Group** L7, A14, R1, B5	**Heavy Rescue**	▪ **Victims are trapped in more than one vehicle** ▪ Victims are trapped under or are pinned by a vehicle ▪ **The vehicle is off the road or difficult to access** ▪ The vehicle is not on all four wheels ▪ **The extrication involves commercial type trucks, trains or heavy equipment** ▪ Vehicles crashed into buildings, **regardless of whether or not victims are trapped**, due to structural stability hazard. ▪ **Extrication situations that seem unusually complex**	757 758
RESICE	**1 Engine, E16, 1 BC, 1 Ladder, 1 Aid Car, 1 Medic Unit, DEP1, SAFT2, STAF10, M44, PTRL4** **Technical Rescue Group** L7, A14, R1, B5	**Ice Rescue**		756
RESLOC-Y	**1 Ladder (Code Yellow)**	**Lock In/Lock Out**		

DRAFT

RESMAJ	**5 Engines, 2 Ladders, 2 BCs, 1 Aid Car, 1 Medic Unit, Air 9, DEP1, SAFT2, STAF10, M44** **Technical Rescue Group** L7, A14, R1, B5	**Major Heavy Rescue**	**Any manpower intensive or unusually complex rescue incident. This includes *(but is not limited to)* building collapses, roof or floor collapses, train derailments, etc.**	758
RESROP	**2 Engines, 2 Ladders, 1 BC, 1 Medic Unit, 1 Aid Car, DEP1, SAFT2, STAF10, M44** **Technical Rescue Group** **L7, A14, R1, B5**	**Rope Rescue**		759
RESSBW	**1 Engine, 1 Medic Unit, PTRL4,** *Water RIG Group* **L7, A14, R1** **Marine Group** **E36, FIREBOAT, E5/FRB5, B7, MRN1**	**Rescue Standby, Water**	**Supports Law Enforcement in an advisory capacity or provides technical assistance.**	759
RESSBY	**1 Engine, 1 BC, 1 Medic Unit,** **L7, A14, R1,**	**Rescue Standby**	**For a high-angle trespasser or jumper**	759

DRAFT

RESTR	**1 Engine, 1 Ladder, 1 BC, 1 Medic Unit, 1 Aid Car, Air 9, DEP1, SAFT2, STAF10, M44** **Technical Rescue Group** **L7, A14, R1, B5**	**Trench Rescue**		
RESWA	**Fireboat, 2 Engines, 1 Ladder, 1 BC, 2 Medic Units, 1 Aid Car, M44, SAFT2, PTRL 4, B7, E5/FRB5** **Technical Rescue Group** **L7, A14, R1, B5**	**Rescue, Salt or Freshwater**	**Rescue Incident in Body of Salt or Freshwater** • **2 victims or less** • **small in scope** • **EXAMPLE: Overturned canoe, pleasure boat sinking, passenger car into body of salt or freshwater**	740 756 613 1000
RESWAM	**5 Engines, 2 Ladders,** **1 BC, DEP1, 2 Medic Units, 1 Aid Car, M44, SAFT2, PTRL 4, STAF10** **Technical Rescue Group** **L7, A14, R1, B5** **Marine Group**	**Rescue, Salt or Freshwater MAJOR**	**MAJOR Rescue Incident in a Body of Salt or Freshwater** • **3 victims or more** • **Large in scope** • **Complex Rescue Situation**	740 756 613 1000

	E36, FIREBOAT, E5/FRB5, B7, MRN1		• **EXAMPLE: Plane crash into Lake Union, pier collapse, bus or other large vehicle crashed into a body of salt or freshwater**	
RMC	**1 BC**	**Chief Officer to RMS**	**Initiate RMC Operations**	
RUBBISH	**1 Engine**	**Rubbish Fire, No Exposure**		
SHED	**1 Engine**	**Detached Shed Fire**		
SOV14	**2 Fire Units, 1 additional Unit,** **1 Aid Unit , 2 Medic Units, 2 BC, M44, SAFT2**	**Scene of Violence MED14**		365 611
SOV7	**1 Fire Unit, 1 Aid Unit, 1 Medic Unit, 1 BC, M44**	**Scence of Violence MED7**		365
SOVMC	**4 Engines, 2 Ladders, 2 BCs, 2 Aid Cars, 3 Medic Units, DEP1, SAFT2, M44, MCI1, E21 or E35, STAF10 & Air 9**	Scene of Violence Mass Casualty Incident		603
SPD	**Call transfer to SPD**	**Transfer to SPD**		385
SPDSBY-Y	**1 Engine, M44, 1 BC (Code Yellow)**	**Standby with SPD**	**Bomb Threats, etc.**	768
SPILL-Y	**1 Fire Unit (Code Yellow)**	**Non-HazMat Spill/Leak**		731

				725
TANKER	**3 Engines, 2 Ladders, 1 BC, 1 Medic Unit, 1 Aid Car, DEP1,** **HOSE WAGON, REHAB1, RIG Engine, RIG Ladder, SAFT2, STAF10, Air 9**	**Tanker Fire**		725 731
TEST	**Any**	**MIS Test**	**Testing CAD**	
TNKFRM	**5 Engines, 2 Ladders, 2 BCs, 1 Aid Car, 1 Medic Unit, Air 9, DEP1, M44, HOSE WAGON, DECON1, RIG Engine, RIG Ladder, SAFT2** **HazMat Group** E10, L1, A10, HAZ1, STAF10 **Decon Group** **E27, L7, DECON1, A14**	**Tank Farm**		725 731
TRAINF	**5 Engines, 2 Ladders, 2 BCs, 1 Aid Car, 1 Medic Unit, Air 9, DEP1, M44, HOSE WAGON, DECON1, RIG Engine, RIG Ladder, SAFT2** **HazMat Group** E10, L1, A10, HAZ1, STAF10	**Train Derailment with Fire and/or HazMat**		750

DRAFT

TRAINR	**2 Engines, 1 Ladder, 1 BC, 1 Medic Unit**	**Reduced Response to Opposite End of Burlington Northern Tunnel**	**Must be used when any full response is sent to the Burlington Northern tunnel**	860
TRANSF	**1 Engine**	**Transformer Fire**		
TUNAID	**1 Aid Car, 1 Engine, 1 Ladder,** **1 BC, SAFT4**	**Aid Response to Tunnel Under Construction**	**FOR TUNNELS UNDER CONSTRUCTION ONLY**	775
TUNF	**5 Engines, 2 Ladders, 1 BC, 1 Aid Car, 1 Medic Unit, DEP1, M44, SAFT2, REHAB1, RIG Engine, RIG Ladder, STAF10, Air 9 and MVU1** **Tunnel Group** **L7, E36, E5, A14, R1, B5, MRN1**	**Fire in Tunnel Under Construction**	**FOR TUNNELS UNDER CONSTRUCTION ONLY**	775
TUNMED	**1 Aid Car,1 Engine, 1 Ladder,** **1 Medic Unit , 1 BC**	**Medic Response to Tunnel Under Construction**	**FOR TUNNELS UNDER CONSTRUCTION ONLY**	775
TUNRES	**2 Engines, 1 Ladder, 1 BC, 1 Aid Car, 1 Medic Unit, DEP1, SAFT2, STAF10, M44, Air 9 and MVU1** **Tunnel Group** **L7, E36, E5, A14, R1, B5, MRN1**	**Rescue in Tunnel Under Construction**	**FOR TUNNELS UNDER CONSTRUCTION ONLY**	775
VAULT	**4 Engines, 2 Ladder, 2 BC, 1 Aid Car, 1 Medic Unit, DEP 1, Air 9, SAFT2, STAF10, Vault Fire Group**	**Vault Fire**	**ELECTRICAL VAULT OR SUBSTATION FIRE**	780 602
WATMI-Y	**1 Ladder (Code Yellow)**	**Minor Water Job**		

DRAFT

WATMJ	**2 Engines, 1 Ladder, 1 BC, SAFT2**	**Major Water Job**		
WIRES	**1 Fire Unit**	**Wires Down, Suspected Energized**		

DRAFT

DRAFT

IT Support Services for City Technology

Engineering and Operations

This division designs, implements, operates, and supports technology solutions and resources in accordance with city wide architecture and governance. Responsibilities for this division include:

- Primary communications networks that provide public safety and constituent access to and from City government; the telephone system, the data network, and Public Safety Radio System. Responsible for sustaining all three systems operating as close to 100% availability as possible 24 hours a day, seven days a week.
- Design, acquisition, installation, maintenance, repair and management of fiber optic cables on behalf of City departments and approximately 20 other local, state and federal agencies.
- Procurement requests, allocation, operation and maintenance of city wide and departmental servers, virtual enterprise computing and SAN storage environments for large scale mission critical applications in a secure, reliable, 24/7 production environment for enterprise computing.
- Allocation, operation and maintenance of enterprise level services like messaging services, web access, file sharing, user management and remote access solutions.
- Collaborate with Enterprise Architecture team to develop standards for information technology equipment and software.
- Service Desk and technical support services for City's computers, peripherals, electronic devices and mobile device management.
- Centralized IT asset management to include research, procurement request, surplus and asset transfer.
- Facility management for a reliable production computing environment to the City departments.
- Support for other enterprise services and tools.

Compute System Technologies

This team manages the operations and maintenance of computing infrastructure, including servers, storage, backup and recovery, and enterprise support systems (e.g., Active Directory, VPN, etc.). The team is also responsible for safeguarding systems and data by performing required security patches, updates, and backups to ensure systems operate at as close to 100% availability as possible 24x7. Units within this group include:

Systems Operations. The team is focused on delivering the computing environment across multiple departments. The team has technical expertise to design, integrate, and operate a secure, reliable computing environment. Key technologies include Windows, Solaris, IBM AIX, and Linux.

Enterprise Services. Enterprise Services (ES) are large scale infrastructure and application services used by the City of Seattle end user community. This includes both SaaS and NGDC hosted infrastructure and application services. The team is responsible for EA vendor management, system administration, upgrades and technical support. Key technologies

includes Microsoft Active Directory (AD), Distributed File System (DFS), Exchange Online, Office 365 and SharePoint Online infrastructure.

Infrastructure Tools. The team provides a single focus for the design, planning, deployment and maintenance of standard enterprise infrastructure monitoring and management tools. This includes system performance (Solarwinds, SCOM), configuration management (SCCM, WSUS), and monitoring and system management (Trend Micro, CRM, Vipre).

Virtual and Data Infrastructure. This team engineers and operates reliable, flexible, performant virtualized Windows, UNIX and Linux platforms and their related technologies in direct support of critical business applications. Key technologies include Solaris, Unix, Linux, Windows, and vmWare, and the associated virtualization Nutanix, IBM LPAR, and Solaris hardware.

The team also engineers and operates reliable, flexible, performant storage and data protection solutions to host and protect critical business data of all types, leveraging SAN, NAS, object, and cloud technologies. Key technologies include Dell Compellent, Quantum, Hitachi, NetApp, Cloud storage, Brocade fiber channel switching, and Commvault.

Network And Communications Technologies

This team is responsible for designing, installing, operating, and maintaining data, voice, radio, fiber optic, and structured cabling infrastructure that integrates with other technologies to provide access to resources used by City departments and the public we serve. Units within this group include:

Network Engineering & Operations. The Network Services team engineers, operates and maintains the City's data network, including data center core networks, the internet perimeter, the network backbone, and local area networks that support systems and users across the City. This group designs, acquires, installs, maintains, repairs, and manages an enterprise data network that aligns with City architectures and standards. This group also participates in development of those standards and provides tier 2 and 3 end user support. This team supports technologies that include routing, switching, load balancing, enterprise Wi-Fi, DNS/DHCP/NTP, and network security (including firewalls, VPN appliances, certificate infrastructure, network access control, and web filtering.)

Telecommunication Engineering & Operations. The Telecommunications Services team engineers, operates, and maintains a highly-reliable enterprise telephone and contact center infrastructure. This group supports end user move and change activity and provides tier 2 and 3 support. The Telecommunication Services team acquires, installs, maintains, and repairs telecommunications equipment and manages commercial telephony circuits. It supports technologies that include VoIP, circuit-switched telephony, voice mail, contact center services (including call routing scripts), audio conference bridges, commercial telephony services, SONET, and WDM.

Radio & Communications Infrastructure. This team delivers radio services for public safety and other government departments. It provides extremely reliable infrastructure and support for end user mobile and portable radio equipment. The group installs and maintains communications equipment inside 911 dispatch centers and City vehicles, with primary support to SPD and SFD. The team also supports regional planning, maintenance, interoperability testing, and projects (including PSERN and Washington

DRAFT

OneNet) in partnership with other local, state, and federal agencies. This team also designs, acquires, installs, maintains, repairs, and manages in-building structured cabling systems and outside plant fiber optic and copper cable infrastructure for the City and approximately 20 external public agency partners. Technologies include trunked and conventional land mobile radio, microwave radio and other wireless communications systems (including point-to-multipoint and mesh networks,) distributed antenna systems, routing/MPLS, DS3/T1/DACS, outside plant cable infrastructure (including fiber and copper,) and structured cabling infrastructure.

End User Support

This team is responsible for providing a single point of contact for IT technical support, trouble ticket and service request resolution and referral services to other IT workgroups, and for communication for all changes, patches, upgrades and standards changes. The team is also responsible for providing technical support for the City's desktop computers, peripherals, electronic devices and mobile devices. Units within this group include:

Service Desk. The Service Desk team provides a single point of contact for Seattle IT services, promptly resolving incidents and service requests when first contacted whenever possible, escalating issues accurately and efficiently, and keeping users and partners aware of service status and changes.

Device Support. This team provides direct customer support for end user computing to all departments within the City and tier 2 escalation support and management of centralized end user computing applications and hardware. requests.

Device Engineering. This team engineers and deploys software packages for end user applications, device drivers, patches, security updates and custom packages as required. This team evaluates and recommends hardware and software for end user standards. In addition, this team provides tier 3 escalation support and management of centralized end user computing applications and hardware.

Asset Management. This team is responsible tracking and inventory controls for city wide IT assets including desktops, laptops, printers, servers, switches, and miscellaneous Information Technology infrastructure. In addition to inventory control, the team will be forecasting replacement cycles for equipment based on City standards to promote a stable computing environment.

IT Operations Support

The IT Operations Support team is responsible for management of Information Technology facilities (including data centers and communications equipment rooms), and installation and cabling equipment within those facilities. This team provides the enterprise Network Operations Center (NOC) that monitors alerts, performs initial incident analysis, dispatches tier 2 and 3 technical support, and provides initial incident communication for network infrastructure and computing systems managed by Engineering and Operations. Units within this group include:

DRAFT

Installation Management. This team installs networking and computing equipment in data centers, communications rooms and wiring closets; installs and maintains network cabling within data centers and equipment rooms according to City standards; and supports repair and end user move and change activity (including telephone move projects).

IT Operations Center. This team manages facilities which support City computing and communications services. This includes managing access to facilities, coordinating vendors, maintaining records (including data center inventory management), and, where applicable, monitoring facility systems (including CRUs, fire alarms, water detection sensors, UPS systems, and power consumption). This team also staffs the NOC that monitors alerts from network infrastructure and computing systems, performs initial problem analysis, dispatches appropriate tier 2 and 3 technical support team(s), and provides initial incident communication.

Application Services

This division designs, develops, integrates, implements, and supports application solutions in accordance with city wide architecture and governance. Its teams are organized to support business functions or service groups**.** The integration of application services will be completed gradually in 2017, with details of the organization and integration process still under development.

Applications

These teams will provide development and support for applications that include customer relationship management, billing, finance, human resources, work and asset management and records management.

Shared Platforms

These teams will provide development and support for applications that include engineering, spatial analysis, business intelligence, analytics, SharePoint Online and document management.

Cross Platform Services

These teams will provide support to application teams, including quality assurance, change control, database administration, integration services, and access management activities.

DRAFT

TriTech Software Systems
9860 Mesa Rim Road
San Diego, CA 92121
Phone: 858.799.7000
Fax: 858.799.7011
Email: sales@tritech.com

SOFTWARE SUPPORT AGREEMENT

TRITECH SOFTWARE SYSTEMS

SOFTWARE SUPPORT AGREEMENT

DRAFT

TABLE OF CONTENTS

1.0 DEFINITIONS 340

2.0 TERM 340

3.0 SUPPORT FEE(S) 340

4.0 TELEPHONE SUPPORT 341

5.0 SOFTWARE ERROR CORRECTION 341

6.0 SOFTWARE UPDATES 342

7.0 LIMITATIONS 342

8.0 EQUIPMENT, SUBCONTRACTOR SOFTWARE AND HARDWARE, AND SYSTEM SOFTWARE 345

9.0 LIMITATION OF LIABILITY 345

10.0 DISPUTE RESOLUTION 345

11.0 SEVERABILITY 347

12.0 FORCE MAJEURE/EXCUSABLE DELAY 347

13.0 CONSTRUCTION AND HEADINGS 348

14.0 WAIVER 348

15.0 ENTIRE AGREEMENT 348

16.0 APPLICABLE LAW 348

17.0 ASSIGNMENT 348

18.0 NOTICES 348

19.0 GENERAL TERMS 349

ADDENDUM A 350

ADDENDUM B 351

DRAFT

SOFTWARE SUPPORT AGREEMENT

Client:	City of Seattle Seattle Fire Department
Address:	301 Second Avenue
City, State, Zip:	Seattle, WA
Phone, Fax:	(206) 386-1476
Contact Name:	Leonard Roberts, MIS Director

DRAFT

This Agreement is made by and between TriTech Software Systems, referred to as "TriTech", with offices at 9860 Mesa Rim Road, San Diego, California 92121 and Client named above, referred to as "Client".

A. WHEREAS, TriTech and Client have entered into a System Purchase Agreement dated _____, (the "Purchase Agreement");

B. WHEREAS, this Software Support Agreement is entered into to provide Software Support for the TriTech Software for a period of one year, subject to annual renewal thereafter;

NOW, THEREFORE, in consideration of the terms, promises, mutual covenants and conditions contained in this Agreement, TriTech and Client agree as follows:

1.0 DEFINITIONS

All capitalized terms used in this Agreement and not otherwise defined herein shall have the meanings given them in the Definitions section of the Purchase Agreement, which section is incorporated by reference herein as though set forth in full.

2.0 Term

The initial term of Software Support services provided under this Agreement shall begin at the end of the Warranty Period and end twelve (12) months thereafter. Software Support for subsequent annual terms shall be subject to renewal of this Agreement and payment of the renewal Software Support fees. On or before the expiration of the Warranty Period, and at each annual anniversary thereof, TriTech shall provide to Client a Software Support Renewal Agreement for signature. TriTech reserves the right to change the terms and conditions upon which Software Support shall be offered for renewal terms, subject to written notice to Client.

3.0 Support Fee(s)

3.1 Software Support fee(s) to be paid by Client for the initial term of this Agreement shall be the amount specified in Addendum A hereto, payable without deduction or offset pursuant to TriTech's invoices, which shall be due and payable on receipt.

3.2 TriTech shall notify Client prior to the end of a support term of the Software Support fees for the next succeeding annual term. Unless otherwise agreed in writing, Software Support fees shall be due on or before the commencement of each annual support term. TriTech support fees shall be subject to change on an annual basis.

3.3 Software Support fees do not include reasonable travel, food or lodging expenses incurred by TriTech for support services provided at Client's site or other locations remote from TriTech's principal place of business. Such expenses shall be paid by Client on receipt of TriTech's invoice for such expenses.

DRAFT

3.4 If Client fails to renew Software Support for any renewal term by execution of the applicable Software Support Renewal Agreement and payment of the applicable Software Support fees, Software Support may be rendered by TriTech, at its discretion, on a time and material basis, at TriTech's then current rates for consulting and support plus expenses and Update license fees. If Client ceases to keep in force an annual Software Support Agreement, any resumption of such annual support shall be subject to payment by Client of all past unpaid Software Support fees in addition to the Software Support fee for the current support year. Client acknowledges and agrees that the preceding clause is reasonable in light of the fact that the expenses incurred and resources devoted by TriTech to further development, enhancement and support of the TriTech Software must be spread over TriTech's client base and fairly shared by all TriTech Software users.

3.5 All amounts due and payable to TriTech hereunder shall, if not paid when due, bear a late charge equal to one and one-half percent (1-1/2 %) per month, or the highest rate permitted by law, whichever is less, from fifteen (15) days after their due date until paid.

3.6 Except for taxes for which Client provides TriTech with written certification of its tax-exempt status, if TriTech is required to collect or pay sales, use, property, value-added, or other such taxes based on the software or services provided under this Agreement, and/or Client's use thereof, then such taxes shall be invoiced to and paid by Client on receipt of such invoice.

4.0 TELEPHONE SUPPORT

TriTech will provide Telephone Support service twenty-four (24) hours a day, seven (7) days a week as more fully described in Addendum B. Client will ensure that only personnel properly trained in the operation and usage of the TriTech Software will utilize the Telephone Support service.

5.0 SOFTWARE ERROR CORRECTION

DRAFT

If, during the term of this Agreement, Client determines that Software Error(s) exist, it will first follow any error procedures specified in the TriTech Documentation. If following the error procedures does not correct the Software Error, Client shall immediately notify TriTech pursuant to the guidelines and procedures described in Addendum B, setting forth the defects noted with specificity requested by TriTech. Upon notification of a reported Software Error, TriTech shall attempt to reproduce and verify the error and, if so verified, will correct the Software Error(s) in accordance with Addendum B. Notwithstanding the foregoing, TriTech may, at its discretion, reasonably applied, correct Low Priority Software Errors (as that term is used in Addendum B), in a future Update to the TriTech Software. If TriTech is unable to reproduce the Software Error and it is necessary to travel to Client's site to reproduce it, Client shall pay TriTech's travel expenses incident to the on-site visit. If the reported problem is determined to have been caused by Equipment, Subcontractor Software or Hardware, or System Software, or is otherwise not attributable to the TriTech Software, Client shall, in addition, pay TriTech's labor related to the on-site visit at its then current hourly rates for technical support and engineering.

6.0 Software updates

From time to time at TriTech's discretion, Updates to the TriTech Software and Release Notes documenting the Updates will be developed and provided to Client. All Updates and their accompanying Release Notes shall be subject to the terms and conditions of the Purchase Agreement and shall be deemed licensed TriTech Software thereunder. (Updates do not include new versions or separate modules or functions that are separately licensed and priced.)

7.0 Limitations

7.1 Software Support for the TriTech Software shall be subject to and conditional on Client's implementation and use of a version of the TriTech Software that is the most current production version thereof that is offered to Client. If Client does not implement the most current production version when it is made available, TriTech shall only be obligated to provide Software Support for Client's version of the TriTech Software for a period of twenty-four (24) months thereafter.

7.2 TriTech shall not be obligated to provide Software Support if Client is not current on the payment of all Software Support fees and expenses.

7.3 If any of the following circumstances exist, TriTech shall be entitled to charge additional Software Support fees plus expenses at its then current rates:

7.3.1 Problems in the TriTech Software are caused by modification of the TriTech Software, Subcontractor Software or Hardware, System Software, or Equipment by Client or a third party whether or not permitted hereunder.

7.3.2 Problems in the TriTech Software are caused by the TriTech Software not being used in accordance with the TriTech Documentation, or other instructions provided by TriTech, or by misuse or neglect.

7.3.3 Problems in the TriTech Software are caused by software not provided by TriTech, not approved by TriTech in writing or not specified as compatible in the TriTech Documentation. (The procedures for seeking approval for loading third party software on a CAD Workstation are set forth in paragraph 7.4 of this Agreement. As provided in said provision, software that is not provided by TriTech shall not be loaded on a CAD Server.)

7.3.4 Problems in the TriTech Software are caused by equipment which does not meet the configuration requirements specified in the TriTech Documentation, by failure of Client to provide and maintain the site and facility requirements described in the Purchase Agreement, or the use of "clones" (generic "look-alike" equipment) as substitutes for the Equipment listed in the Purchase Agreement.

7.3.5 Problems in the TriTech Software are caused by one or more computer viruses that have not been introduced into Client's system by TriTech. Client shall maintain up to date virus checking software and shall check all software received from TriTech or any other person or entity for viruses before introducing that software into any part of the CAD System. If desired by Client, TriTech will provide Updates on media rather than direct downloading to facilitate this virus checking. If, despite such check, a virus is introduced by TriTech, TriTech will provide a virus-free copy of the TriTech Software, and will, at its expense, reload said software (but not client's data) on Client's Equipment. Client shall be responsible for reloading its data and, to that end, shall practice reasonable back-up procedures for the CAD system.

7.3.6 Problems in the TriTech Software are caused by Subcontractor Software or System Software, including but not limited to operating system software, except where such software is used by City at TriTech's direction.

7.3.7 Problems in the TriTech Software are caused by lack of Year 2000 Compliance of hardware, firmware, software, data or other facilities manufactured, developed and/or otherwise provided by Client or third parties, including but not limited to Equipment, Subcontractor Software or Hardware, or System Software.

7.3.8 Problems in the TriTech Software are caused by Equipment or software provided by Client or third parties with which the TriTech Software interfaces or operates (including but not limited to Subcontractor Software or Hardware or System Software), including but not limited to problems caused by changes in such Equipment or software.

DRAFT

7.4 If, at any time during any Software Support term, Client desires to load on a CAD Workstation any software not provided by TriTech, it shall, before loading such software, contact the TriTech Technical Services Department at the telephone numbers listed in Addendum B for purposes of seeking approval therefore. **Such action shall not constitute approval, express or implied, unless approval for the loading of specific software on a CAD Workstation has been provided to Client in writing by TriTech's Manager of Technical Services.** Client shall provide information about the software proposed to be loaded as requested by the Technical Services Department. **Until such specific written approval by TriTech's Manager of Technical Services is received, the software shall not be loaded on any CAD Workstation.** In no event will such software be loaded on a CAD Server. Approval by TriTech for the loading of such software on a CAD Workstation shall not constitute approval, express or implied, for loading such software on a CAD Server, or for loading other software on a CAD Workstation. Approval by TriTech pursuant to the foregoing shall not constitute any express or implied warranty, representation or other obligation by TriTech with respect to such software, including but not limited to its suitability, operability or capability to meet Client's needs or expectations. Violation of this provision may seriously degrade the CAD System, shall void all warranties under the Purchase Agreement or Software Support obligations under this Agreement, and shall absolve, discharge and release TriTech from any obligations or liabilities related to operation or performance of the CAD System, the TriTech Software, or any other item provided by TriTech under this Agreement, including but not limited to any liabilities for damages related thereto.

7.5 TriTech Software Support under this Agreement, or any renewal or extension thereof, shall not include design, engineering, programming, testing, implementation or other services rendered necessary by changes in Subcontractor Software, System Software or Equipment, or in any other hardware, firmware or software provided by third parties or Client ("Third Party Changes"). Any such services shall be subject to additional charges by TriTech and the mutual agreement of the parties as to the terms and conditions under which such services are rendered. Absent such agreement, TriTech shall be under no obligation, express or implied, with respect to such Third Party Changes.

DRAFT

8.0 Equipment, subcontractor software and hardware, and system software

8.1 Maintenance and support for Equipment provided under the Purchase Agreement (except as noted at section 13.4.1 therein for the Stratus ftServers™) is not included under this Agreement. However, since proper computer equipment maintenance is required for proper system operation, Client shall acquire and keep in force equipment maintenance agreements for the computer and peripheral equipment used to operate the TriTech Software, or to provide such maintenance in-house with qualified personnel. If Client determines that an item of Equipment provided under this Agreement does not perform as provided in the applicable specifications, Client may contact TriTech using the procedures described in Addendum B. TriTech shall thereupon provide Help Desk services to Client with respect to the reported problem. Notwithstanding the above, TriTech is not and shall not be a party to such third party maintenance agreements nor shall TriTech have any obligation or liability thereunder.

8.2 Maintenance and support for Subcontractor Software, Subcontractor Hardware, or System Software sold or licensed under the Purchase Agreement shall be subject to and provided in accordance with any maintenance agreements between Client and the suppliers thereof, or other third party maintenance providers. If Client determines that an item of Subcontractor Software or Hardware, or System Software provided under the Purchase Agreement does not perform as provided in the applicable Specifications, Client may contact TriTech using the procedures described in Addendum B. TriTech shall thereupon provide Help Desk services to Client with respect to the reported problem. Notwithstanding the above, TriTech is not and shall not be a party to such third party maintenance agreements nor shall TriTech have any obligation or liability thereunder.

9.0 LIMITATION OF LIABILITY

9.1 The total liability of TriTech for any claim or damage arising under this Agreement or renewals thereof, whether in contract, tort, by way of indemnification or under statute shall be limited to (i) direct damages which shall not exceed the Software Support fees paid under this Agreement by Client to TriTech for the twelve (12) month term during which the cause of action for such claim or damage arose or (ii) in the case of bodily injury or property damage for which defense and indemnity coverage is provided by TriTech's insurance carrier(s), the coverage limits of such insurance.

9.2 IN NO EVENT SHALL TRITECH BE LIABLE, WHETHER IN CONTRACT OR IN TORT, FOR LOST PROFITS, LOST SAVINGS, LOST DATA, LOST OR DAMAGED SOFTWARE, OR ANY OTHER CONSEQUENTIAL OR INCIDENTAL DAMAGES ARISING OUT OF THE USE OR NON-USE OF THE TRITECH SOFTWARE, OR OTHERWISE RELATED TO THIS AGREEMENT, REGARDLESS OF WHETHER TRITECH HAD KNOWLEDGE OF THE POSSIBILITY OF ANY SUCH LOSS OR DAMAGE.

10.0 DISPUTE RESOLUTION

DRAFT

10.1 The parties desire to resolve certain disputes, controversies and claims arising out of this Agreement without litigation. Accordingly, the parties agree to use the following alternative procedure as their sole remedy with respect to any dispute, controversy or claim arising from or relating to this Agreement or its breach. The term "Arbitrable Dispute" means any dispute, controversy or claim arising under or related to this Agreement.

10.2 At the written request of a party, each party shall appoint a knowledgeable, responsible representative to meet and negotiate in good faith to resolve any Arbitrable Dispute arising under this Agreement. The parties intend that these negotiations be conducted primarily by non-lawyer, business representatives. (However, the parties may be assisted by legal counsel in such negotiations.) The discussions shall be left to the discretion of the representatives. Upon their mutual agreement, the representatives may utilize other alternative dispute resolution procedures such as mediation to assist in the negotiations. Discussions and correspondence among the representatives for purposes of these negotiations shall be treated as confidential information developed for purposes of settlement, shall be exempt from discovery and production, and shall not be admissible in the arbitration described below or in any lawsuit without the concurrence of all parties. Documents identified in or provided with such communications, which are not prepared for purposes of the negotiations, are not so exempted, may be produced in discovery, and may, if otherwise admissible, be admitted in evidence in the arbitration or lawsuit.

10.3 If the negotiations described above do not resolve the Arbitrable Dispute within sixty (60) days of the initial written request, the Arbitrable Dispute shall be submitted to mediation under the Commercial Mediation Rules of the American Arbitration Association (the "Association"). If the Arbitrable Dispute is not completely resolved in such mediation, any remaining issues shall be submitted to binding arbitration by a single arbitrator pursuant to the Commercial Arbitration Rules of the Association. A party may demand such arbitration in accordance with the procedures set out in those rules. The arbitration hearing shall (unless otherwise agreed by the parties) be held in the county of the principal place of business of the party against whom the demand for arbitration is filed. The arbitrator shall control the scheduling so as to process the matter expeditiously. The arbitrator shall rule on the Arbitrable Dispute by issuing a reasoned decision. In no event shall the arbitrator have the authority to make any award that provides for punitive or exemplary damages. Notwithstanding anything to the contrary herein, the arbitrator shall have the power, concurrent with a court of competent jurisdiction, to award provisional relief such as a temporary restraining order or a preliminary injunction. The times specified in this Section may be extended upon mutual agreement of the parties or by the arbitrator upon a showing of good cause.

10.4 The mediator and/or arbitrator shall be selected from the national panel of arbitrators of the American Arbitration Association with expertise in computer law and technology. Any court having jurisdiction over the matter may enter a judgment upon the award of the arbitrator. Service of a petition to confirm the arbitration award may be made by United States Mail, postage prepaid, or by any regularly conducted commercial express mail service, to the attorney for the party or, if not so represented, to the party at the address set forth herein, or to the party's last-known business address.

DRAFT

10.6 Each party shall bear its own costs of these procedures. A party seeking discovery permitted by the arbitrator shall reimburse the responding party the reasonable out-of-pocket cost of production of documents (to include search time and reproduction time costs). The parties shall initially equally share the administrative fees of the arbitration and the arbitrator's fees. The prevailing party shall be entitled to reimbursement of its share of said fees actually paid, as well as to an award of reasonable attorney fees.

10.7 THE PARTIES UNDERSTAND AND ACKNOWLEDGE THAT BY AGREEING TO THIS ARBITRATION PROVISION, THEY ARE GIVING UP THE RIGHT TO TRIAL BY JURY WITH RESPECT TO THIS AGREEMENT AND THEY HEREBY WAIVE SUCH RIGHT.

11.0 SEVERABILITY

If any term, clause, sentence, paragraph, article, subsection, section, provision, condition or covenant of this Agreement is held to be invalid or unenforceable, for any reason, it shall not affect, impair, invalidate or nullify the remainder of this Agreement, but the effect thereof shall be confined to the term, clause, sentence, paragraph, article, subsection, section, provision, condition or covenant of this Agreement so adjudged to be invalid or unenforceable.

12.0 FORCE MAJEURE/EXCUSABLE DELAY

Neither party shall be responsible for failure to fulfill its obligations hereunder or liable for damages resulting from delay in performance as a result of war, fire, strike, riot or insurrection, natural disaster, delay of carriers, governmental order or regulation, complete or partial shutdown of plant, unavailability of Equipment or software from suppliers, default of a subcontractor or vendor to the party if such default arises out of causes beyond the reasonable control of such subcontractor or vendor, the acts or omissions of the other party, or its officers, directors, employees, agents, contractors, or elected officials, and/or other occurrences beyond the party's reasonable control ("Excusable Delay" hereunder). In the event of such Excusable Delay, performance shall be extended on a day for day basis or as otherwise reasonably necessary to compensate for such delay.

DRAFT

13.0 CONSTRUCTION AND HEADINGS

The division of this Agreement into sections and the use of headings of sections and subsections are for convenient reference only and shall not be deemed to limit, construe, affect, modify, or alter the meaning of such sections or subsections.

14.0 WAIVER

14.1 The failure or delay of any party to enforce at any time or any period of time any of the provisions of this Agreement shall not constitute a present or future waiver of such provisions nor the right of either party to enforce each and every provision.

14.2 No term or provision hereof shall be deemed waived and no breach excused unless such waiver or consent shall be in writing and signed by the party claimed to have waived or consented. Any consent by any party to, or waiver of, a breach by the other, whether expressed or implied, shall not constitute a consent to, waiver of or excuse for any other, different or subsequent breach.

15.0 ENTIRE AGREEMENT

This Agreement and its Addenda or Amendment(s) represent the entire agreement between the parties hereto and a final expression of their agreements with respect to the subject matter of this Agreement and supersedes all prior written agreements, oral agreements, representations, understandings or negotiations with respect to the matters covered by this Agreement.

16.0 APPLICABLE LAW

Except to the extent that this Agreement is governed by the laws of the United States, this Agreement shall be governed, interpreted and enforced in accordance with the laws of the State of Washington without regard to its conflict of law provisions and not including the United Nations Convention on Contracts for the International Sale of Goods if such convention would otherwise be applicable.

17.0 ASSIGNMENT

TriTech may assign this Agreement entirely in its discretion upon the express written assumption of the obligations hereunder by the assignee.

18.0 NOTICES

All notices required to be given under this Agreement shall be made in writing by (i) first-class mail, postage prepaid, certified, return receipt, (ii) by regularly scheduled overnight delivery, (iii) by facsimile or e-mail followed immediately by first-class mail, or (iv) by personal delivery, to the address set forth below, or such other address as provided in writing. Such notices shall be deemed given three (3) days after mailing a notice or one (1) day after overnight delivery thereof.

To Client:	To TriTech:
City of Seattle	TriTech Software Systems
Seattle Fire Department	9860 Mesa Rim Road

DRAFT

301 Second Avenue
Seattle, WA 98104
Attn: Leonard Roberts
MIS Director

San Diego, Calif. 92121
Attn: Christopher D. Maloney,
President

And to:Deputy Chief of Communications
Seattle Fire Department
301 Second Avenue
Seattle, WA 98104

19.0 GENERAL TERMS

19.1 This Agreement shall be binding on and shall inure to the benefit of the heirs, executors, administrators, successors and assigns of the parties hereto, but nothing in this paragraph shall be construed as a consent to any assignment of this Agreement by either party except as provided in the ASSIGNMENT section of this Agreement.

19.2 This Agreement shall not become a binding contract until signed by an authorized officer of both parties, and it is effective as of the date so signed.

19.3 This Agreement may be executed in any number of identical counterparts, and each such counterpart shall be deemed a duplicate original thereof.

19.4 The provisions contained herein shall not be construed in favor of or against either party because that party or its counsel drafted this Agreement, but shall be construed as if all parties prepared this Agreement.

19.5 Whenever the singular number is used in this Agreement and when required by the context, the same shall include the plural, and the use of any gender, be it masculine, feminine or neuter, shall include all of the genders.

19.6 A facsimile of this Agreement, its exhibits and amendments, and notices and documents prepared under this Agreement, generated by a facsimile machine (as well as a photocopy thereof) shall be treated as an original.

19.7 **THE PARTY'S ACCEPTANCE IS EXPRESSLY LIMITED TO THE TERMS HEREOF AND NO DIFFERENT OR ADDITIONAL TERMS CONTAINED IN ANY PURCHASE ORDER, CONFIRMATION OR OTHERWRITING SHALL HAVE ANY FORCE OR EFFECT UNLESS EXPRESSLY AGREED TO IN WRITING BY EACH PARTY.**

DRAFT

ADDENDUM A

SUPPORT FEES

Based on the following licenses, the initial annual support fee will be $151,380. Prior to the end of the Warranty Period, TriTech will forward an invoice to Client for the annual support fee. The initial support period will become effective at the end of the Warranty Period and continue for twelve (12) months thereafter. An increase in the TriTech Software licenses granted to Client will result in an increase in the Software Support fee.

Software	Number of Licenses	Value
*VisiCAD Command (Fire/EMS) Database Server License	1	35,700
*VisiCAD Archive License	1	29,750
*VisiCAD Router License	1	17,850
*VisiCAD Facility Divert License	1	8,925
*VisiCAD MultiAssign License	1	5,950
*VisiCAD MapImport Utility License	1	31,357
*VisiCAD Disaster Server with Manual Failover License	1	23,8090
*VisiCAD Snapshot License (N/C for Support)	1	5,950
*VisiCAD Training License	1	5,950
*VisiCAD Test License	1	5,950
*Ground Timer Module License	1	5,950
*911 Simulator Module License	1	2,975
*SQL English Query	1	8,925
*Proxy Message Switch	1	71,400
*Call taker/Dispatcher Client Workstation License	8	133,280
*Supervisor Client Workstation (WebView) License	2	33,320
*CAD Remote Client Workstation License	1	82,110
Digital Voice Alerting/Announcement – Station Alert Interface	1	23,800
Records Management System Interface	1	59,500
Mobile Data System AVL Interface	1	121,400
Paging Interface	1	21,420
Positron Interface	1	14,280
EMD Interface	1	17,850

DRAFT

PSAP Net-PTT Interface	1	59,500
WebView Map View	1	53,550
Move Up Module	1	17,850

*These items are subject to sales tax (included in the support fees above).

ADDENDUM B

SOFTWARE ERROR CORRECTION GUIDELINES AND PROCEDURES

(1) All Software Errors reported by Client employees shall be resolved as set forth below. Initial response by TriTech will be based upon the priority assigned by Client's supervisor of the CAD. Resolution response will be based upon the priority jointly agreed on by TriTech and Client. Client will specify a central contact person at each CAD site and a Client CAD coordinator who will be the focal point for all CAD activity.

(2) If Client determines a Software Error exists, Client shall immediately notify TriTech by telephone, followed by an error report in writing, setting forth the defects noted with specificity requested by TriTech. The written report must be faxed to TriTech at (858) 799-7013. Telephone notification will be made to TriTech's VisiCAD support line at 1 (800) VisiCAD, 1 (888) VisiCAD, or (858) 799-7050.

(3) "Normal Technical Services Hours" are 5:30a.m. through 5:30p.m. (PT/PST), Monday through Friday, excluding holidays. "Normal TriTech Office Hours" are 8:30a.m. through 5:30p.m. (PT/PST), Monday through Friday, excluding holidays.

(4) The main support line will be answered by an automated attendant at all hours. The Client can either remain on the line or press 1 to transfer to the Technical Services Department. If a Technical Services representative is available, the call will be answered and handled immediately. If all representatives are busy, the Client will be given the option to leave a message or press 0 (zero) in the case of a Critical Priority Problem, as described below. In the case of Critical Priority Problems (as described below) the Client shall press zero. All other problem reports will operate on a call-back basis after leaving a message in the support voice mailbox.

(5) During Normal TriTech Office Hours, pressing zero will transfer the caller to the receptionist who will assist the Client. The receptionist will use these procedures to handle the call appropriately, including finding a Technical Services representative or other personnel to assist the Client.

(6) After Normal TriTech Office Hours, pressing zero will transfer the caller to our emergency answering service. When connected to the service, the Client shall provide the operator with his or her name, organization name, call-back number where the Technical Services representative may reach the calling party, and a brief description of the problem (including, if applicable, the information that causes the issue to be a Critical Priority Problem).

DRAFT

(7) During Normal Technical Services Hours, each Software Error report or enhancement request will be assigned an issue number. This number should be used for all subsequent inquiries relating to the original Software Error report. Problems reported after Normal Technical Services Hours will be logged and assigned an issue number the next business day.

(8) Clients shall provide TriTech with VPN access with a back-up modem (or alternatively, a dedicated ISDN line), a separate data quality telephone modem line and a dedicated voice line (in each case as specified by TriTech) to each physical area in which a Server or interface equipment is located to enable TriTech to access, diagnose, update or install a workaround to the system. Client shall additionally provide a voice telephone line located near such areas to allow simultaneous voice and data access.

(9) If the problem is not a Critical Priority Problem, TriTech will operate on a call-back basis. If requested or specified in the response time criteria below, a TriTech representative will return the call in a manner consistent with the priority and order in which the call was received. Client will make every effort to respond to TriTech in a timely fashion when requests are made for follow-up calls or additional documentation on the reported problem.

(10) Priorities and Support Response.

(a) Critical Priority

Hours of Availability:	24 hours a day, 7 days a week, 365 days a year.
Description:	A critical software error, which severely impacts the ability of Client to dispatch emergency vehicles. These Software Errors are:

DRAFT

Appendix J: CTO Notification of Surveillance Technology

Thank you for your department's efforts to comply with the new Surveillance Ordinance, including a review of your existing technologies to determine which may be subject to the Ordinance. I recognize this was a significant investment of time by your staff; their efforts are helping to build Council and public trust in how the City collects and uses data.

As required by the Ordinance (SMC 14.18.020.D), this is formal notice that the technologies listed below will require review and approval by City Council to remain in use. This list was determined through a process outlined in the Ordinance and was submitted at the end of last year for review to the Mayor's Office and City Council.

The first technology on the list below must be submitted for review by March 31, 2018, with one additional technology submitted for review at the end of each month after that. The City's Privacy Team has been tasked with assisting you and your staff with the completion of this process and has already begun working with your designated department team members to provide direction about the Surveillance Impact Report completion process.

Please let me know if you have any questions.

Thank you,

Michael Mattmiller
Chief Technology Officer

DRAFT

Technology	Description	Proposed Review Order
Emergency Scene Cameras	Photos at incidents (not retained after transmission per department policy) are collected as part of the investigation and documentation of emergency responses and may include photographs of identifiable individuals and property.	1
Hazmat Camera	This wireless system transmits pictures related to hazardous materials sites to document and identify clean up and management requirements.	2
Computer-Aided Dispatch	Computer-aided dispatch (CAD) is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.	3

[i] What is Considered PHI Under HIPAA: HIP{AA Journal; https://www.hipaajournal.com/considered-phi-hipaa/#:~:text=PHI%20is%20health%20information%20in,when%20it%20includes%20individual%20identifiers. Posted online 12/28/2017.

DRAFT

City of Seattle

2020 Surveillance Impact Report Executive Overview

Computer-Aided Dispatch

Seattle Fire Department

DRAFT

Overview

The Operational Policy statements in this document represent the only allowable uses of the equipment and data collected by this technology.

This Executive Overview documents information about the collection, use, sharing, security and access controls for data that is gathered through Seattle Fire Department's Computer-Aided Dispatch (CAD). All information provided here is contained in the body of the full Surveillance Impact Review (SIR) document but is provided in a condensed format for easier access and consideration.

Note: **All use of CAD as described in this document and the SIR is governed by SFD's Policy and Operating Guidelines (POG) Section 500-535 and Section 4007, which contain details on policy and training related to deployment and use of SFD's CAD system.**

1.0 Technology Description

CAD is a distributed server environment utilizing multiple workstations to centrally manage 911 emergency calls. CAD receives information from callers in order to properly respond to emergency situations, often including their name, phone number, address from which they are calling, medical conditions, and potentially other personally identifiable information. While most of this information is consciously volunteered by callers, some of the information may be stored for future reference in emergency situations or for quality assurance purposes. Additionally, information may be provided to CAD about someone or a situation with identifiable information without their knowledge.

2.0 Purpose

Operational Policy:

> **Computer Aided Dispatch (CAD) is a suite of software packages that provide unit recommendations for 911 emergency calls based on the reported problem and location of a caller.**

Computer Aided Dispatch (CAD) is a suite of software packages that provide unit recommendations for 911 emergency calls based on the reported problem and location of a caller. All subsequent actions taken by SFD personnel in responding to emergency calls and events are predicated on the information obtained by CAD after a call has been received.

3.0 Data Collection and Use

Operational Policy:

> **SFD's Policy and Operating Guidelines (POG) Section 500-535, contain details on policy and training related to deployment and use of SFD's CAD system.**

CAD information includes both manually collected and automated data. Details about both are as follows:

Manually collected information includes the call information that CAD operators input into the system in the course of an emergency call. In addition to this information, there is an Emergency Medical Dispatch CAD plug in application which includes a decision tree protocol that facilitates interactions with callers.

Automated information include data from phone companies that they are required to collect and use to route emergency communications. The automated information includes but is not limited to automatically collected phone numbers with address links. These are described below:

- ANI is Automatic Number Identification. The ANI is a 10-digit Telephone Number (TN) associated with a device originating a 9-1-1 call. The ANI may be the actual number of a device, such as at a home; it may be a number that represents a Billing Telephone Number (BTN). This representation is often the case when calling from a business MLTS / PBX; it also may be called an Emergency Location Identification Number (ELIN), often used to indicate a more granular location within a business, especially in large campus or building environments.
- ALI is Automatic Location Identification. The ALI information is the '911 call location data' that is displayed to the 9-1-1 call taker on their computer display when answering 9-1-1 calls.

4.0 Data Minimization & Retention

Operational Policy:

All records are kept in accordance with state retention requirements.

Information intake occurs during the initial call, during evaluation and response triage. When trying to validate location information to determine response resources, the operator may attempt to clarify this information from the caller and/or use computerized look up or confirmation of location. Once on scene at an emergency, there may be a need to update the initial intake information based on the existing situation.

Data is retained for the life of the system. The following roles are responsible for ensuring compliance with data retention requirements:

- Assistant Chief of Risk Prevention
- Communications Deputy Chief

5.0 Access & Security

Operational Policy:

Only trained members of the Fire Alarm Center can input information into CAD.

DRAFT

Access

Uniformed Seattle Fire Department personnel assigned to emergency response are involved with the use of the CAD system. This includes but is not limited to call dispatch operators, departmental operations, and mobile apparatus operators. The following divisions within the organization use the CAD system:

- Fire Alarm Center (FAC)
- SFD Operations Staff (SFD HQ)

Seattle Fire Department employees have access to CAD view, which is restricted via Active Directory controls and firewall rules. There is also a software firewall built into the system server to limit access and provide an additional level of system security.
Access to CAD systems and data are as following:

- Caller information is collected by SFD dispatchers. The data is then accessible by all Fire Department personnel and is role-based depending on need to access the information and system.
- CAD data is also shared with American Medical Response (AMR) in real-time in order to coordinate resources needed for basic life support (BLS) EMS calls. AMR has their own access into the CAD system via Mobile Data Computer (MDC) in real time to aid in determining dynamic resource allocation and immediate response dispatch if warranted by the emergency.
- Some basic information including emergency response time, location, whether the incident is active or closed, and the date and time is also available online to the public via Realtime 911: http://www2.seattle.gov/fire/realtime911/ with a one-minute delay.
- Pulse Point, a phone app that coordinates CPR volunteers and the location of AEDs with emergency cardiac victims. The app receives CAD info on cardiac emergencies at the same rate as the SFD personnel do for specific cardiac event response and public assistance for CPR. This has saved lives over the use of the system.

Additionally, incidental data access may occur through delivery of technology client services. All ITD employees are required to comply with appropriate regulatory requirements regarding security and background review.

Security

Seattle Fire Department CAD data is stored on a secure server located at the Fire Alarm Center. A back-up physical server in case of catastrophic failure is also maintained at the Seattle Police Department's West Precinct. SFD personnel arrive at the backup location when that is activated.

DRAFT

6.0 Data Sharing and Accuracy

Operational Policy:

Data sharing partners include:

- **American Medical Response (AMR)**
- **The University of Washington, Harborview Medical Center (UWHMC)**
- **ESO Solutions, current vendor for electronic healthcare records (eHR)**
- **King County – King County Emergency Medical Services (KC EMS) contracts through KC for hosted eHR records access**
- **In case of suspected criminal activity resulting in or from an emergency response, applicable event data is provided to SPD for investigative purposes.**

Data sharing with law enforcement occurs only when criminal involvement is suspected in an emergency event. SPD complies with CJIS requirements for investigative data collection.

The following are entities that use the CAD system:

- AMR accesses a limited view of CAD data for staging ambulances close to an incident. The data access and protocols for use are outlines in the memorandum of agreement (MOA) between the company and SFD.
- King County gets a nightly extract of the data via an electronic health records (eHR) data export of CAD to a data secure FTP server.
- National Fire Protection Association (NFPA: FEMA/DHS) receives a quarterly update on performance measure, per regulatory requirement.

All patients can request reports from CAD via the Public Disclosure Officer (PDO). However, the PDO and other SFD staff will never alter a record once it has been created. If a data error is discovered, the quality assurance manager at the FAC will make note of the error and any subsequent corrections made to a record.

Per City of Seattle's Privacy Statement, outlining commitments to the public about how we collect and manage their data: *We do not sell personal information to third parties for marketing purposes or for their own commercial use.* The full Privacy Statement may be found **here.**

DRAFT

7.0 Equity Concerns

Operational Policy:

> **Prior to any disclosure, a subject matter expert will evaluate the relevant CAD data and who can access the information. A quality assurance manager will also regularly check the data for accuracy and compliance with Department policies and procedures related to dispatching.**

The entire set of CAD data is only made available to members of the Seattle Fire Department and some Seattle IT employees who may manage the system from a technical standpoint. External agencies, including law enforcement, are only provided data for specific incidents as part of a law enforcement investigation.

DRAFT

SUMMARY and FISCAL NOTE*

Department:	Dept. Contact/Phone:	CBO Contact/Phone:
SFD / ITD	Evan Ward / 206-386-1475 Jonathan Porat / 206-256-5520	Jennifer Breeze/206-256-5972

** Note that the Summary and Fiscal Note describes the version of the bill or resolution as introduced; final legislation including amendments may not be fully described.*

1. BILL SUMMARY

Legislation Title: AN ORDINANCE relating to surveillance technology implementation; authorizing approval of uses and accepting the 2019 surveillance impact reports for the Seattle Fire Department's use of Computer Aided Dispatch.

Summary and background of the Legislation: Per SMC Chapter 14.18 (also known as the Surveillance Ordinance), authorizing the approval of the surveillance impact reports for Seattle Fire Department's use of existing Computer Aided Dispatch (CAD) system.

2. CAPITAL IMPROVEMENT PROGRAM

Does this legislation create, fund, or amend a CIP Project? ___ Yes _X_ No

3. SUMMARY OF FINANCIAL IMPLICATIONS

Does this legislation amend the Adopted Budget? ___ Yes _X_ No

Does the legislation have other financial impacts to the City of Seattle that are not reflected in the above, including direct or indirect, short-term or long-term costs?
This technology is currently in use by the Seattle Fire Department and no additional costs, either direct or indirect, will be incurred based on the continued use of the technology. However, should it be determined that SFD should cease use of the technology, there would be costs associated with decommissioning the technologies. Additionally, there may be potential financial penalty related to breach of contract with the technology vendors.

Is there financial cost or other impacts of *not* implementing the legislation?
Per the Surveillance Ordinance, the City department may continue use of the technology until legislation is implemented. As such, there are no financial costs or other impacts that would result from not implementing the legislation.

4. OTHER IMPLICATIONS

a. Does this legislation affect any departments besides the originating department?
This legislation does not affect other departments. The technology under review is used exclusively by the Seattle Fire Department.

b. Is a public hearing required for this legislation?
A public hearing is not required for this legislation.

c. Is publication of notice with *The Daily Journal of Commerce* and/or *The Seattle Times* required for this legislation?
No publication of notice is required for this legislation.

d. Does this legislation affect a piece of property?
This legislation does not affect a piece of property.

e. Please describe any perceived implication for the principles of the Race and Social Justice Initiative. Does this legislation impact vulnerable or historically disadvantaged communities? What is the Language Access plan for any communications to the public?
The Surveillance Ordinance in general is designed to address civil liberties and disparate community impacts of surveillance technologies. Each Surveillance Impact Review included in the attachments, as required by the Surveillance Ordinance, include a Racial Equity Toolkit review adapted for this purpose.

f. Climate Change Implications

1. **Emissions: Is this legislation likely to increase or decrease carbon emissions in a material way?**
   No.

2. **Resiliency: Will the action(s) proposed by this legislation increase or decrease Seattle's resiliency (or ability to adapt) to climate change in a material way? If so, explain. If it is likely to decrease resiliency in a material way, describe what will or could be done to mitigate the effects.**
   No.

g. If this legislation includes a new initiative or a major programmatic expansion: What are the specific long-term and measurable goal(s) of the program? How will this legislation help achieve the program's desired goal(s).
There is no new initiative or programmatic expansion associated with this legislation. It approves the continuation of use for the specific technologies under review.

List attachments/exhibits below:

SEATTLE CITY COUNCIL
CENTRAL STAFF

February 25, 2021

M E M O R A N D U M

To: Transportation and Utilities Committee
From: Lise Kaye, Analyst
Subject: Council Bill 120003 - Authorizing approval of uses and accepting the surveillance impact report for the Seattle Fire Department's use of Computer Aided Dispatch

On Wednesday, March 3, 2021 the Transportation and Utilities Committee will discuss Council Bill 120003. The proposed bill is intended to meet the requirements of Seattle Municipal Code Chapter 14.18, Acquisition and Use of Surveillance Technologies.[1] (Attachment 1 to this memo summarizes these requirements and process by which the Executive develops the required Surveillance Impact Reports.) The proposed bill would approve the Seattle Fire Department's (SFD's) continued use of existing Computer-Aided Dispatch technology and accept the Surveillance Impact Report (SIR) for this technology. As required by SMC 14.18.020(3), the Executive conducted a public engagement process to receive public comments and/or concerns about this technology. In addition, the Community Surveillance Working Group ("Working Group") has completed a Privacy and Civil Liberties Impact Assessment ("Impact Assessment") of the technology, and the City's Chief Technology Officer (CTO) has provided his response ("Response") to the Impact Assessment.

This memo describes each technology and summarizes both the potential civil liberties and potential disparate impacts and the public engagement processes for each, as reported in the SIRs. It also summarizes key concerns and recommendations from the Working Group's Impact Assessment and the CTO's Response. Finally, the memo identifies several policy considerations for possible Council action.

SFD Computer-Aided Dispatch

Council passage of CB 120003 would approve the SFD's continued use of and accept the SIR for SFD's Computer-Aided Dispatch technology that supports personnel who dispatch Fire and Emergency Medical Services units in emergency situations. The software advises dispatchers as to the type of unit or units to send in response to 911 emergency and non-emergency calls for fire or medical aid. It determines the type of recommended unit based on the reported problem and location of the caller. The software manufacturer, TriTech, merged in 2018 with two other software companies into one entity called CentralSquare.[2]

[1] (Ord. 125679 , § 1, 2018; Ord. 125376 , § 2, 2017.)
[2] Superion, TriTech Software Systems and its subsidiary, Zuercher Technologies, and Aptean merged into one entity named CentralSquare. The SIR has since been updated to reflect the merger of Tri-Tech with other entities and to make technical corrections to internal references.

Civil Liberties and Potential Disparate Impacts on Historically Marginalized Communities

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit (RET) to inform the SIR public engagement process and to highlight and mitigate impacts on racial equity from the use of the technology. The RET for the SFD's Computer-Aided Dispatch identifies disclosure of personally identifiable information gathered during 911 calls as a potential civil liberties impact. Such a disclosure could occur in response to a public information request or to a request from an external agency. SFD notes that, while medical information can be redacted from public disclosure, names, phone numbers and addresses are not exempt. SFD works to mitigate this impact by working with requesters to voluntarily redact personal information before disclosure and may provide notice to potentially affected individuals to allow them opportunity to enjoin the release of records via a court order.

The RET also notes that sensitive information on individuals and locations obtained during 911 calls could potentially be used by law enforcement to target members of historically marginalized communities and to track the location and history of requests for services for specific locations and individuals. SFD works to mitigate this risk by providing information to law enforcement officials only if they are conducting an active investigation, as confirmed by SFD's Public Disclosure Officer and recorded for auditing purposes. SFD also uses a quality assurance manager to check data for accuracy and compliance with departmental policies and procedures related to dispatching. The RET does not identify metrics to be used as part of the CTO's annual equity assessments.[3]

Public Engagement

The Executive accepted public comments on this technology from February 5 – March 5, 2019 and conducted one public meeting for multiple SIRs on February 27, 2019.[4] In addition, the Department of Neighborhoods conducted four focus group meetings in partnership with four organizations serving communities of color and other marginalized communities.[5] The SIR includes all notes from the focus groups (Appendix D); comments pertaining solely to this technology received from members of the public (Appendix E), and letters from organizations or commissions (Appendix G). The few comments reported about this technology addressed data access and retention, data sharing and transparency.

[3] SMC 14.18.050B requires that the Chief Technology Officer produce and submit to the City Council a Surveillance Technology Community Equity Impact Assessment and Policy Guidance Report that addresses whether Chapter 14.18 of the SMC is effectively meeting the goals of the Race and Social Justice Initiative, any recommended adjustments to laws and policies to achieve a more equitable outcome, and any new approaches and considerations for the SIRs.

[4] The February 27, 2019 City Surveillance Technology Fair solicited comments on SFD's Computer-Aided Dispatch technology, as well as Seattle City Light's Current Diversion Technologies, Seattle Department of Transportation's Acyclica travel time measurement technology, and three Seattle Police Department Technologies: 911 Call Logging Recorder, Computer-Aided Dispatch, and CopLogic.

[5] Appendix D contains notes from these meetings, which were conducted as part of a "World Café" pilot project in collaboration with the Council on American-Islamic Relations, Entre Hermanos, Byrd Barr Place, and Friends of Little Saigon. Notes from Entre Hermanos are in Spanish; Executive staff are reviewing options to translate these notes into English.

Privacy and Civil Liberties Impact Assessment

The Impact Assessment identifies four "Key Concerns" about the use of SFD's Computer-Aided Dispatch technology and recommends that Council adopt four specific policies. The "Key Concerns" include questions about data accessibility, retention and sharing. Tables 1 and 2 below summarize the CTO's Response to the "Key Concerns" and describe whether and how the SIR as drafted would address the Working Group's recommended policies.

Key Concerns and the CTO's Response. Table 1 summarizes CTO's response to each of the Working Group's "Key Concerns." The Response concludes that SFD's policy, training and limitations from the technologies themselves provide adequate mitigation for the potential privacy and civil liberty concerns raised by the Working Group.

Table 1. CTO Response to Privacy and Civil Liberties Impact Assessment of SFD's Computer-Aided Dispatch Technology

Working Group Key Concern	CTO Response
1. No limits on data retention.	Data is retained for the life of the system. All records are kept in accordance with state retention requirements. Two positions in SFD are responsible for ensuring compliance with data retention requirements.
2. Lack of clarity on what data is accessible to the vendor.	Vendor may collect and store data for aggregate reporting services but is prohibited from disclosing Protected Health Information unless permitted by law and may not identify the Customer without Customer's consent.
3. No clear limits on and terms of third-party data sharing.	Role-based requirements restrict access to required services or support the technology. American Medical Response and the City have a Memorandum of Agreement.
4. Lack of clarity on whether original contracts and privacy policies have remained unchanged as a result of the CentralSquare merger.	The privacy and contractual provisions remain unchanged. SFD's Computer-Aided Dispatch data is not shared with the vendor or any of the other customers they have acquired. This SIR was drafted prior to the CentralSquare merger and does not reference this change. (The SIR has since been updated to recognize this change.)

Recommended Policies. The Impact Assessment recommends that Council ensure that SFD adopt "clear and enforceable policies that ensure, at a minimum, the following:

1. The purpose of use of Computer-Aided Dispatch (SFD) must be clearly defined as emergency operations, and its operation and data collected must be explicitly restricted to that purpose only.
2. Data retention must be limited to the time needed to effectuate the purpose defined (i.e., Computer-Aided Dispatch data that is no longer needed must be promptly deleted)—in other words, the current indefinite retention policy should be justified or ended.
3. Data sharing with third parties, if any, must be limited to those held to the same restrictions as SFD, and all partnerships and data flows between SFD and third parties must be explicitly disclosed and protected by written agreements.

4. Clear policies must govern operation of Computer-Aided Dispatch, and all operators should be trained in those policies."

Table 2 describes how the SIR as drafted would address these four recommendations. Areas not fully addressed are included in the "Policy Considerations" section below.

Table 2. Working Group Recommendations Addressed in the SIR

Working Group Recommendation	Whether/How Addressed in SIR
1. Define the purpose of Computer-Aided Dispatch (SFD) as emergency operations and restrict its operation and data collected to that purpose.	**Executive Overview.** Operational Policies represent the only allowable uses of the equipment and data collected by this technology. Note: the Executive Overview is not adopted by CB 120003. *See "Policy Considerations" below.*
2. Justify or end the current indefinite data retention policy.	**5.2** All records are kept in accordance with state retention requirements, but data is retained for the life of the system (beyond state retention requirements). *See "Policy Considerations" below.*
3. Data-sharing with third parties must be disclosed, protected by written agreements, and limited to those who meet the same restrictions as SFD	**6.1.** SFD has written agreements with several third parties (American Medical Response, King County EMS, ESO Solutions (vendor for electronic healthcare records). Non-disclosure agreements are required for sharing with "other partners" and SPD must request data through a Public Disclosure Request. The SIR does not identify a policy requiring that its partners are bound by the same restrictions as SFD. **7.4** states that SPD must comply with Criminal Justice Information Services (CJIS) requirements for investigative data collection, and medical partners must comply with the Health Care Information Access and Disclosure Law. *See "Policy Considerations" below.*
4. Operation of Computer-Aided Dispatch should be governed by clear policies in which all operators have been trained.	**3.1** Only specially trained members of the Fire Alarm Center can input information into CAD. **7.2** Other department personnel receive yearly training on privacy and security awareness

Policy Considerations

Central Staff has identified the following potential policy considerations relative to the Working Group's key concerns and recommendations:

1. Restrictions on use. SFD's policies do not concisely specify the allowable uses of Computer-Aided Dispatch (SFD) and its data. Council may wish to amend the proposed Council Bill to also adopt the Executive Overview of the SIR which identifies specific language as constituting the enforceable policies and procedures applicable to the Computer-Aided Dispatch technology.
2. Data retention. SFD's practice of retaining Computer-Aided Dispatch data for the life of the system exceeds minimum requirements in State law (six years for fire incident reports and three years for Computer-Aided Dispatch Backup Data/Tapes).[6] Council may wish to consider establishing a limit as to the period for which SFD retains Computer-Aided Dispatch data not required for any legal or fire safety investigation.
3. Third-party data sharing. The SIR does not have an explicit policy that third parties with whom SFD shares data must comply with the same privacy provisions as SFD. Council may wish to direct SFD to incorporate this requirement into its written agreements, where feasible.
4. Annual equity assessment metrics. SFD has not yet finalized metrics to be used in evaluating the Computer Aided Dispatch Technology as part of the CTO's annual equity assessments. These assessments are intended to play a key role in determining whether the City's surveillance legislation is meeting the goals of the Race and Social Justice Initiative. Council may wish to request a report on the proposed metrics by a date certain and/or Council may wish to defer approval of this SIR, pending completion of these metrics.

Committee Action

Options for Council action are as follows:

1. Pass CB 120003 as transmitted;
2. Request Central Staff to prepare amendments to the Council Bill and/or to the SIR to address additional concerns or issues; or
3. Take no action.

Attachment:

1. Background Summary and Surveillance Impact Report Process

cc: Dan Eder, Interim Director
Aly Pennucci, Budget and Policy Manager

[6] https://www.sos.wa.gov/archives/recordsmanagement/managing-fire-and-emergency-medical-service-records.aspx, FM53-04-14 Rev. 1; and EM50-20-03 Rev. 0

Attachment 1 - Background Summary and Surveillance Impact Report Process

Recent Legislative History

Ordinance 125376, passed by Council on July 31, 2017, required City of Seattle departments intending to acquire surveillance technology to obtain advance Council approval, by ordinance, of the acquisition and of a surveillance impact report (SIR).[1] Departments must also submit a SIR for surveillance technology in use when Ordinance 125376 was adopted (referred to in the ordinance as "retroactive technologies"). The Executive originally included 28 "retroactive technologies," on its November 30, 2017 Master List but revised that list to 26 in December 2019. The Council has approved two SIRs and twice extended the initial March 3, 2020 deadline for completion of SIRs for all 26 technologies: first by six months to accommodate extended deliberation of the first two SIRS; and then by a second six months due to COVID-related delays. Either the Chief Technology Officer or the Council may determine whether a specific technology is "surveillance technology" and thus subject to the requirements of SMC 14.18. Each SIR must describe protocols for a "use and data management policy" as follows:

- How and when the surveillance technology will be deployed or used and by whom, including specific rules of use
- How surveillance data will be securely stored
- How surveillance data will be retained and deleted
- How surveillance data will be accessed
- Whether a department intends to share access to the technology or data with any other entity
- How the department will ensure that personnel who operate the technology and/or access its data can ensure compliance with the use and data management policy
- Any community engagement events and plans
- How the potential impact of the surveillance on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities have been taken into account; and a mitigation plan
- The fiscal impact of the surveillance technology

Community Surveillance Working Group

On October 5, 2018, Council passed Ordinance 125679, amending SMC 14.18, creating a "community surveillance working group" charged with creating a Privacy and Civil Liberties Impact Assessment for each SIR.[2] At least five of the seven members of the Working Group

[1] As codified in SMC 14.18.030, Ordinance 125376 identified a number of exemptions and exceptions to the required Council approval, including information voluntarily provided, body-worn cameras and cameras installed in or on a police vehicle, cameras that record traffic violations, security cameras and technology that monitors City employees at work.

[2] Ordinance 125679 also established a March 31, 2020 deadline for submitting SIRs on technologies already in use (referred to as "retroactive technologies") when Ordinance 125376 was passed, with provision to request a six-month extension.

must represent groups that have historically been subject to disproportionate surveillance, including Seattle's diverse communities of color, immigrant communities, religious minorities, and groups concerned with privacy and protest.[3] Each Privacy and Civil Liberties Impact Assessment must describe the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities and will be included in the SIR. Prior to submittal of a SIR to Council, the Chief Technology Officer may provide a written statement that addresses privacy rights, civil liberty or other concerns in the Working Group's impact assessment.

Executive Overviews

In May 2019, members of the Governance, Equity, and Technology Committee requested that IT staff prepare a summary section for each of the two lengthy SIR documents under review at that time. The Committee then accepted the resultant "Condensed Surveillance Impact Reports (CSIRs) together with the complete SIRs. The Executive has continued this practice with subsequent SIRs but has renamed the documents "Executive Overviews." The Operational Policy Statements in the Executive Overview represent the only allowable uses of the subject technology.

SIR Process

Chart 1 is a visual of the SIR process from inception to Council Review:

Chart 1. Surveillance Impact Report (SIR) Process

Department drafts SIR about technology use, privacy, and data security.	Draft SIR made public. One or more public meetings scheduled to solicit feedback.	Working Group reviews SIR; creates Impact Assessment, documenting privacy and civil liberty concerns.	City's Chief Technology Officer addresses any Working Group concerns.	Council reviews Executive's proposed ordinance reflecting the SIR, authorizing the use of existing or new technology.

[3] The Mayor appoints four members and Council appoints three members.

Group 2 Surveillance Impact Report (SIR) Legislation

Transportation & Utilities Committee

March 3, 2021

Presentation by Seattle IT Privacy Office

City of Seattle

Surveillance Impact Report (SIR) Overview

- 2017: Ordinance 125376 took effect Sept 4th, revising the law to address the intended use of technologies with potential to impact civil liberties
- 2017: City identifies 29 technologies in use by 4 departments, later reduced to 26 technologies
- 2018: Ordinance amended to add an external Surveillance Advisory Working group
- 9/23/2019: Group 1 SIR legislation approved by Council (Ordinance 125936)
- 2020: Deadline extension from 9/1/2020 to 3/1/2021 due to COVID-19 delays
- **1/20/2021: Presented Overview of Surveillance Ordinance at the Transportation and Utilities Committee**
- **1/26/2021: Group 2 SIR legislation transmitted to Council**
- **2/22/2021: Group 3 SIR legislation transmitted to City Clerk**

Surveillance Criteria

Definition: *Technology whose primary purpose is to observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice. Identifiable individuals also include individuals whose identity can be revealed by license plate data when combined with any other record.*

Exclusions

- Consents to provide the data
- Opt-out notice
- Body-worn cameras
- Police vehicle cameras
- Cameras installed pursuant to state law…or to record traffic violations
- Security cameras
- City infrastructure protection cameras
- Technology that monitors only City employees

Inclusions

- Disparately impacts disadvantaged groups
- PII shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service
- Collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection
- Raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice

Surveillance Impact Report (SIR) Process

- Submitted for all retroactive and newly proposed technologies that meet the definition and have no exclusion criteria
- Created by the Departments with project management from IT

1. Privacy Impact Assessment
2. Financial Information
3. Racial Equity Toolkit
4. Public Engagement Comments and Analysis
5. Privacy and Civil Liberties Impact Assessment
6. CTO Response
7. Appendices & Supporting Documentation

General SIR Creation Timeline

1) Draft & Review SIRs	2) Public Comment Period	3) Public Comment Analysis	4) Working Group Review	5) CTO Response	6) Executive Overview	7) Council Review
Staff from the department requesting the technology completes SIR content	The initial draft released for public review and comment. One or more public meetings will take place to solicit feedback.	City staff compiles public comments and finalizes the SIR content.	The Surveillance Advisory Working Group reviews each SIR, complete an Assessment included in SIR submission	The CTO responds to the Privacy and Civil Liberties Assessment.	City Staff creates condensed version of the SIR for submission to Council (formerly called the Condensed SIR – CSIR)	City Council will decide on the use of the surveillance technology, by full Council vote.

8-9 months

Group 2 Surveillance Impact Reports (CB 120002, CB 120003, CB 120004)

1	**Binoculars / Spotting Scope (SCL)**	The spotting scope is used to read meters from a distance when direct access to the meter is obstructed.
2	**Check Meter Device (SCL)**	This device measures the total amount of power being consumed at a service location where current diversion is confirmed or suspected. The device is set at the transformer and is used when a prolonged reading is desired by the Current Diversion team.
3	**SensorLink Amp Fork (SCL)**	The SensorLink Amp Fork is used by SCL's Current Diversion team to measure the load online-side entrance conductors, allowing SCL to determine the total amount of power being consumed at a service location. This tool provides an instantaneous reading to the group conducting the investigation.
4	**Computer Aided Dispatch (SFD)**	Computer-aided dispatch (CAD) is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.
5	**Computer Aided Dispatch (SPD)**	CAD is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field.
6 / 7	**Automated License Plate Reader (ALPR) for Patrol and Parking Enforcement (SPD)**	ALPRs are computer-controlled, high-speed camera systems mounted on parking enforcement or police vehicles that automatically capture an image of license plates that come into view and converts the image of the license plate into alphanumeric data that can be used to locate vehicles reported stolen or otherwise sought for public safety purposes and to enforce parking restrictions.
8	**CopLogic (SPD)**	System allowing individuals to submit police reports on-line for certain low-level crimes in non-emergency situations where there are no known suspects or information about the crime that can be followed up on. Use is opt-in, but individuals may enter personally identifying information about third-parties without providing notice to those individuals.
9	**911 Logging Recorder (SPD)**	System providing networked access to the logged telephony and radio voice recordings of the 911 center.

Group 2 SIR Public Engagement

Short 1-2 minute video overview of each technology provided on SIR website.

Binoculars / Spotting Scope (City Light)

The spotting scope is used to read meters from a distance when direct access to the meter is obstructed. Scopes are used by SCL's Current Diversion team to conduct investigations. Use of this technology may occur without informing a domicile's resident(s).

View Summary Watch Review View Full Report

Check Meter Device (City Light)

This device measures the total amount of power being consumed at a service location where current diversion is confirmed or suspected. The device is set at the transformer and is used when a prolonged reading is desired by the Current Diversion team. Use of this technology may occur without informing a domicile's resident(s).

View Summary Watch Review View Full Report

SensorLink AmpFork (City Light)

The SensorLink Amp Fork is used by SCL's Current Diversion team to measure the load on line-side entrance conductors, allowing SCL to determine the total amount of power being consumed at a service location. This too provides an instantaneous reading to the group conducting the investigation. Use of this technology may occur without informing a domicile's resident(s).

View Summary Watch Review View Full Report

Computer Aided Dispatch (CAD) (Fire)

Computer-aided dispatch (CAD) is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.

View Summary Watch Review View Full Report

Computer Aided Dispatch (CAD) (Police)

CAD is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field.

View Summary Watch Review View Full Report

Automated License Plate Readers (Police)

ALPRs are computer-controlled, high-speed camera systems mounted on parking enforcement or police vehicles tha automatically capture an image of license plates that come into view and converts the image of the license plate into alphanumeric data that can be used to locate vehicles reported stolen or otherwise sought for public safety purpose and to enforce parking restrictions.

View Summary Watch Review View Full Report View Policy Appendix

CopLogic (Police)

System allowing individuals to submit police reports on-line for certain low-level crimes in non-emergency situatio where there are no known suspects or information about the crime that can be followed up on. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.

View Summary Watch Review View Full Report

911 Logging Recorder (Police)

System providing networked access to the logged telephony and radio voice recordings of the 911 cente

View Summary Watch Review View Full Report

Group 2 SIR Public Engagement

- February 5th – March 26th, 2019
- Technology Fair Style Event
- Recorded presentations and posted online
- Produced 2-minute video overviews of technologies

Engagement Method	(Approximate) Number of Individuals Participating	Number of Comments Received	Number of Questions Received
Focus Groups	18	12	13
Public Meeting	19	1	0
Online Comments	16	16	29
Letter	4	4	0
Email	2	2	0
Total	59	35	42

SEATTLE CITY COUNCIL
CENTRAL STAFF

Group 2 Surveillance Impact Reports

LISE KAYE, COUNCIL CENTRAL STAFF

TRANSPORTATION AND UTILITIES COMMITTEE| MARCH 3, 2021

Proposed Council Bills

I. Bills would approve the continuing use of specific surveillance technologies and accept Surveillance Impact Reports (SIRs) on those technologies

   a. CB 120002: Seattle City Light Current Diversion (3 SIRs)

   b. CB 120003: Seattle Fire Dept Computer-Aided Dispatch (1 SIR)

   c. CB 120004: Seattle Police Department (5 SIRs)

II. Committee Options

   a. Pass CB 120002, 120003 and/or 120004 as transmitted;

   b. Request Central Staff to prepare amendments to the Council Bill and/or to one or more of the SIRs to address additional concerns or issues; or

   c. Take no action

Proposed Council Bills – Today's Agenda

I. Introduction

II. Executive Overview

III. CB 120002: Seattle City Light Current Diversion (3 SIRs)

   a. Central Staff Summary
   b. Council Q&A

IV. CB 120003: Seattle Fire Dept Computer-Aided Dispatch (1 SIR)

   a. Central Staff Summary
   b. Council Q&A

V. CB 120004: Seattle Police Department (5 SIRs)

   a. Central Staff Summary
   b. Council Q&A

Elements to Consider

1. Purpose and Use of Each Technology
2. Civil Liberties and Potential Disparate Impacts on Historically Marginalized Communities (Racial Equity Toolkit)
3. Public Engagement
4. Privacy and Civil Liberties Impact Assessment
5. Chief Technology Officer's Response

Elements to Consider

- Policy Considerations
  - Primarily areas where Working Group's recommendations go beyond the mitigations described in the SIRs – not intended as staff recommendations
  - Incomplete information in a SIR
  - Legal and logistical parameters around addressing Working Group concerns (e.g. holding third-parties to City privacy standards; state mandated data retention schedules)

CB 120002: Seattle City Light Current Diversion technologies – 3 SIRs

Used to investigate potential electricity theft

- Binoculars/Spotting Scope
- Check Meter Device
- SensorLink AmpFork

SCL Current Diversion Technologies

- Civil Liberties and Potential Disparate Impacts
  - None anticipated
  - Equity analysis of past enforcement locations – not yet complete
  - Metrics for CTO's annual equity assessments – not identified
- Public comments: some support; concerns about outdated technology and invasion of privacy

SCL Current Diversion Technologies

- Impact Assessment issues:
  - Allowable uses
  - Data protection
  - Data retention
- CTO's Response: SCL's policy and training and limitations of the technologies provide adequate mitigation for Working Group concerns

SCL Current Diversion Technologies

- Policy Considerations
  - Restrictions on use
  - Annual equity assessment metrics
  - Title of Binoculars/Spotting Scope SIR

CB 120003: Seattle Fire Department Computer-Aided Dispatch – 1 SIR

Supports personnel who dispatch Fire and Emergency Medical Services units in emergency situations.

SFD Computer-Aided Dispatch

- Civil Liberties and Potential Disparate Impacts
  - Potential disclosure of personally identifiable information
  - Sensitive information could be used by law enforcement to target of members of historically marginalized communities or track locations and history of service requests
  - Metrics for CTO's annual equity assessments – not identified
- Public comments: some support; concerns about outdated technology and invasion of privacy

SFD Computer-Aided Dispatch

- Impact Assessment issues:
  - Allowable uses
  - Data accessibility, retention and sharing
  - Operators trained to policies
  - Continuity of contractual terms and privacy policies through merger
- CTO's Response: SFD's policy and training and limitations of the technologies provide adequate mitigation for Working Group concerns

SFD Computer-Aided Dispatch

- Policy Considerations
  - Restrictions on use
  - Data retention
  - Third-party data sharing
  - Annual equity assessment metrics

CB 120004: Seattle Police Department surveillance technologies – 5 SIRs

- Automated License Plate Readers
- Parking Enforcement System
- Computer-Aided Dispatch
- CopLogic
- 911 Logging Recorder

CB 120004: Automated License Plate Readers

Assist in identification of stolen vehicles, and vehicles wanted in conjunction with felonies or associated with wanted persons or Amber and Silver Alerts (abducted children and missing people).

* SIR updated in January 2019, with new policies effective February 1, 2019

SPD Automated License Plate Readers

- Civil Liberties and Potential Disparate Impacts
  - Could be used to identify individuals without reasonable suspicion of having committed a crime
  - Could be used to search for information that is not incidental to any active investigation
  - Could over-surveil vulnerable or historically targeted communities
- Public comments: support, concerns about data retention, security, privacy, potential for error or misuse, surveillance in general

SPD Automated License Plate Readers

- Impact Assessment issues:
  - Allowable use of data
  - Data access, collection, retention and sharing,
  - System audits,
  - Role/effectiveness of this technology in solving crimes
- CTO's Response: SPD's updated policies and training and limitations of the technologies provide adequate mitigation for Working Group concerns

SPD Automated License Plate Readers

- Policy Considerations
  - Restrictions on use

CB 120004: Parking Enforcement Systems

Enforce parking laws, such as vehicle impoundment for unpaid fines, time-restricted parking areas, and restricted parking zones. Identify stolen vehicles or those sought in connection with a criminal investigation using specialized license plate reader software.

* SIR updated in January 2019, with new policies effective February 1, 2019

SPD Parking Enforcement Systems

- Civil Liberties and Potential Disparate Impacts
  - Could be used to identify individuals without reasonable suspicion of having committed a crime
  - Could be used to search for information that is not incidental to any active investigation
  - Could over-surveil vulnerable or historically targeted communities
- Public comments: some support, concerns included data retention, equitable enforcement and surveillance in general

SPD Parking Enforcement Systems

- Impact Assessment issues:
  - Allowable use of data
  - Data access, collection, retention and third-party sharing,
  - Data sharing between Patrol and Parking Enforcement
  - System audits; financial and operational records, including use by neighborhood and demographic
  - Role/effectiveness of this technology in solving crimes
- CTO's Response: SPD's updated policies and training and limitations of the technologies provide adequate mitigation for Working Group concerns

SPD Parking Enforcement Systems

- Policy Considerations
  - Restrictions on use
  - Data Sharing between Patrol and Parking Enforcement
  - Equitable Enforcement
  - Genetec Patroller Software as “non-surveillance” technology

CB 120004: Computer-Aided Dispatch

Supports personnel who dispatch SPD Patrol units in emergency situations.

SPD Computer-Aided Dispatch

- Civil Liberties and Potential Disparate Impacts
  - Potential disclosure of personally identifiable information
  - Potential to contribute to structural racism through data sharing, storage and retention, thereby creating a disparate impact on historically targeted communities
  - Metrics for CTO's annual equity assessments – not identified
- Public comments: some support; concerns included data security

SPD Computer-Aided Dispatch

- Impact Assessment issues:
  - Allowable use of data
  - Data access
  - Data retention
  - Operators trained to policies
- CTO's Response: SIR provided information specific to each concern

SPD Computer-Aided Dispatch

- Policy Considerations
  - Restrictions on use
  - Annual equity assessment metrics

CB 120004: CopLogic

Crime-reporting software with two applications:

1) Individual reporting of low-level crimes

2) Retail theft reporting

SPD CopLogic

- Civil Liberties and Potential Disparate Impacts
  - Information could be disseminated in ways that could negatively impact peoples' civil liberties
  - Racial or ethnicity-based information may be entered into the system
  - Potential to contribute to structural racism through data sharing, storage and retention, thereby creating a disparate impact on historically targeted communities
  - Metrics for CTO's annual equity assessments – not identified

SPD CopLogic

- Public comments:
  - Some support
  - Request for technology to be available in languages other than English
  - Concerns about: uneven access to the programs, potential for racial bias in reports and for inaccurate reports, unfair treatment of suspects, data collection, retention and sharing

SPD CopLogic

- Impact Assessment issues:
  - Allowable use of data
  - Data retention
  - Civil liberty impacts of the retail theft program; recommend discontinuing the program
  - Third-party data sharing
- CTO's Response: SPD's policies and training and limitations of the technologies provide adequate mitigation for Working Group concerns

SPD CopLogic

- Policy Considerations
  - Retail theft reporting component of CopLogic
  - Lexis-Nexis contract provisions: purpose and use restrictions, data retention, data sharing
  - Annual equity assessment metrics

CB 120004: 911 Logging Recorder

Automatically records all telephone calls received by the Seattle Police Department's 9-1-1 Center as well as all radio traffic between dispatchers and SPD patrol officers.

SPD 911 Logging Recorder

- Civil Liberties and Potential Disparate Impacts
  - Potential disclosure of personally identifiable information
  - Potential to contribute to structural racism through data sharing, storage and retention, thereby creating a disparate impact on historically targeted communities
  - Metrics for CTO's annual equity assessments – not identified
- Public comments: some support; concerns included data use, retention and sharing

SPD 911 Logging Recorder

- Impact Assessment issues:
  - Allowable use of data
  - Data retention and sharing
  - Data retention
  - Vendor and third-party contract provisions
- CTO's Response: SIR provided information specific to each concern

SPD 911 Logging Recorder

- Policy Considerations
  - Restrictions on use (internal to City)
  - Third-party restrictions on use
  - Annual equity assessment metrics – not included

File #: CB 120004, **Version:** 1

CITY OF SEATTLE

ORDINANCE _____

COUNCIL BILL _____

AN ORDINANCE relating to surveillance technology implementation; authorizing approval of uses and accepting surveillance impact reports for the Seattle Police Department's use of surveillance technologies.

WHEREAS, Ordinance 125376 requires Council approval of surveillance impact reports (SIRs) related to approval of uses for certain technology, with existing/retroactive technology to be placed on a Master Technology List; and

WHEREAS, the ordinance provisions apply to the 911 Logging Recorder, Computer Aided Dispatch, CopLogic, and Automated License Plate Reader (ALPR) for Patrol and ALPR for Parking Enforcement, in use by Seattle Police Department (SPD); and

WHEREAS, SPD conducted policy rule review and community review as part of the development of the SIRs; and

WHEREAS, Seattle Municipal Code Section 14.18.080, enacted by Ordinance 125679, also requires review of the SIRs by a Community Surveillance Working Group composed of relevant stakeholders and a statement from the Chief Technology Officer in response to the Working Group's recommendations; and

WHEREAS, development of the SIRs and review by the Working Group has been completed; NOW, THEREFORE,

BE IT ORDAINED BY THE CITY OF SEATTLE AS FOLLOWS:

Section 1. Pursuant to Ordinances 125376 and 125679, the City Council approves use of the Seattle Police Department's 911 Logging Recorder, Computer Aided Dispatch, CopLogic, and Automated License

Plate Reader (ALPR) for Patrol and ALPR for Parking Enforcement and accepts the Surveillance Impact Reports (SIRs), for these technologies, attached to this ordinance as Attachment 1, 2, 3, 4, and 5 and the Executive Overviews, for the same technologies, attached to this ordinance as Attachment 6, 7, 8, 9, and 10.

Section 2. This ordinance shall take effect and be in force 30 days after its approval by the Mayor, but if not approved and returned by the Mayor within ten days after presentation, it shall take effect as provided by Seattle Municipal Code Section 1.04.020.

Passed by the City Council the _____ day of _____, 2021, and signed by me in open session in authentication of its passage this _____ day of _____, 2021.

_____

President _____ of the City Council

Approved / returned unsigned / vetoed this _____ day of _____, 2021.

_____

Jenny A. Durkan, Mayor

Filed by me this _____ day of _____, 2021.

_____

Monica Martinez Simmons, City Clerk

(Seal)

Attachments:
Attachment 1 - 911 Logging Recorder SIR

Attachment 2 - Parking Enforcement Systems SIR
Attachment 3 - Automated License Plate Readers (ALPR) (Patrol) SIR
Attachment 4 - Computer-Aided Dispatch (CAD) SIR
Attachment 5 - CopLogic SIR
Attachment 6 - 911 Logging Recorder Executive Overview
Attachment 7 - Parking Enforcement Systems Executive Overview
Attachment 8 - Automated License Plate Readers (ALPR) (Patrol) Executive Overview
Attachment 9 - Computer-Aided Dispatch (CAD) Executive Overview
Attachment 10 - CopLogic Executive Overview

City of Seattle

2019 Surveillance Impact Report

911 Logging Recorder

Seattle Police Department

City of Seattle

Table of Contents

Submitting Department Memo 3
Surveillance Impact Report ("SIR") overview 5
Privacy Impact Assessment 6
Financial Information 24
Expertise and References 26
Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet 27
Privacy and Civil Liberties Assessment 38
CTO Response 43
Appendix A: Glossary 51
Appendix B: Meeting Notice(s) 53
Appendix C: Meeting Sign-in Sheet(s) 61
Appendix D: Department of Neighborhood Focus Group Notes 86
Appendix E: All Comments Received from Members of the Public 118
Appendix F: Department Responses to Public Inquiries 122
Appendix G: Letters from Organizations or Commissions 123
Appendix H: Comment Analysis Methodology 147
Appendix I: Supporting Policy Documentation 150
Appendix J: CTO Notification of Surveillance Technology 167

City of Seattle

Submitting Department Memo

Memo

Date: April 29, 2019
To: City Council
From: Deputy Chief GarthGreen, Seattle Police Department
Subject: Cover Memo – 9-1-1 Logging Recorder

Description

The NICE Systems 9-1-1 Logging Recorder is an application that automatically records all telephone calls received by the Seattle Police Department's 9-1-1 Center as well as all radio traffic between dispatchers and SPD patrol officers. This technology audio-records 9-1-1 and non-emergency telephone calls and police radio traffic for evidentiary and public disclosure purposes.

Purpose

The mission of the Seattle Police Department is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional, and dependable police services. Audio recordings of 9-1-1 calls and police radio traffic can provide critical evidence to officers and detectives who investigate crimes and the prosecutors who prosecute offenders. These recordings also provide transparency and accountability for SPD, as they record in real time the interactions between 9-1-1 call takers and callers, and the radio traffic between 9-1-1 dispatchers and police officers. The NICE system also supports the 9-1-1 center's mission of quickly determining the nature of the call and getting the caller the assistance they need as quickly as possible with high quality, consistent and professional services.

Benefits to the Public

The 9-1-1 Logging Recorder supports the 9-1-1 Center's mission of providing high quality, consistent, and professional dispatch and call taking services. These recordings provide transparency, accountability, and quality assurance to the public by recording real-time interactions between 9-1-1 call takers and callers, and all radio traffic between patrol officers and dispatchers.

Privacy and Civil Liberties Considerations

During the public comment period SPD heard concerns about privacy from community members. They raised concerns about lack of clarity on data retention in the NICE Systems 9-1-1 Logging Recorder and how SPD may share information from the recordings with third parties. Recordings in the NICE system are retained for 90 days. Recordings requested for law enforcement and public disclosure are downloaded and saved within other SPD systems for the retention period related to the incident type to which the recording is related.

SPD recognizes that the content and nature of the phone calls to the 9-1-1 Center may include highly sensitive information and that callers may report personally-identifying information about third parties without providing notice to those individuals. No person, outside of SPD and Seattle IT authorized users, has direct access to data in the NICE system. Specific data, including call audio, time stamps for start and end of calls, staff position of the individual answering the call, duration of the call, and the phone number and/or radio channels used to contact 9-1-1, is shared with outside entities, such as Seattle City Attorney's Office, King County Prosecuting Attorney's Office, King County Department of Public Defense, and private defense attorneys, etc., in connection with criminal prosecutions. Audio recordings are made available to the public only via the Public Disclosure Request process.

Summary

The mission of the Seattle Police Department is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional, and dependable police services. Audio recordings of 9-1-1 calls and police radio traffic can provide critical evidence to officers and detectives who investigate crimes and the prosecutors who prosecute offenders. These recordings also provide transparency and accountability for SPD, as they record in real time the interactions between 9-1-1 call takers and callers, and the radio traffic between 9-1-1 dispatchers and police officers.

The most important unintended possible consequence related to the continued utilization of the NICE 9-1-1 Logging Recorder by SPD is the unintentional release of privacy data. All users of the NICE 9-1-1 Logging Recorder must be CJIS certified, maintain Washington State ACCESS certification, and follow SPD policies including SPD Policy 12.080 which addresses department records access, inspection, and dissemination.

City of Seattle

Surveillance Impact Report ("SIR") overview

About the Surveillance Ordinance

The Seattle City Council passed Ordinance 125376, also referred to as the "Surveillance Ordinance," on September 1, 2017. SMC 14.18.020.b.1 charges the City's executive with developing a process to identify surveillance technologies subject to the ordinance. Seattle IT, on behalf of the executive, developed and implemented a process through which a privacy and surveillance review is completed prior to the acquisition of new technologies. This requirement, and the criteria used in the review process, are documented in Seattle it policy pr-02, the "surveillance policy".

How this Document is Completed

This document is completed by the requesting department staff, support and coordinated by the Seattle information technology department ("Seattle it"). As Seattle it and department staff complete the document, they should keep the following in mind.

1. Responses to questions should be in the text or check boxes only; all other information (questions, descriptions, etc.) Should **not** be edited by the department staff completing this document.
2. All content in this report will be available externally to the public. With this in mind, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.

Surveillance Ordinance Review Process

The following is a high-level outline of the complete SIR review process.

Upcoming for Review	Initial Draft	Open Comment Period	Final Draft	Working Group	Council Review
The technology is upcoming for review, but the department has not begun drafting the surveillance impact report (SIR).	Work on the initial draft of the SIR is currently underway.	The initial draft of the SIR and supporting materials have been released for public review and comment. During this time, one or more public meetings will take place to solicit feedback.	During this stage the SIR, including collection of all public comments related to the specific technology, is being compiled and finalized.	The surveillance advisory working group will review each SIR's final draft and complete a civil liberties and privacy assessment, which will then be included with the SIR and submitted to Council.	City Council will decide on the use of the surveillance technology, by full Council vote.

City of Seattle

Privacy Impact Assessment

Purpose

A Privacy Impact Assessment ("PIA") is a method for collecting and documenting detailed information collected in order to conduct an in-depth privacy review of a program or project. A PIA asks questions about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. It also requests information about policies, training and documentation that govern use of the technology. The PIA responses are used to determine privacy risks associated with a project and mitigations that may reduce some or all of those risks. In the interests of transparency about data collection and management, the City of Seattle has committed to publishing all PIAs on an outward facing website for public access.

When is a Privacy Impact Assessment Required?

A PIA may be required in two circumstances.

1. When a project, technology, or other review has been flagged as having a high privacy risk.
2. When a technology is required to complete the surveillance impact report process. This is one deliverable that comprises the report.

1.0 Abstract

1.1 Please provide a brief description (one paragraph) of the purpose and proposed use of the project/technology.

The NICE 9-1-1 Logging Recorder audio-records all telephone calls to SPD's 9-1-1 communications center and all radio traffic between dispatchers and patrol officers.

1.2 Explain the reason the project/technology is being created or updated and why the PIA is required.

This application automatically records telephone calls received by the 9-1-1 communications center. The content and nature of those phone calls may include highly sensitive information such as the caller's name, phone number, address from which they are calling, medical conditions, detailed information about suspects, witnesses, or victims of a crime or other emergency events, and potentially other personally identifiable information. Callers may report personally-identifying information about third parties without providing notice to those individuals. While most of this information is consciously volunteered by callers, some of the information may be stored for future reference in emergency situations, for quality assurance purposes, or as evidence in a criminal investigation.

2.0 Project / Technology Overview

Provide an overview of the project or technology. The overview gives the context and background necessary to understand the purpose, mission and justification for the project / technology proposed

2.1 Describe the benefits of the project/technology.

This technology audio-records 9-1-1 and non-emergency telephone calls and police radio traffic for evidentiary and public disclosure purposes. Audio recordings are routinely used in criminal prosecutions and are routinely used within the 9-1-1 Center for training and quality control purposes.

Recordings of 9-1-1 calls and radio traffic are routinely provided to detective units to assist in criminal investigations. In addition, SPD provides approximately 5000 recordings to the Seattle Law Department each year to support legal proceedings Recordings are also used as a quality assurance measure to review calls to ensure that call takers and dispatchers are following SPD policies and procedures and to ensure SPD practices meet or exceed industry standards.

2.2 Provide any data or research demonstrating anticipated benefits.

The National Emergency Number Association's E9-1-1 PSAP (Public Safety Answering Point) Equipment Standards, a standard that defines PSAP equipment requirements for providers of 9-1-1 services, states, "as a minimum, each 9-1-1 call must be recorded." (https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/nena-sta-027.3-2018_20180702.pdf)

2.4 Describe how the project or use of technology relates to the department's mission.

The mission of the Seattle Police Department is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional, and dependable police services. Audio recordings of 9-1-1 calls and police radio traffic can provide critical evidence to officers and detectives who investigate crimes and the prosecutors who prosecute offenders. These recordings also provide transparency and accountability for SPD, as they record in real time the interactions between 9-1-1 call takers and callers, and the radio traffic between 9-1-1 dispatchers and police officers. The NICE system also supports the 9-1-1 center's mission of quickly determining the nature of the call and getting the caller the assistance they need as quickly as possible with high quality, consistent and professional services.

2.5 Who will be involved with the deployment and use of the project / technology?

SPD's authorized users of the NICE 9-1-1 Logging Recorder include police communications analysts who routinely capture audio recordings germane to police investigations and forward those recordings to detective units, outside legal entities such as the City Attorney's Office, the King County Prosecutor's Office and defense attorneys. Police Communications Supervisors and Analysts routinely listen to audio recordings for Quality Assurance purposes. The 9-1-1 Recordings Office is overseen by the 9-1-1 Administrative Manager.

Additionally, Seattle IT provides client services and operational support for IT technologies and applications. In supporting SPD systems, operational and application services deploy and service SPD technology systems. Details about the IT department are found in the appendix of this SIR.

All authorized users of the NICE 9-1-1 Logging Recorder are Criminal Justice Information Services (CJIS) certified and maintain Washington State ACCESS (A Central Computerized Enforcement Service System) certification. More information on CJIS compliance may be found at the CJIS Security Policy website. Additional information about ACCESS may be found on the Washington State Patrol's website.

3.0 Use Governance

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities contracting with the City are bound by restrictions specified in the surveillance ordinance and privacy principles and must provide written procedures for how the entity will comply with any restrictions identified.

3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

The technology is used in two distinct ways. Primarily it automatically records all calls into the 9-1-1 system, police non-emergency phone line, and police radio traffic. Secondarily, it is used to retrieve recordings by authorized personnel.

Authorized SPD users may access the recordings by logging into the NICE 9-1-1 Logging Recorder utilizing a unique user name and password. Access for personnel into the system is predicated on state and federal law governing access to criminal justice information systems. This includes thorough background investigations for each user, appropriate access and permissions dependent on the personnel role, and an audit of access and transaction logs within the system.

For information regarding CJIS security and compliance policies, see Appendices K and M of this SIR.

3.2 List the legal standards or conditions, if any, that must be met before the project / technology is used.

The technology is used to record all telephone calls between the public and the 9-1-1 Center, and police radio traffic. This is triggered when a community member contacts the department by calling 9-1-1 or the departments non-emergency numbers, including all outbound calls placed by 9-1-1 call takers and dispatchers and all radio traffic between dispatchers and police personnel including police officers, parking enforcement officers, and police detectives utilizing the police radio system.

Requests for audio recordings are initiated by detective units investigating a crime, legal counsel, and other outside entities. Recordings may also be initiated by the public using the Public Disclosure Process.

In addition, RCW 9.73.090 permits police, fire, emergency medical service, emergency communication center, and poison control center personnel to record incoming telephone calls to police and fire stations, licensed emergency medical service providers, emergency communication centers, and poison centers.

3.3 Describe the policies and training required of all personnel operating the project / technology, and who has access to ensure compliance with use and management policies.

Only authorized SPD users can access the system, technology, or the data. Access to the application is limited to SPD personnel via password-protected login credentials. Supervisors and commanding officers are responsible for ensuring compliance with SPD policies.

Data is securely input and used on SPD's password-protected network with access limited to authorized detectives and identified supervisory personnel.

All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.

SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures. All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

SPD Communications Section Policy 3.005 – Employee Conduct.

ITD client services interaction with SPD systems is governed by the terms of the 2018 Management Control Agreement (MCA)t between ITD and SPD, which states that:

"Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is there fore required to support, enable, enforce and comply with SPD policy requirements, including the FBIs Criminal Justice Information Services, (CJIS) Security Policy."

The MCA document may be found in Appendix I. Per the CJIS security policy, records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained. Details of the compliance program in Appendix I.

4.0 Data Collection and Use

4.1 Provide details about what information is being collected from sources other than an individual, including other IT systems, systems of record, commercial data aggregators, publicly available data and/or other City departments.

No information is collected from a source other than individual who calls 9-1-1 or from the officers and dispatchers.

4.2 What measures are in place to minimize inadvertent or improper collection of data?

The 9-1-1 audio recordings do not verify whether the information that was collected is accurate. They record, in real time, conversations between 9-1-1 callers and call takers. Only calls to the 9-1-1 system and specific designated phone lines are logged and recorded. Calls to other SPD phone lines are not recorded by this system. The telephone lines which SPD records are 9-1-1, the department's published non-emergency number, and the department's non-published 10-digit direct line to SPD dispatch. These telephone lines are used by the public to report crimes to the department and/or request police services. This system does not record conversations on any desk phone assigned to specific individuals within the department. Audio recordings that have not been requested within 90 days of their capture are deleted. Recordings requested for law enforcement and public disclosure are downloaded and maintained for the retention period related to the incident type.

Use of the technology other than the recording of calls to and from 9-1-1, police radio traffic, and retrieval of those recordings for law enforcement or public disclosure purposes is out of policy and subject to SPD disciplinary action.

4.3 How and when will the project / technology be deployed or used? By whom? Who will determine when the project / technology is deployed and used?

The NICE 9-1-1 Logging Recorder is automatically used to record all calls into the 9-1-1 system, police non-emergency phone line, and police radio traffic. Police communications analysts also routinely use the NICE 9-1-1 Logging Recorder to capture audio recordings germane to police investigations and forward those recordings to detective units, outside legal entities such as the Seattle City Attorneys' Office, the King County Prosecutors Office, and defense attorneys. Police Communications Supervisors and Analysts routinely listen to audio recordings for Quality Assurance purposes. The 9-1-1 Recordings Office is overseen by the 9-1-1 Administrative Manager.

4.4 How often will the technology be in operation?

The 9-1-1 audio recordings are automatic and are ongoing on a 24/7 basis.

4.5 What is the permanence of the installation? Is it installed permanently, or temporarily?

The NICE 9-1-1 Logging Recorder is a permanent installation.

4.6 Is a physical object collecting data or images visible to the public? What are the markings to indicate that it is in use? What signage is used to determine department ownership and contact information?

Per Washington State law, (RWC 9.73.030) communications of an emergency nature are not included in the requirement to obtaining consent to record. Audio recordings are made available to the public only via the Public Disclosure Request process. Audio recordings that are not requested within 90 days of their capture are deleted.

4.7 How will data that is collected be accessed and by whom?

Only authorized SPD users can access the system, technology, or the data. Access to the application is limited to SPD personnel via password-protected login credentials.

Data is securely input and used on SPD's password-protected network with access limited to authorized detectives and identified supervisory personnel.

Per the CJIS security Policy:

"The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services."

All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.

Incidental data access may be necessary through delivery of technology client services. All ITD employees are required to comply with appropriate regulatory requirements regarding security and background review. ITD CJIS Policy, the remote access policy, and information on ITD client services support roles related to this technology can be found in Appendices K and M.

ITD client services interaction with SPD systems is governed according to the terms of the 2018 Management Control Agreement between ITD and SPD, which states that:

"Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBIs Criminal Justice Information Services, (CJIS) Security Policy."

The MCA document may also be found in Appendix I.

4.8 If operated or used by another entity on behalf of the City, provide details about access, and applicable protocols.

This application is used by Seattle Police staff and occasionally Seattle Fire Department staff when they are in place at their backup 9-1-1 positions located at West Police Precinct. The software vendor NICE is given escorted access as needed (on site or via remote Web Ex connection) to help triage problems, configure system settings, and resolve technical issues. There is an annual maintenance contract with NICE for this system support. This system is not accessible by any outside entity without making a specific request to the Seattle Police Department through official means.

As mentioned, Seattle IT Department personnel have administrative access to the system for support services. As such, incidental data access may occur through delivery of technology client services.

4.9 What are acceptable reasons for access to the equipment and/or data collected?

Verified users access the system to capture and disseminate audio recordings based on the requests received from detective units, outside legal entities, and the public.

Incidental data access may occur through delivery of technology client services. All ITD employees are required to comply with appropriate regulatory requirements regarding security and background review.

ITD client services interaction with SPD systems is governed according to the terms of the 2018 Management Control Agreement between ITD and SPD, which states that:

"Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBIs Criminal Justice Information Services, (CJIS) Security Policy."

Incidental access to the data may also occur by way of ITD services. The CJIS remote access policy is applicable here and can be found in the appendices of this document.

4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

Only authorized SPD users can access the system, technology, or the data. Access to the application is limited to SPD personnel via password-protected login credentials. Logs of system activity are kept for both automatic system functions and user actions which provide an audit trail to safeguard against potential unauthorized access to stored information.

Data is securely input and used on SPD's password-protected network with access limited to authorized detectives and identified supervisory personnel.

The entire system is located on the SPD network which is protected by industry standard firewalls. The Seattle IT Department performs routine monitoring of the SPD network.

All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.

SPD's Audit, Policy and Research Section (APRS) can conduct an audit of the any and all systems at any time. The Office of Inspector General and the federal monitor can also access all data and audit for compliance at any time.

ITD client services interaction with SPD systems is governed according to the terms of the 2018 Management Control Agreement between ITD and SPD, which states that:

"Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBIs Criminal Justice Information Services, (CJIS) Security Policy."

This MCA document may be found in Appendix I.

Additionally, per the CJIS Security Policy, the following safeguards are in place:

- The agency shall establish identifier and authenticator processes.
- Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. 08/16/2018 CJISD-ITS-DOC-08140-5.7 37 password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).
- Unsuccessful login attempts - the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10 minute time period unless released by an administrator.

- When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit strength to protect CJI.
- When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption. When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.
- Intrusion Detection Tools/Techniques such as monitor inbound and outbound communications for unusual or unauthorized activities, send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort, employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.
- Audit - Each agency shall be responsible for complying with all audit requirements for use of CJIS Systems. Each CSO is responsible for completing a triennial audit of all agencies with access to CJIS Systems through the CSO's lines.
- The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.
- A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage.

Publicly accessible computers shall not be used to access, process, store or transmit CJI.

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

The data is stored in the NICE system, much of the NICE system is physically housed at the SPD 9-1-1 center, with some of the servers hosted virtually on SPD network in SPD section of the city data center. Data collect is located on the server's storage in the above locations. Extracted data is stored on file shares for SPD and City Law (these reside SPD Network Storage or Law storage system managed by Seattle ITD). Extracted data is electronically sent to Law, Discovery or as redacted material in response to PDR (posted to the City PDR system, GOVQA).

Per the CJIS Security Policy found in Appendix I:

Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history 08/16/2018 CJISD-ITS-DOC-08140-5.7 D-3 records. Additionally, each CSO must ensure that all agencies establish an information security structure that provides for an ISO and complies with the CJIS Security Policy.

Network Diagrams - Network diagrams, i.e. topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the "big picture" – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest.

5.2 How will the owner allow for departmental and other entities, to audit for compliance with legal deletion requirements?

SPD's Audit, Policy and Research Section (APRS) can conduct an audit of the any and all systems at any time. In addition, the Office of Inspector General and the federal monitor can access all data and audit for compliance at any time.

The 2017 Technical Security Audit for CJIS Compliance for SPD can be found in Appendix I.

5.3 What measures will be used to destroy improperly collected data?

SPD policy contains multiple provisions to avoid improperly collecting data. SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a GO Report. SPD Policy 7.090 specifically governs the collection and submission of photographic evidence. Evidence is submitted to the Evidence Unit and associated with a specific GO Number and investigation. And, SPD Policy 7.110 governs the collection and submission of audio recorded statements. It requires that officers state their name, the Department name, the General Offense number, date and time of recording, the name of the interviewee, and all persons present at the beginning of the recording.

Additionally, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002. SPD Policy 5.001 also ensures that communication on the systems subject to collection on this system is official in nature.

Per the CJIS security policy:

5.8.3 Digital Media Sanitization and Disposal The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

5.4 Which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

Unit managers are responsible for ensuring compliance with data retention requirements within SPD. Audit, Policy & Research Section personnel can also conduct audits of all data collection software and systems. Additionally, any appropriate auditor, including the Office of Inspector General and the federal monitor can audit for compliance at any time.

The CJIS security policy in Appendix I of this SIR includes applicable data retention requirements associated with the CAD system. The MCA between SPD and ITD is the inter-departmental agreement that ensures compliance with the CJIS Security Policy, and can be found in Appendices K and M.

6.0 Data Sharing and Accuracy

6.1 Which entity or entities inside and external to the City will be data sharing partners?

No person, outside of SPD and Seattle IT, has direct access to the application or the data.

As Seattle IT supports the NICE system on behalf of SPD, a Management Control Agreement exists between SPD and Seattle IT. The agreement outlines the specifications for compliance, and enforcement related to supporting the NICE system through inter-departmental partnership. The MCA can be found in the appendices of this SIR.

Data obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law.

Data may be shared with outside entities in connection with criminal prosecutions:

- Seattle City Attorney's Office
- King County Prosecuting Attorney's Office
- King County Department of Public Defense
- Private Defense Attorneys
- Seattle Municipal Court
- King County Superior Court
- Similar entities where prosecution is in Federal or other State jurisdictions

Data may be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

Discrete pieces of data collected by CAD may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by SPD Policy 12.050 and 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayoral Directive, dated February 6, 2018.

SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the system.

6.2 Why is data sharing necessary?

Data sharing is not an automatic component of the 9-1-1 recording system. Instead, discrete recordings may be shared only within the context of the situations outlined in 6.1.

6.3 Are there any restrictions on non-City data use?

Yes ☒ No ☐

6.3.1 If you answered yes, provide a copy of the department's procedures and policies for ensuring compliance with these restrictions.

Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20, regulating criminal justice information systems. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260 (auditing and dissemination of criminal history record information systems), and RCW Chapter 10.97 (Washington State Criminal Records Privacy Act).

Once disclosed in response to PRA request, there are no restrictions on non-City data use; however, applicable exemptions will be applied prior to disclosure to any requestor who is not authorized to receive exempt content.

6.4 How does the project/technology review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?

Research agreements must meet the standards reflected in SPD Policy 12.055. Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

6.5 Explain how the project/technology checks the accuracy of the information collected. If accuracy is not checked, please explain why.

The SPD business users typically inform IT support if the calls are not present or appear to be inaccurate in any manner. These phone lines are isolated for 9-1-1 traffic or Communications Center business needs only. The few lines that are business lines that come into the VIPER system are also being recorded. The recorded phone lines are identified and mapped to indicate which ones are 9-1-1 lines and which ones are not.

6.6 Describe any procedures that allow individuals to access their information and correct inaccurate or erroneous information.

Individuals may request records pursuant to the PRA, and individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

7.0 Legal Obligations, Risks and Compliance

7.1 What specific legal authorities and/or agreements permit and define the collection of information by the project/technology?

SPD's use of 9-1-1 audio recordings is governed by RCW 9.73, other legal requirements, and policies as outlined in 3.1, 3.2, 3.3, 4.2, 4.6, and 5.3 of this SIR.

7.2 Describe what privacy training is provided to users either generally or specifically relevant to the project/technology.

SPD Policy 12.050 mandates that all employees receive Security Awareness Training (Level 2), and all employees also receive City Privacy Training. All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), many of which contain specific privacy requirements. Any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

The CJIS training requirements can be found in the appendices of this document, as well as in question 3.3, above.

7.3 Given the specific data elements collected, describe the privacy risks identified and for each risk, explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy risks may arise when information is collected about citizens, unrelated to a specific incident. These concerns are mitigated by policy and procedures. In addition, 9-1-1 audio recordings may capture highly sensitive and private incidents and information.

SMC 14.12 and SPD Policy 6.060 direct all SPD personnel that "any documentation of information concerning a person's sexual preferences or practices, or their political or religious activities must be for a relevant reason and serve a legitimate law enforcement purpose." Additionally, officers must take care "when photographing demonstrations or other lawful political activities. If demonstrators are not acting unlawfully, police can't photograph them."

Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

Finally, see 5.3 for a detailed discussion about procedures related to noncompliance.

7.4 Is there any aspect of the project/technology that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?

The privacy risks outlined in 7.3 above are mitigated by legal requirements and auditing processes (i.e., maintenance of all requests, copies of consent forms/statements and warrants) that allow for any auditor, including the Office of Inspector General and the federal monitor, to inspect use and deployment of 9-1-1 audio recordings.

The largest privacy risk is the un-authorized release of 9-1-1 audio recordings that contained information deemed private or offensive in the RCW. To mitigate this risk, the technology falls under the current SPD policies around dissemination of Department data and information reflected in 6.1.

8.0 Monitoring and Enforcement

8.1 Describe how the project/technology maintains a record of any disclosures outside of the department.

Per SPD Policy 12.080, the Crime Records Unit is responsible to receive and record all requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies." Any subpoenas and requests for public disclosure are logged by SPD's Legal Unit. Any action taken, and data released subsequently in response to subpoenas is then tracked through a log maintained by the Legal Unit. Public disclosure requests are tracked through the City's GovQA Public Records Response System, and responses to Public Disclosure Requests, including responsive records provided to a requestor, are retained by SPD for two years after the request is completed.

All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayoral Directive, dated February 6, 2018.

8.2 What auditing measures are in place to safeguard the information, and policies that pertain to them, as well as who has access to the audit data? Explain whether the project/technology conducts self-audits, third party audits or reviews.

SPD's Audit, Policy and Research Section is authorized to conduct audits of all investigative data collection software and systems. In addition, the Office of Inspector General and the federal monitor can conduct audits of the software, and its use, at any time. Audit data is available to the public via Public Records Request.

The latest CJIS technical security audit from 2017 can be found in Appendix I of this SIR.

Financial Information

Purpose

This section provides a description of the fiscal impact of the surveillance technology, as required by the surveillance ordinance.

1.0 Fiscal Impact

Provide a description of the fiscal impact of the project/technology by answering the questions below.

1.1 Current or potential sources of funding: initial acquisition costs.

Current ☒ potential ☐

Date of initial acquisition	Date of go live	Direct initial acquisition cost	Professional services for acquisition	Other acquisition costs	Initial acquisition funding source
12/20/2013	N/A	$116,729.23	$97,002.03	Tax: $20,304.47	General Fund, partially reimbursed by King County E 9-1-1

Notes:

N/A

1.2 Current or potential sources of funding: on-going operating costs, including maintenance, licensing, personnel, legal/compliance use auditing, data retention and security costs.

Current ☒ potential ☐

Annual maintenance and licensing	Legal/compliance, audit, data retention and other security costs	Department overhead	IT overhead	Annual funding source
$98,495				ITD for SPD

Notes:

"NICE GOLD System Support for the period 11/01/17 - 10/31/18. KC E911 Reimbursable up to 75%. Annual Renewal of NICE System Recorder at Comm Center NICE System Service Agreement (audio Recorder 9-1-1) for SPD"

1.3 Cost savings potential through use of the technology

These are not quantified; however, potential cost savings may result from enhancements to 9-1-1 center response through training and quality assurance practices.

1.4 Current or potential sources of funding including subsidies or free products offered by vendors or governmental entities

KC E911 Reimbursable up to 75%.

Expertise and References

Purpose

The following information is provided to ensure that Council has a group of experts to reference while reviewing the completed surveillance impact report ("SIR"). Any individuals or agencies referenced must be made aware ahead of publication that their information has been included. All materials must be available for Council to access or review, without requiring additional purchase or contract.

1.0 Other Government References

Please list any other government bodies that have implemented this technology and can speak to the implementation of this technology.

Agency, municipality, etc.	Primary contact	Description of current use
None	None	None

2.0 Academics, Consultants, and Other Experts

Please list any experts in the technology under consideration, or in the technical completion of the service or function the technology is responsible for.

Agency, municipality, etc.	Primary contact	Description of current use
None	None	None

3.0 White Papers or Other Documents

Please list any authoritative publication, report or guide that is relevant to the use of this technology or this type of technology.

Title	Publication	Link
None	None	None

City of Seattle

Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet

Purpose

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit ("RET") in order to:

- Provide a framework for the mindful completion of the SIR in a way that is sensitive to the historic exclusion of vulnerable and historically underrepresented communities. Particularly, to inform the public engagement efforts departments will complete as part of the surveillance impact report.
- Highlight and mitigate any impacts on racial equity from the adoption and the use of the technology.
- Highlight and mitigate any disparate impacts on individuals or vulnerable communities.
- Fulfill the public engagement requirements of the surveillance impact report.

Adaptation of the RET for Surveillance Impact Reports

The RET was adapted for the specific use by the Seattle Information Technology Departments' ("Seattle IT") Privacy Team, the Office of Civil Rights ("OCR"), and Change Team members from Seattle IT, Seattle City Light, Seattle Fire Department, Seattle Police Department, and Seattle Department of Transportation.

Racial Equity Toolkit Overview

The vision of the Seattle Race and Social Justice Initiative ("RSJI") is to eliminate racial inequity in the community. To do this requires ending individual racism, institutional racism and structural racism. The RET lays out a process and a set of questions to guide the development, implementation and evaluation of policies, initiatives, programs, and budget issues to address the impacts on racial equity.

1.0 Set Outcomes

1.1. Seattle City Council has defined the following inclusion criteria in the surveillance ordinance, and they serve as important touchstones for the risks departments are being asked to resolve and/or mitigate. Which of the following inclusion criteria apply to this technology?

☐ The technology disparately impacts disadvantaged groups.

☐ There is a high likelihood that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service.

☒ The technology collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection.

☐ The technology raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice.

City of Seattle

1.2 What are the potential impacts on civil liberties through the implementation of this technology? How is the department mitigating these risks?

Some personally identifiable information (PII) gathered during emergency responses could be used to identify individuals, such as their name, home address or contact information. Victims of criminal activity may also be identified during incident responses, whose identities should be protected in accordance with RCW 42.56.240 and RCW 70.02.

1.3 What are the risks for racial or ethnicity-based bias through each use or deployment of this technology? How is the department mitigating these risks?

Include a description of any issues that may arise such as algorithmic bias or the possibility for ethnic bias to emerge in people and/or system decision-making.

The mission of the Seattle Police Department is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional and dependable police services. While race and ethnicity information of individuals may be recorded by the NICE 9-1-1 audio recording system, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

1.4 Where in the City is the technology used or deployed?

☒ all Seattle neighborhoods

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County.

If possible, please include any maps or visualizations of historical deployments / use.

N/A

City of Seattle

1.4.1 What are the racial demographics of those living in this area or impacted by these issues?

The demographics for the City of Seattle: White - 69.5%; Black or African American - 7.9%; Amer. Indian & Alaska Native - 0.8%; Asian - 13.8%; Native Hawaiian & Other Pac. Islander - 0.4; Other race - 2.4%; Two or more races - 5.1%; Hispanic or Latino ethnicity (of any race): 6.6%; Persons of color: 33.7%.

1.4.2 How does the Department to ensure diverse neighborhoods, communities, or individuals are not specifically targeted through the use or deployment of this technology?

The the NICE 9-1-1 Logging Recorderis used to record all calls placed to 9-1-1 and the police non-emergency numbers without regard to where the call originates from. There is no distinction in the levels of service this system provides to the various and diverse neighborhoods, communities, or individuals within the city.

1.5 How do decisions around data sharing have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

The Aspen Institute on Community Change defines *structural racism* as "…public policies, institutional practices, cultural representations and other norms [which] work in various, often reinforcing ways to perpetuate racial group inequity."[1] Data sharing has the potential to be a contributing factor to structural racism and thus creating a disparate impact on historically targeted communities. In an effort to mitigate this possibility, SPD has established policies regarding the dissemination of data in connection with criminal prosecutions, Washington Public Records Act (Chapter 42.56 RCW), and other authorized researchers.

Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

No person outside of SPD has direct access to the application or the data recorded by the NICE 9-1-1 audio recording system. Data obtained by the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law.

1.6 How do decisions around data storage and retention have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

Like decisions around data sharing, data storage and retention have similar potential for disparate impact on historically targeted communities. SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

1.7 What are potential unintended consequences (both negative and positive potential impact)? What proactive steps can you can / have you taken to ensure these consequences do not occur.

The most important unintended possible consequence related to the continued utilization of the the NICE 9-1-1 Logging Recorder by SPD is the unintentional release of privacy data. All users of the the NICE 9-1-1 Logging Recorder must be CJIS certified and maintain Washington State ACCESS certification and existing SPD policies mitigate the risks of unintentional release of information.

2.0 Public Outreach

2.1 Organizations who received a personal invitation to participate.

Please include a list of all organizations specifically invited to provide feedback on this technology.

1. ACLU of Washington	2. Ethiopian Community Center	3. Planned Parenthood Votes Northwest and Hawaii
4. ACRS (Asian Counselling and Referral Service)	5. Faith Action Network	6. PROVAIL
7. API Chaya	8. Filipino Advisory Council (SPD)	9. Real Change
10. API Coalition of King County	11. Friends of Little Saigon	12. SCIPDA
13. API Coalition of Pierce County	14. Full Life Care	15. Seattle Japanese American Citizens League (JACL)
16. CAIR	17. Garinagu HounGua	18. Seattle Neighborhood Group
19. CARE	20. Helping Link	21. Senior Center of West Seattle
22. Central International District Business Improvement District	23. Horn of Africa	24. Seniors in Action
25. Church Council of Greater Seattle	26. International ImCDA	27. Somali Family Safety Task Force
28. City of Seattle Community Police Commission (CPC)	29. John T. Williams Organizing Committee	30. South East Effective Development
31. City of Seattle Community Technology Advisory Board	32. Kin On Community Health Care	33. South Park Information and Resource Center SPIARC
34. City of Seattle Human Rights Commission	35. Korean Advisory Council (SPD)	36. STEMPaths Innovation Network
37. Coalition for Refugees from Burma	38. Latina/o Bar Association of Washington	39. University of Washington Women's Center
40. Community Passageways	41. Latino Civic Alliance	42. United Indians of All Tribes Foundation
43. Council of American Islamic Relations - Washington	44. LELO (Legacy of Equality, Leadership, and Organizing)	45. Urban League
46. East African Advisory Council (SPD)	47. Literacy Source	48. Wallingford Boys & Girls Club
49. East African Community Services	50. Millionair Club Charity	51. Washington Association of Criminal Defense Lawyers
52. Education for All	53. Native American Advisory Council (SPD)	54. Washington Hall
55. El Centro de la Raza	56. Northwest Immigrant Rights Project	57. West African Community Council
58. Entre Hermanos	59. OneAmerica	60. YouthCare
61. US Transportation expertise	62. Local 27	63. Local 2898
64. (SPD) Demographic Advisory Council	65. South Seattle Crime Prevention Coalition (SSCPC)	66. CWAC
67. NAAC		

2.2 Additional Outreach Efforts

Department	Outreach Area	Description
ITD	Social Media Outreach Plan: Twitter	Directed Tweets and Posts related to Open Public Comment Period for Group 2 Technologies, as well as the BKL event.
SPD, SFD, OPCD, OCR, SPL, SDOT, SPR, SDCI, SCL, OLS, Seattle City Council	Social Media Outreach Plan: Twitter	Tweets and Retweets regarding Group 2 comment period and/or BKL event.
ITD	Press Release	Press release sent to several Seattle media outlets.
ITD	Ethnic Media Press Release	Press Release sent to specific ethnic media publications.
ITD	Social Media Outreach Plan: Facebook Event Post	Seattle IT paid for boosted Facebook posts for their BKL event.
ITD	CTAB	Presented and utilized the Community Technology Advisory Board (CTAB) network and listserv for engaging with interested members of the public
ITD	Blog	Wrote and published a Tech Talk blog post for Group 2 technologies, noting the open public comment period, BKL event, and links to the online survey/comment form.
ITD	Technology Videos	Seattle IT worked with the Seattle Channel to produce several short informational/high level introductory videos on group 2 technologies, which were posted on seattle.gov/privacy. And used at a number of Department of Neighborhoods-led focus groups.

2.3 Scheduled public meeting(s).

Meeting notes, sign-in sheets, all comments received, and questions from the public will be included in Appendix B, C, D, E, F, G, H and I. Comment analysis will be summarized in section 3.0 Public Comment Analysis.

Location	Bertha Knight Landes Room, 1st Floor City Hall 600 4th Avenue, Seattle, WA 98104
Time	February 27, 2018; 6 p.m. – 8 p.m.
Capacity	100+
Link to URL Invite	BKL Event Invitation

2.4 Scheduled Focus Group Meeting(s)

Meeting 1

Community Engaged	Council on American-Islamic Relations - Washington (CAIR-WA)
Date	Thursday, February 21, 2019

Meeting 2

Community Engaged	Entre Hermanos
Date	Thursday, February 28, 2019

Meeting 3

Community Engaged	Byrd Barr Place
Date	Thursday, February 28, 2019

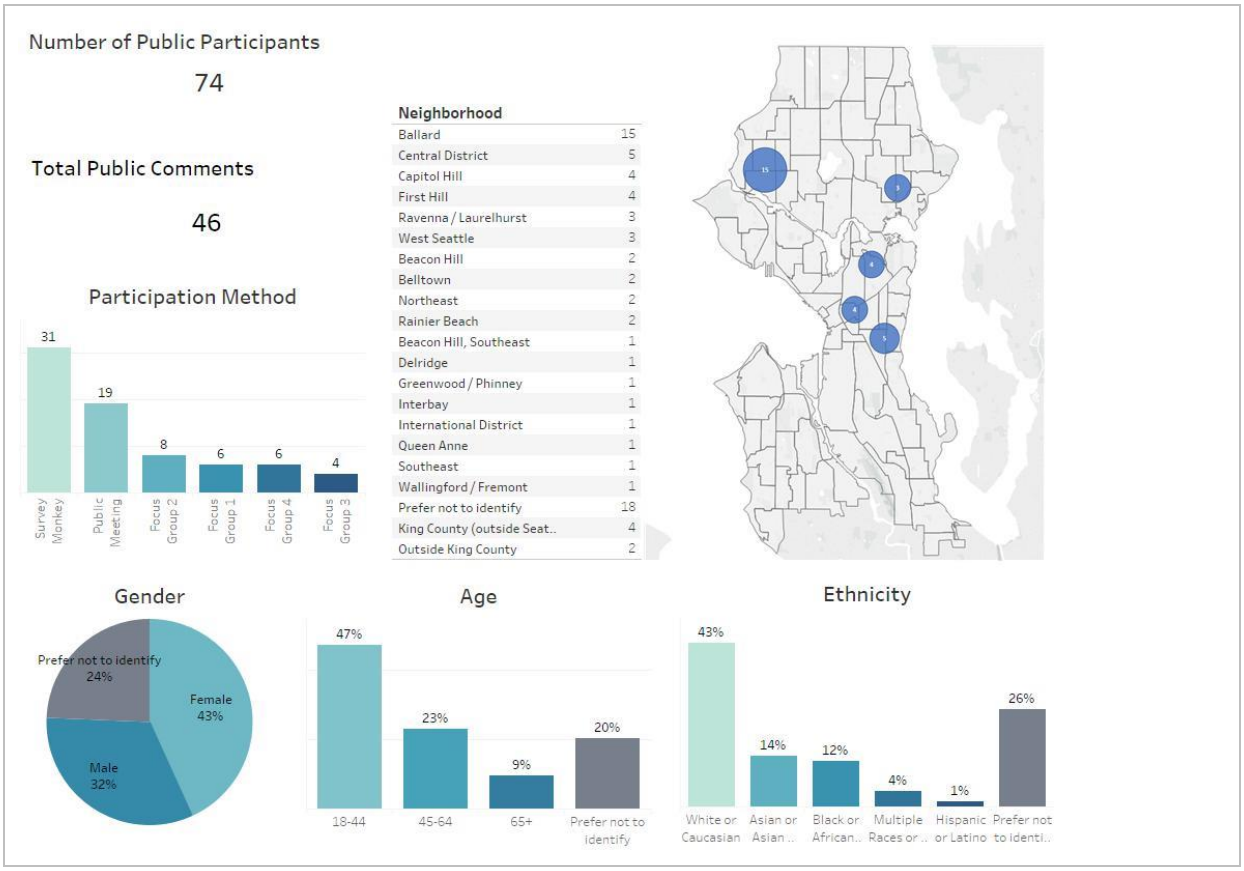
Meeting 4

Community Engaged	Friends of Little Saigon
Date	Wednesday, February 27, 2019

City of Seattle

3.0 Public Comment Analysis

3.1 Summary of Response Volume



3.2 Question One: What concerns, if any, do you have about the use of this technology?

Due to the low volume of responses received about this technology, a comment analysis was not able to be completed. Please see Appendix E for all comments received from the public about this technology.

3.3 Question Two: What value, if any, do you see in the use of this technology?

Due to the low volume of responses received about this technology, a comment analysis was not able to be completed. Please see Appendix E for all comments received from the public about this technology.

3.4 Question Three: What do you want City leadership to consider about the use of this technology?

Due to the low volume of responses received about this technology, a comment analysis was not able to be completed. Please see Appendix E for all comments received from the public about this technology.

3.5 Question Four: Do you have any other comments?

Due to the low volume of responses received about this technology, a comment analysis was not able to be completed. Please see Appendix E for all comments received from the public about this technology.

4.0 Equity Annual Reporting

4.1 What metrics for this technology be reported to the CTO for the annual equity assessments?

The Seattle Police Department is currently working to finalize these metrics.

Privacy and Civil Liberties Assessment

Purpose

This section shall be completed after public engagement has concluded and the department has completed the racial equity toolkit section above. The privacy and civil liberties assessment is completed by the community surveillance working group ("working group"), per the surveillance ordinance which states that the working group shall:

"Provide to the executive and the City Council a privacy and civil liberties impact assessment for each SIR that must be included with any departmental request for surveillance technology acquisition or in-use approval. The impact assessment shall include a description of the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities. The CTO shall share with the working group a copy of the SIR that shall also be posted during the period of public engagement. At the conclusion of the public engagement period, the CTO shall share the final proposed SIR with the working group at least six weeks prior to submittal of the SIR to Council for approval. The working group shall provide its impact assessment in writing to the executive and the City Council for inclusion in the SIR within six weeks of receiving the final proposed SIR. If the working group does not provide the impact assessment before such time, the working group must ask for a two-week extension of time to City Council in writing. If the working group fails to submit an impact statement within eight weeks of receiving the SIR, the department and City Council may proceed with ordinance approval without the impact statement."

Working Group Privacy and Civil Liberties Assessment

The Working Group's Privacy and Civil Liberties Impact Assessment (PCLIA) for this technology is below, and is also included in the Ordinance submission package, available as an attachment.

From: Seattle Community Surveillance Working Group
(CSWG) To: Seattle Chief Technology Officer
Date: July 10, 2019
Re: Privacy and Civil Liberties Impact Assessment for NICE 9-1-1 Logging Recorder

Executive Summary

On June 4, 2019, the CSWG received the Surveillance Impact Report (SIR) on the NICE 9-1-1 Logging Recorder, a surveillance technology included in Group 2 of the Seattle Surveillance Ordinance technology review process. This document is CSWG's Privacy and Civil Liberties Impact Assessment for this technology as set forth in SMC 14.18.080(B)(1), which we provide for inclusion in the final SIR submitted to the City Council.

This document first provides our recommendations to the Council, then provides background information, key concerns, and outstanding questions on the Logging Recorder technology.

Our assessment of the Logging Recorder focuses on three major issues rendering protections around this technology inadequate:

1. There is no clear policy defining the purpose and allowable uses of the Logging Recorder data.
2. The 90-day data retention period for Logging Recorder data is lengthy and is not clearly justified in the SIR.
3. There is no clear designation of what data collected by the Logging Recorder is shared with third parties and for what purposes.

Recommendations

The Council should adopt clear and enforceable rules that ensure, at the minimum, the following:

1. The purpose and allowable uses of the Logging Recorder data must be clearly defined, and both SPD and NICE (the vendor of the technology) must be restricted to those uses.
2. NICE must delete all Logging Recorder data after 7 days.
3. There must be a clear designation of what data collected by the Logging Recorder is shared with third parties and for what purposes.
4. NICE or any other third party that has access to Logging Recorder data must be held to the same restrictions as SPD, including industry best practice security standards.

City of Seattle

Background

The 9-1-1 Logging Recorder is a technology provided by the company NICE Ltd. and used by the Seattle Police Department (SPD) to automatically audio-record all telephone calls received by SPD's 9-1-1 Center as well as all radio traffic between dispatchers and SPD patrol officers. These recordings are then used for evidentiary purposes by officers, detectives, and prosecutors, and within the 9-1-1 Center for training and quality control purposes.[1]

Data storage is described in the SIR as follows:

> "The data is stored in the NICE system, with much of the NICE system physically housed at SPD's 9-1-1 Center. Some servers are hosted virtually on SPD's network in SPD's section of the city data center. Data collected are located in server storage, and extracted data are stored on file shares for SPD and City Law—these reside in SPD Network Storage or Law storage system managed by Seattle IT. Extracted data is electronically sent to Law, Discovery, or as redacted material in response to Public Disclosure Requests."[2]

Key privacy and civil liberties concerns relate to purpose of use, data retention, and data shared with third parties. Because the content and nature of phone calls to the 9-1-1 Center may include highly sensitive and/or personally-identifying information, it is important that such information is used only for a specifically defined purpose, retained only for the length of time necessary to fulfill that purpose, and data shared with third parties is limited to fulfilling the defined purpose.

Key Concerns

1. **There is no clear policy defining the purpose and allowable uses of the Logging Recorder data.** With a 90-day retention policy[3] and with SPD receiving 900,000 calls per year,[4] there are about 220,000 audio recordings existing at any given time. This volume of data is large enough to be repurposed for data mining or other unauthorized uses.[5] SPD, NICE, and third parties must be prohibited from using Logging Recorder data for any purpose beyond evidentiary, SPD officer training, quality control for the 9-1-1 calls system, and public disclosure purposes.[6]

2. **The 90-day data retention period for Logging Recorder data is lengthy and is not clearly justified in the SIR.** A memo in the SIR from SPD Deputy Chief Garth Green (dated April 29, 2019)[7] states:

[1] Privacy Impact Assessment, Surveillance Impact Report, 911 Logging Recorder, SPD, page 8.
[2] Privacy Impact Assessment, Surveillance Impact Report, 911 Logging Recorder, SPD, page 16.
[3] Submitting Department Memo, Surveillance Impact Report, 911 Logging Recorder, SPD, page 3-4.
[4] https://www.seattle.gov/police/about-us/about-policing/9-1-1-center
[5] Appendix G: Letters from Organizations or Commissions, Surveillance Impact Report, 911 Logging Recorder, page 114.
[6] Privacy Impact Assessment, Surveillance Impact Report, 911 Logging Recorder, SPD, page 7.
[7] Submitting Department Memo, Surveillance Impact Report, 911 Logging Recorder, SPD, page 3-4.

"Recordings in the NICE system are retained for 90 days. Recordings requested for law enforcement and public disclosure are downloaded and saved within other SPD systems for the retention period related to the incident type to which the recording is related." But as stated above, this massive volume of data could be repurposed, and a shorter retention period would help alleviate this concern.

3. **There must be a clear designation of what data collected by the Logging Recorder is shared with third parties and for what purposes.** Section 6.0 of the SIR states that "discrete pieces of data" are shared with outside entities and individuals, but does not elaborate further. The April 29 memo from Deputy Chief Garth Green provides examples of specific data shared with outside entities (e.g., call audio, time stamps for start and end of calls, staff position of the individual answering the call, duration of the call, and the phone number and/or radio channels used to contact 9-1-1), but it is not clear that these examples constitute an exhaustive list. A more systematic and comprehensive catalogue of what third parties may receive data from the system, and for what purpose, should be created to ensure consistency and guard against mission creep.

4. **NICE has a concerning history of data breaches.**[8] A severe vulnerability discovered in 2014 allowed unauthorized users full access to a NICE customer's databases and audio recordings.[9] Again, in 2017, a NICE-owned server was set up with public permissions, exposing phone numbers, names, and PINs of 6 million Verizon customers.[10] Given this history, it is even more important to ensure that best practice data security is implemented on this sensitive data.

Outstanding Questions

The following information should be included in an update to the 9-1-1 Logging Recorder SIR:

1. Is there a policy defining the allowed uses of 9-1-1 Logging Recorder data by NICE?
2. What justifies NICE's lengthy 90-day data retention period?
3. What are types of data may be shared with third parties and under what circumstances?

The answers to these questions can further inform the content of any binding policy the Council chooses to include in an ordinance on this technology, as recommended above.

[8] Appendix G: Letters from Organizations or Commissions, Surveillance Impact Report, 911 Logging Recorder, page 114.

[9] https://krebsonsecurity.com/2014/05/backdoor-in-call-monitoring-surveillance-gear/

[10] https://www.techspot.com/news/70106-nice-systems-exposes-14-million-verizon-customers-open.html

City of Seattle

CTO Response

Memo

Date: 11/17/2020

To: Seattle City Council, Transportation and Utilities Committee

From: Saad Bashir

Subject: CTO Response to the Surveillance Working Group 911 Logging Recorder SIR Review

---

To the Council Transportation and Utilities Committee Members,

I look forward to continuing to work together with Council and City departments to ensure continued transparency about the use of surveillance technologies and finding a mutually agreeable means to use technology to improve City services while protecting the privacy and civil rights of the residents we serve.

As provided in the Surveillance Ordinance, SMC 14.18.080, this memo outlines the Chief Technology Officer's (CTO's) response to the Surveillance Working Group assessment on the Surveillance Impact Report for Seattle Police Department's 911 Logging Recorder.

Background

The Information Technology Department (ITD) is dedicated to the Privacy Principles and Surveillance Ordinance objectives to provide oversight and transparency about the use and acquisition of specialized technologies with potential privacy and civil liberties impacts. All City departments have a shared mission to protect lives and property while balancing technology use and data collection with negative impacts to individuals. This requires ensuring the appropriate use of privacy invasive technologies through technology limitations, policy, training and departmental oversight.

The CTO's role in the SIR process has been to ensure that all City departments are compliant with the Surveillance Ordinance requirements. As part of the review work for surveillance technologies, ITD's Privacy Office has facilitated the creation of the Surveillance Impact Report documentation, including collecting comments and suggestions from the Working Group and members of the public about these technologies. IT and City departments have also worked collaboratively with the Working Group to answer additional questions that came up during their review process.

Technology Purpose

This application automatically records telephone calls received by the 9-1-1 communications center. The content and nature of those phone calls may include highly sensitive information such as the caller's name, phone number, address from which they are calling, medical conditions, detailed information about suspects, witnesses, or victims of a crime or other emergency events, and potentially other personally identifiable information. Callers may report personally identifying information about third parties without providing notice to those individuals. While most of this information is consciously

volunteered by callers, some of the information may be stored for future reference in emergency situations, for quality assurance purposes, or as evidence in a criminal investigation.

Recordings of 9-1-1 calls and radio traffic are routinely provided to detective units to assist in criminal investigations. In addition, SPD provides approximately 5000 recordings to the Seattle Law Department each year to support legal proceedings Recordings are also used as a quality assurance measure to review calls to ensure that call takers and dispatchers are following SPD policies and procedures and to ensure SPD practices meet or exceed industry standards.

Working Group Concerns

In their review, the Working Group raised concerns about this technology being used in a privacy impacting way, including issues relating to use specification, retention, and data sharing and security. The concerns are:

1. Lack of clear policy defining the purpose and allowable uses of the Logging Recorder data.
2. Justification for the 90-day data retention period for Logging Recorder data.
3. Lack of clarity about third-party data sharing content and purpose or justification.

We believe that policy, training and technology limitations enacted by Seattle Police Department and outlined in the SIR provide adequate mitigation for the potential privacy
and civil liberties concerns raised by the Working Group about the use of this important operational technology.

Response to Specific Concerns: 911 Logging Recorder

Concern: There is no clear policy defining the purpose and allowable uses of the Logging Recorder data.

CTO Assessment: The uses for this technology are outlined in the SIR. It is used to record all incoming calls to the 9-1-1 system, non-emergency calls and police radio traffic for use later in investigations, legal action, and public records requests. Access and security of the information and system is assured through access controls and security measures as required by Criminal Justice Information Systems Security Policy. The responses in the appropriate sections of the SIR provide clear and detailed information about the laws and policies regarding the use and access to this system.

SIR Response:
Section 3.1: Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

The technology is used in two distinct ways. Primarily it automatically records all calls into the 9-1-1 system, police non-emergency phone line, and police radio traffic. Secondarily, it is used to retrieve recordings by authorized personnel.

Authorized SPD users may access the recordings by logging into the NICE 9-1-1 Logging Recorder utilizing a unique username and password. Access for personnel into the system is predicated on state and federal law governing access to criminal justice information systems. This includes thorough background investigations for each user, appropriate access and permissions dependent on the personnel role, and an audit of access and transaction logs within the system.

Section 3.2: List the legal standards or conditions, if any, that must be met before the project / technology is used.

The technology is used to record all telephone calls between the public and the 9-1-1 Center, and police radio traffic. This is triggered when a community member contacts the department by calling 9-1-1 or the departments non-emergency numbers, including all outbound calls placed by 9-1-1 call takers and dispatchers and all radio traffic between dispatchers and police personnel including police officers, parking enforcement officers, and police detectives utilizing the police radio system.

Requests for audio recordings are initiated by detective units investigating a crime, legal counsel, and other outside entities. Recordings may also be initiated by the public using the Public Disclosure Process.

In addition, RCW 9.73.090 permits police, fire, emergency medical service, emergency communication center, and poison control center personnel to record incoming telephone calls to police and fire stations, licensed emergency medical service providers, emergency communication centers, and poison centers.

Concern: The 90-day data retention period for Logging Recorder data is lengthy and is not clearly justified in the SIR.

CTO Assessment: The data retention for the information collected through this system provides adequate time for any investigation, review, audit or litigation that may occur regarding the recordings. A shorter period of time for data retention is not required or advised. In addition, the SIR provides details and policy information about data deletion and governance of the data collected.

SIR Response:
Section 5.3: What measures will be used to destroy improperly collected data?

SPD policy contains multiple provisions to avoid improperly collecting data. SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a GO Report. SPD Policy 7.090 specifically governs the collection and submission of photographic evidence. Evidence is submitted to the Evidence Unit and associated with a specific GO Number and investigation. And, SPD Policy 7.110 governs the collection and submission of audio recorded statements. It requires that officers state their name, the Department name, the General Offense number, date and time of recording, the name of the interviewee, and all persons present at the beginning of the recording.

Additionally, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002. SPD Policy 5.001 also ensures that communication on the systems subject to collection on this system is official in nature.

Per the CJIS security policy:

5.8.3 Digital Media Sanitization and Disposal The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

Concern: There is no clear designation of what data collected by the Logging Recorder is shared with third parties and for what purposes.

CTO Assessment: SPD provides clear and adequate details about third party agencies with whom the 911 logging recording data is shared and for what purposes. Specification and compliance to the agreements between departments and agencies are provided in the SIR, including information about the Washington Public Records Act and possible redaction or exemptions.

SIR Response:
Section 6.1: Which entity or entities inside and external to the City will be data sharing partners?
No person, outside of SPD and Seattle IT, has direct access to the application or the data.

As Seattle IT supports the NICE system on behalf of SPD, a Management Control Agreement exists between SPD and Seattle IT. The agreement outlines the specifications for compliance, and enforcement related to supporting the NICE system through inter-departmental partnership. The MCA can be found in the appendices of the SIR.

Data obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law. Data may be shared with outside entities in connection with criminal prosecutions:

- Seattle City Attorney's Office
- King County Prosecuting Attorney's Office
- King County Department of Public Defense
- Private Defense Attorneys
- Seattle Municipal Court
- King County Superior Court
- Similar entities where prosecution is in Federal or other State jurisdictions

Data may be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

Discrete pieces of data collected by CAD may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by SPD Policy 12.050 and 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayoral Directive, dated February 6, 2018.

SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the system.

Section 6.1: Data sharing is not an automatic component of the 9-1-1 recording system. Instead, discrete recordings may be shared only within the context of the situations outlined in 6.1.

Section 6.3.1: Are there any restrictions on non-City data use?

Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20, regulating criminal justice information systems. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260 (auditing and dissemination of criminal history record information systems), and RCW Chapter 10.97 (Washington State Criminal Records Privacy Act). Once disclosed in response to PRA request, there are no restrictions on non-City data use; however, applicable exemptions will be applied prior to disclosure to any requestor who is not authorized to receive exempt content.

Concern: Security of system and protection from data breach

CTO Assessment: No computer system is completely immune from potential data breach however, SPD and Seattle IT have implemented industry best practices regarding access controls, intrusion detection tools, multi-factor authentication, audit logs, and firewalls per CJIS regulatory requirements to ensure the security of the data collected by this and all other SPD systems. The relevant SIR responses below provide details about the measures in place to secure data at collection, in transit and at rest.

SIR Response:

Section 4.10: What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

Only authorized SPD users can access the system, technology, or the data. Access to the application is limited to SPD personnel via password-protected login credentials. Logs of system activity are kept for both automatic system functions and user actions which provide an audit trail to safeguard against potential unauthorized access to stored information. In addition, the following security measures are in place to ensure data and system security:

- Data is securely input and used on SPD's password-protected network with access limited to authorized detectives and identified supervisory personnel.

- The entire system is located on the SPD network which is protected by industry standard firewalls. The Seattle IT Department performs routine monitoring of the SPD network.

- All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.

- SPD's Audit, Policy and Research Section (APRS) can conduct an audit of the any and all systems at any time. The Office of Inspector General and the federal monitor can also access all data and audit for compliance at any time.

- ITD client services interaction with SPD systems is governed according to the terms of the 2018 Management Control Agreement between ITD and SPD, which states that:

- "Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBIs Criminal Justice Information Services, (CJIS) Security Policy."
- This MCA document may be found in Appendix I.

CJIS Security Policy
Additionally, per the CJIS Security Policy, the following safeguards are in place:

- The agency shall establish identifier and authenticator processes.

- Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. 08/16/2018 CJISD-ITS-DOC-08140-5.7 37 password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).

- Unsuccessful login attempts - the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10-minute time period unless released by an administrator.

- When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128-bit strength to protect CJI.

- When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption. When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256-bit strength.

- Intrusion Detection Tools/Techniques such as monitor inbound and outbound communications for unusual or unauthorized activities, send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort, employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.

- Audit - Each agency shall be responsible for complying with all audit requirements for use of CJIS Systems. Each CSO is responsible for completing a triennial audit of all agencies with access to CJIS Systems through the CSO's lines.

- The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and

update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.

- A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage.

- Publicly accessible computers shall not be used to access, process, store or transmit CJI.

Appendix A: Glossary

Accountable: (taken from the racial equity toolkit.) Responsive to the needs and concerns of those most impacted by the issues you are working on, particularly to communities of color and those historically underrepresented in the civic process.

Community outcomes: (taken from the racial equity toolkit.) The specific result you are seeking to achieve that advances racial equity.

Contracting equity: (taken from the racial equity toolkit.) Efforts to achieve equitable racial outcomes in the way the City spends resources, including goods and services, consultants and contracting.

DON: "department of neighborhoods."

Immigrant and refugee access to services: (taken from the racial equity toolkit.) Government services and resources are easily available and understandable to all Seattle residents, including non-native English speakers. Full and active participation of immigrant and refugee communities exists in Seattle's civic, economic and cultural life.

Inclusive outreach and public engagement: (taken from the racial equity toolkit.) Processes inclusive of people of diverse races, cultures, gender identities, sexual orientations and socio-economic status. Access to information, resources and civic processes so community members can effectively engage in the design and delivery of public services.

Individual racism: (taken from the racial equity toolkit.) Pre-judgment, bias, stereotypes about an individual or group based on race. The impacts of racism on individuals including white people internalizing privilege, and people of color internalizing oppression.

Institutional racism: (taken from the racial equity toolkit.) Organizational programs, policies or procedures that work to the benefit of white people and to the detriment of people of color, usually unintentionally or inadvertently.

OCR: "Office of Civil Rights."

Opportunity areas: (taken from the racial equity toolkit.) One of seven issue areas the City of Seattle is working on in partnership with the community to eliminate racial disparities and create racial equity. They include: education, health, community development, criminal justice, jobs, housing, and the environment.

Racial equity: (taken from the racial equity toolkit.) When social, economic and political opportunities are not predicted based upon a person's race.

Racial inequity: (taken from the racial equity toolkit.) When a person's race can predict their social, economic, and political opportunities and outcomes.

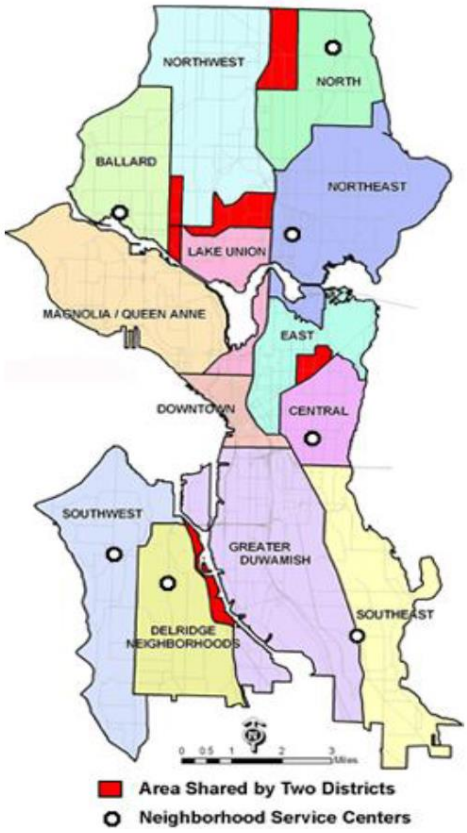
RET: "racial equity toolkit"

Seattle neighborhoods: (taken from the racial equity toolkit neighborhood.) Boundaries defined for the purpose of understanding geographic areas in Seattle.

Stakeholders: (taken from the racial equity toolkit.) Those impacted by proposed policy, program, or budget issue who have potential concerns or issue expertise. Examples might include: specific racial/ethnic groups, other institutions like Seattle housing authority, schools, community-based organizations, change teams, City employees, unions, etc.

Structural racism: (taken from the racial equity toolkit.) The interplay of policies, practices and programs of multiple institutions which leads to adverse outcomes and conditions for communities of color compared to white communities that occurs within the context of racialized historical and cultural conditions.

Surveillance ordinance: Seattle City Council passed ordinance 125376, also referred to as the "surveillance ordinance."



SIR: "surveillance impact report", a document which captures the fulfillment of the Council-defined surveillance technology review process, as required by ordinance 125376.

Workforce equity: (taken from the racial equity toolkit.) Ensure the City's workforce diversity reflects the diversity of Seattle.

City of Seattle

Appendix B: Meeting Notice(s)

City Surveillance Technology Fair

February 27, 2018

6:00 p.m. – 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Join us for a public meeting to comment on a few of the City's surveillance technologies:

Seattle City Light
- Binoculars
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation
- Acyclica

Seattle Fire Department
- Computer Aided Dispatch

Seattle Police Department
- 911 Call Logging Recorder
- Computer Aided Dispatch
- CopLogic

Can't join us in person?

Visit www.seattle.gov/privacy to leave an online comment or send your comment to **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** The Open Comment period is from **February 5 - March 5, 2019.**

Please let us know at Surveillance@seattle.gov if you need any accommodations. For more information, visit Seattle.gov/privacy.

Surveys, sign-in sheets and photos taken at this event are considered a public record and may be subject to public disclosure. For more information see the Public Records Act RCW Chapter 42.56 or visit Seattle.gov/privacy. All comments submitted will be included in the Surveillance Impact Report.

City of Seattle

Giám Sát Thành Phố Hội Chợ Công Nghệ

ngày 27 tháng 2 năm 2019
6 :00 giờ chiều – 8:00 giờ chiều
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Hãy tham gia cuộc họp công cộng cùng chúng tôi để nhận xét về một số công nghệ giám sát của Thành phố:

Seattle City Light
- Ống nhòm quan sát
- Sensorlink Ampstik
- Đồng hồ đo máy biến áp của Sensorlink

Seattle Department of Transportation (Sở Giao Thông Vận Tải Seattle)
- Acyclica

Seattle Fire Department (Sở Phòng Cháy Chữa Cháy Seattle)
- Hệ Thống Thông Tin Điều Vận Có Máy Tính Trợ Giúp

Seattle Police Department (Sở Cảnh Sát Seattle)
- Hệ Thống Ghi Âm Cuộc Gọi 911
- Hệ Thống Thông Tin Điều Vận Có Máy Tính Trợ Giúp
- CopLogic

Quý vị không thể tới tham dự trực tiếp cùng chúng tôi?

Hãy truy cập www.seattle.gov/privacy và để lại nhận xét trực tuyến hoặc gửi ý kiến của quý vị tới **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** Giai đoạn Góp Ý Mở từ **Ngày 5 tháng 2 - Ngày 5 tháng 3 năm 2019.**

Vui lòng thông báo cho chúng tôi tại Surveillance@seattle.gov nếu quý vị cần bất kỳ điều chỉnh nào. Để có thêm thông tin, hãy truy cập Seattle.gov/privacy.

Các khảo sát, danh sách đăng ký và ảnh chụp tại sự kiện này được coi là thông tin công cộng và có thể được tiết lộ công khai. Để biết thêm thông tin, hãy tham khảo Public Records Act (Đạo Luật Hồ Sơ Công Cộng) RCW Chương 42.56 hoặc truy cập Seattle.gov/privacy. Tất cả các ý kiến đóng góp mà quý vị gửi đến sẽ được đưa vào Báo Cáo Tác Động Giám Sát.

City of Seattle

Eksibisyon ng Teknolohiya Sa Pagmamatyag sa Lungsod

Pebrero 27, 2019

6:00 p.m. - 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Samahan kami para sa isang pampublikong pagpupulong upang magbigay ng komento sa ilan sa mga teknolohiya sa pagmamanman ng Lungsod:

Seattle City Light
- Mga Binocular
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation (Departamento ng Transportasyon ng Seattle)
- Acyclica

Seattle Fire Department (Departamento para sa Sunog ng Seattle)
- Pagdispatsa sa Tulong ng Computer

Seattle Police Department (Departamento ng Pulisya ng Seattle)
- Rekorder ng Pagtawag sa 911
- Pagdispatsa sa Tulong ng Computer
- CopLogic

Hindi kami masasamahan nang personal?

Bumisita sa www.seattle.gov/privacy upang mag-iwan ng online na komento o ipadala ang iyong komento sa **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** Ang panahon ng Bukas na Pagkomento ay sa **Pebrero 5 - Marso 5, 2019.**

Mangyaring ipaalam sa amin sa Surveillance@seattle.gov kung kailangan mo ng anumang tulong. Para sa higit pang impormasyon, bumisita sa Seattle.gov/privacy.

Itinuturing na pampublikong rekord ang mga survey, papel sa pag-sign-in at mga larawan na makukuha sa pangyayaring ito at maaaring mapasailalim sa paghahayag sa publiko. Para sa higit pang impormasyon, tingnan ang Public Records Act (Batas sa Mga Pampublikong Rekord) RCW Kabanata 42.56 o bumisita sa Seattle.gov/privacy. Isasama ang lahat ng isinumiteng komento sa Surveillance Impact Report (Ulat sa Epekto ng Pagmamanman).

City of Seattle

Feria de tecnología de vigilancia ciudadana

27 febrero de 2019

De 6:00 p. m. a 8:00 p. m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Acompáñenos en la reunión pública para dar su opinión sobre algunas de las tecnologías de vigilancia de la ciudad:

Seattle City Light
- Binoculars
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation (Departamento de Transporte de Seattle)
- Acyclica

Seattle Fire Department (Departamento de Bomberos de Seattle)
- Computer Aided Dispatch

Seattle Police Department (Departamento de Policía de Seattle)
- 911 Call Logging Recorder
- Computer Aided Dispatch
- CopLogic

¿No puede asistir en persona?

Visite www.seattle.gov/privacy para dejar un comentario en línea o enviar sus comentarios a **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** El período de comentarios abiertos es desde el **5 de febrero al 5 de marzo de 2019.**

Avísenos en Surveillance@seattle.gov si necesita adaptaciones especiales. Para obtener más información, visite seattle.gov/privacy.

Las encuestas, las planillas de asistencia y las fotos que se tomen en este evento se consideran de dominio público y pueden estar sujetas a la difusión pública. Para obtener más información, consulte la Public Records Act (Ley de Registros Públicos), RCW capítulo 42.56, o visite Seattle.gov/privacy. Todos los comentarios enviados se incluirán en el Informe del efecto de la vigilancia.

City of Seattle

Kormeerida Bandhigga Tiknoolajiyada ee Magaalada

Feebaraayo 27, 2019
6:00 p.m. - 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Nagulasoo biir bandhigga dadweynaha si fikir looga dhiibto dhawr kamid ah aaladaha tiknoolajiyada ee City surveillance:

Seattle City Light
- Binoculars
- Sensorlink Ampstik
- Sensorlink Cabiraha mitirka Gudbiyaha

Seattle Department of Transportation
(Waaxda Gaadiidka ee Seattle)
- Acyclica

Seattle Fire Department
(Waaxda Dab damiska ee Seattle)
- Adeeg Qaybinta Kumbuyuutarka loo adeegsado

Seattle Police Department
(Waaxda Booliiska ee Seattle)
- Qalabka Duuba Wicitaanada 911
- Computer Aided Dispatch
- CopLogic

Nooguma imaan kartid miyaa si toos ah?

Booqo barta www.seattle.gov/privacy si aad fikirkaaga oonleen ahaan uga dhiibato **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.**
Mudada Fikrad Dhiibashadu furantahay waxay kabilaabanaysaa
Feebaraayo 5 - Maarso 5, 2019.

Fadlan noogusoo gudbi ciwaankaan Surveillance@seattle.gov hadaad ubaahantahay hooy laguusii qabto. Wixii macluumaad dheeri ah, booqo Seattle.gov/privacy.

Xog aruurinada, waraaqaha lasaxixaayo iyo sawirada lagu qaado munaasabadaan waxaa loo aqoonsanayaa diiwaan bulsho waxaana suuragal ah in bulshada lagu dhex faafiyo. Wixii macluumaad dheeri ah kafiiri Public Records Act (Sharciga Diiwaanada Bulshada) RCW Cutubkiisa 42.56 ama booqo Seattle.gov/privacy. Dhammaan fikradaha ladhiibto waxaa lagusoo darayaa Warbixinta ugu danbaysa ee Saamaynta Qalabka Muraaqabada.

City of Seattle

城市监控技术博览会

2019 年 2 月 27 日
下午 6:00 至下午 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 9810

加入我们的公众会议，留下您对纽约市监控技术的意见：

Seattle City Light
- 望远镜
- Sensorlink Ampstik
- Sensorlink 变压器表

Seattle Department of Transportation（西雅图交通局）
- Acyclica

Seattle Fire Department（西雅图消防局）
- 计算机辅助调度

Seattle Police Department（西雅图警察局）
- 911 通话记录录音器
- 计算机辅助调度
- CopLogic

无法亲自前来？

访问 www.seattle.gov/privacy 发表在线评论或将您的意见发送至 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124。开放评论期：2019 年 2 月 5 日至 3 月 5 日。

如果您需要任何住宿服务，请通过 Surveillance@seattle.gov 联系我们。要获得更多信息，请访问 Seattle.gov/privacy。

此次活动中的调查、签到表和照片被视为公共记录，可能会被公开披露。有关更多信息，请参阅 Public Records Act（信息公开法）RCW 第 42.56 章或访问 Seattle.gov/privacy。提交的所有意见都将包含在监控影响报告内。

City of Seattle

도시 감시 기술 박람회

2019 년 2 월 27 일
오후 6:00 – 오후 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

공개모임에 참여하시고, 도시 감시 기술과 관련한 의견을 공유해 주십시오.

Seattle City Light
- 쌍안경
- Sensorlink Ampstik
- Sensorlink 변압기 미터

Seattle Department of Transportation(시애틀 교통국)
- Acyclica

Seattle Fire Department(시애틀 소방국)
- 컴퓨터 지원 출동 지시

Seattle Police Department(시애틀 경찰국)
- 911 전화 기록 녹음기
- 컴퓨터 지원 출동 지시
- CopLogic

현장 참여가 어려우신가요?

www.seattle.gov/privacy 를 방문하셔서 온라인 의견을 남기시거나 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124 로 의견을 송부해 주시기 바랍니다. 공개 의견 수렴 기간은 2019 년 2 월 5 일 – 3 월 5 일입니다.

편의사항이 필요하신 경우 Surveillance@seattle.gov 로 문의해 주시기 바랍니다.
자세한 정보는 Seattle.gov/privacy 를 참조해 주십시오.

본 행사에서 수집된 설문 조사, 참가 신청서 및 사진은 공개 기록으로 간주되며 일반에 공개될 수 있습니다. 자세한 사항은 Public Records Act(공공기록물법) RCW 챕터 42.56 을 참조하시거나, Seattle.gov/privacy 를 방문하시기 바랍니다. 제출된 모든 의견은 감시 영향 보고서에 수록됩니다.

City of Seattle

城市監視技術展覽會

2019 年 2 月 27 日
下午 6:00 至下午 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

加入我們的公眾會議，留下您對紐約市監視技術的意見：

Seattle City Light
- 望遠鏡
- Sensorlink Ampstik
- Sensorlink 變壓器表

Seattle Department of Transportation（西雅圖交通局）
- Acyclica

Seattle Fire Department（西雅圖消防局）
- 電腦輔助發送

Seattle Police Department（西雅圖警察局）
- 911 通話紀錄錄音機
- 電腦輔助發送
- CopLogic

無法親自前來？

造訪 www.seattle.gov/privacy 發表線上評論或將您的意見傳送至 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124。開放評論期：2019 年 2 月 5 日至 3 月 5 日。

如果您需要任何便利服務，請透過 Surveillance@seattle.gov 聯絡我們。要獲得更多資訊，請造訪 Seattle.gov/privacy。

此次活動中的調查、簽入表和照片被視為公共紀錄，可能會被公開披露。有關更多資訊，請查閱 Public Records Act（資訊公開法）RCW 第 42.56 章或造訪 Seattle.gov/privacy。提交的所有意見都將包含在監視影響報告內。

City of Seattle

Appendix C: Meeting Sign-in Sheet(s)

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☒ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☒ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

☐ Include Middle Eastern

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☒ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☒ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☒ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☑ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☑ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☒ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☒ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☑ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☒ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☒ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☑ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☑ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☑ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

2

Queen Anne

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☑ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☑ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☒ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☒ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☒ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☑ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☑ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

X

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☒ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☒ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☒ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☒ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☒ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☒ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☑ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

leighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
] Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☒ 18-44
☐ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☒ Female
☐ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☑ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
] Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☐ 45-64
☑ 65+
☐ Prefer not to identify

Gender

☐ Female
☑ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

☑ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
] Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☑ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☑ Female
☐ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

SE KING COUNTY

☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☑ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
✓ Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☑ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☐ Female
☑ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☒ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☒ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☒ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☒ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☒ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☑ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☑ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☑ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☑ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☑ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☑ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Appendix D: Department of Neighborhood Focus Group Notes

Friends of Little Saigon (FOLS)

Please select which technology you wish to comment on:

☐SCL: Binoculars	☐SCL: Sensorlink Transformer Meter (TMS)	☐SFD: Computer-Aided Dispatch	☐SPD:9-11 Call Recorder
☐SCL: Sensorlink Ampstik	☐SDOT: Acyclica	☐SPD: Computer-Aided Dispatch	☒SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

- Will they keep the data safe on coplogic?
- Can it be hacked?
- What if you report your neighbour and your neighbour hacks the system and find out?
- What is the money amount limit for coplogic / Why is there a limit for coplogic?: (a community member says that she believes that the limit $500 or under, but it's hard to have a limit because a lot of packages cost more than $500 such as electronics get stolen and you won't be able to report it online)
- The departement is having all these technologies being used but not letting the public aware of it
- Coplogic is not clear and is confusing to use (what you can report and what you can't report)
- If coplogic is known by the community would they use it ? (Community members agreed that no one would use coplogic because it's not in Vietnamese. Not even people who speak english fluently even use it.
- Many community members don't trust the system)

What value, if any, do you see in the use of this technology?

- Coplogic has been going on for a few years it's not very effective. The only effective thing is that coplogic is doing saving police hours and time.

What do you want City leadership to consider about the use of this technology?

- Most of the time, our community don't report things because they don't trust the system, they often tell someone that they trust a friend. Is there an option that someone and report a crime for someone else?

Other comments:

- The government should be more transparent with the technology system with the public.

- The translation is much far removed from the actual Vietnamese language.
- The translation is very hard to understand, the language is out of context (The flyer is poorly translate)
- Is there resources to support these technologies? Is there translations so that it is accessible for everyone? Will this accommodate everyone?
- Police should have a software that connects them to translation and interpretation right away instead of having to call a translator
- How will other people know of the technology if they can't come to focus group meetings? Such as flyers? Social media? Etc.
- Besides face to face meetings, are there plans to execute this information of the technology and surveillance to the community?
- Will the City of Seattle go to community events, temple, the church to reach out to the community and explain the technologies?
- These technologies are taking a part of our taxes, so everyone should know. It should be for everyone to know, not only catered to one group or population.

Are there any questions you have, or areas you would like more clarification?

- How effective are the tools/technology?
- How many people know of these technologies? Provide statistics
- What are the statistics of the coplogic?
- What is the data and statistics for coplogic and what are people reporting?
- What is the most common crime that they are reporting?
- And how effective is coplogic based on the statistics and data?

City of Seattle

Friends of Little Saigon (FOLS)

Please select which technology you wish to comment on:

☐SCL: Binoculars	☐SCL: Sensorlink Transformer Meter (TMS)	☐SFD: Computer-Aided Dispatch	☒SPD:9-11 Call Recorder
☐SCL: Sensorlink Ampstik	☐SDOT: Acyclica	☒SPD: Computer-Aided Dispatch	☐SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

- CAD did not work from experience. A community member said that they reported that they needed assistance at 10:00pm and no one showed up, then had to call 911 at 12:00am and someone finally showed up at 4:30am
- Why create more options and technologies if the police department and government can not support it? It's a waste of time and money (taxes). Should have enough personals before they implement technology.
- Government should have enough personals to support translation if they choose to translate.

What do you want City leadership to consider about the use of this technology?

- The city should focus on having the community review the technologies that are yet to be implemented.
- The Vietnamese community is not getting the information we need to report crimes

Other comments:

- Engagement is very important. Engaging the community and engaging different demographics.
- Friday night, Saturdays, and Sunday afternoon work the best for the Vietnamese community.
- If the city wants to involve the vietnamese community and engage the Vietnamese community, it is important to accommodate with our community It is important to proofread the translation, have 3 people proofread. Someone
  pre 1975, post 1975 and current Vietnamese language. The government clearly does not proofread the translation.

Council on American Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington
Thursday, Feb. 21, 2019
Technology Discussed: CopLogic

1. Do you have concerns about this specific technology or how it's used?
    - Having used the system myself the one thing I noted was the type of report you can file, they ask questions like if you knew the suspect, and if you're saying no I don't know who did it. and you check a box that says I understand that no one is going to investigate this
        - What is the point of having a system in place than If no one is going to investigate it
        - It is for common things like my car is broken into and stuff was taken out of my car, you can file it if you need a report for insurance. But if you were to call that and report to the police, they wouldn't come for days
    - So for example if I can be a straight up Islamophobe and I can see a Muslim woman and make a bunch of false reports online, and how long would it take for someone to say I see you making all these reports. Because people can make so many different reports, how do you deal with that
        - There are very limited types of reports that it will accept. So if someone wanted to report graffiti and they were reporting more hate crime related graffiti an officer will review the report
        - So I think the review process would be really important
    - Another barrier is that it's an online system so we need to think about wifi access and there is this assumption that everyone has access to internet and computers. And what I'm hearing is that people can just file a report at a click of their finger. And if these people can do that on their computer what stops them from being able to file all these cases about certain groups and individuals.
    - Additional there have been cases in the past where people are abusing reporting system. This one doesn't allow you to report against known suspect but I could see that happening in the future so I wanted that to be mentioned. The other thing under protection is says all activity can be stored and the data Is monitored by lexis nexus… and this company does a lot of research on crime mapping which brings up some of the concerns on like CVE
        - But what you are saying is that lexis nexus does other mapping that it can use this information for
        - Yes, because I want to clarify what is the technological ambition of SPD because I don't think this would work well in the communities that SPD is supposed to served. And I would want a contract review of what lexis nexus does. Will the info stay on the data and server of lexis nexus, what happens to it
    - Another thing is has SPD given Lexis nexus to use this in any of the research data they do, because they put out a lot of information regarding mapping, and crime control. And what information are they allowed to take
    - We have seen recently people doing interesting things when reporting crimes. I think its important to realize that when reporting crime people have a different perception when

reporting crime. People will see you in a certain neighborhood and might think they stole that car, or are doing something bad here. So when we give people the ability to report online we need to be concerned with accessibility about people being able to report freely… and we saw for a year that if an African American person came to use a swimming pool someone can call and say they don't live here. I think SPD is trying alleviate some of those calls they are getting, but I don't think this is the solution to the problem
    - What is the logic behind this overall, because is seems like it presents more cons than pros, and what is analytics database you use to look at these reports. Because when I am using government data base I can see where I need more surveillance etc. so we are getting all these open wholes in the system. Is this a right wing Donald trump agenda to watch neighbors of color and surveillance
    - I think im more concerned with where does this information end up and how is it used
    - What is the usefulness of the information that is not followed up on. And how does it help the people it's actually serving? So for example someone works for an anti-Muslim white supremacy group and they have people in different areas report issues about different Muslim groups in Seattle how do you prove the validity of these information and make sure they aren't just causing harm
2. What value do you think this brings to our city?
    - I think technology saves time, money, makes filing a report easy, I had to do that once it takes a lot of time.
    - I appreciate that it is easier so something like a hit or run or a car breaking in, that's fine.
3. What worries you about how this is used?
    - The only issues I can think of right now is it seems like it would be very easy to make a fraudulent report or a report that is for a small thing that you can make into a big thing, like the things you see go viral on the internet. So now it seems like the barrier to making a police report is smaller
    - I agree I think the bar is lowered and different people are perceived differently. And we have seen how SPD criminalizes different communities for behaviors that don't need to be criminalizing
    - A lot of different kinds of reports have to do with peoples perceived notion, so my concern comes from how do we make sure that this kind of technology isn't used to map our where Muslims live/are, and there types of religious belief. Or isn't being used to monitor them. How do we ensure that this isn't used to map our communities
    - The only comment I have that in the forms I have filled out is it won't allow you to fill out the form if you are naming a specific individual, you can name a group, but a not a person. The following criteria is there no known suspects, it happens in Seattle, so things like thefts. So you can report, graffiti, identity theft, credit card fraud, simple shop lift. So when I click report it says if you have a suspect it says please call. And when I press report it allows me to report anonymously, so I could report against a community with no follow up
        - Well that doesn't stop them from targeting al-Noor masjid, or Safeway in new holly, or new holly gathering hall, and it can target the people in that

community. And people don't feel comfortable with increase police presences, so it targets area if not targeting people

- When I was buying the house in Dallas (participant currently still lives/works/plays in Seattle) one of the first things I did was looking at a crime map and based off of that if someone is making a lot of reports can that be used for crime mapping because than that can lower the property value. And if the police isn't following up then how is it being used
- Its definitely possible for people to report inaccurate information

4. What recommendations would you give policy makers at the City about this technology?
    a. But my concern is reporting someone that can really target people of color. And that happens much more threatening to people. So the concept of an upset black women is more intimidating than an upset women that is another race and how many times will behavior like that be reported. Or how many times will a black man be reported against because it seems scary. So I think it lowers the bar when you don't have to talk to an individual when you don't have to talk to a police
    b. My questions are, how accessible are cop logic to people who don't read or speak English. How is SPD going to do what they can to make sure that this doesn't negatively impact communities they are already having issues with like the Sea Tac community that already feels threaten and criminalized by communities.

5. Can you imagine another way to solve the problem this technology solves?
    - So the SPD is very data driven these days and the one thing we repeat is report report report, call 911 and report online whatever you thinking is happening because all of that goes into their data base and is used for them to use resources and put police based off of where there is more crime. The report report report mentality assumes there are good relationships between the community and police, so even if someone doesn't do something bad, I don't know that they would feel comfortable reporting, even if online
    - From the community I have come from I am almost certain that they haven't even used online reporting so how do we make sure that we are giving everyone access to use online reporting. And there are certain crimes that are so common in areas that they don't even report it because they think the police should already know about it
    - I think the department should solely rely on the technology only as a way of collecting info they should still use in personal resources to actively participant in local community and make connections you can't rely only on this technology alone to do this

6. Other comments
    a. Also in this day in age we need to consider that immigration is a issue, and this administrative has blended the different agencies so people have a hard time knowing where SPD starts and ICE starts and those lines have been blurred and that is a real concern for many families

Council on Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington

Thursday, Feb. 21, 2019

Technology Discussed: Binoculars/Spotting Scope

1. Do you have concerns about this specific technology or how it's used?
    0. People in our community don't have the access to say or be apart of these conversation. A lot of these people are literate, and might not have the same cultural values. For Muslim women there are a type of consent that you have when you walk outside and are covered in a certain away versus when you are in the privacy of your own home. And people might not have that cultural and religious awareness
    1. I had one quick concerns, as far as the data that is collected using these binoculars, who has access to it
        - Seattle City Light: Information goes into the billing system, which customers can access if they have the automated reader but do not have access to under the current system
    - I know the focus is on binoculars but my mind is on new technologies and when people who are consumers and feel like I am overcharged how do I follow up and get those issues resolved. For systems that are completed based off of technologies how will I know if that data is being altered.
    2.
2. What value do you think this brings to our city?
    0. I would just add this is more my general comments I think its good that Seattle city lights is providing notifications to people when this is happening. Are they wearing something visible that show people they are from Seattle city lights? And is there a way for people to complain?
        - Yes they are wearing vests that are very visible. Yes we have a couple different avenues the easiest is to call the customer service line and to submit a complaint there
3. What worries you about how this is used?
    0. My primary concerns on my end is if someone is looking into my home with binoculars its a privacy concern. Most Muslim women wear hijab and I don't feel comfortable if someone is using binoculars looking from the outside when we are not wearing the hijab. My concern is that it is a huge invasion of privacy
    1. I have a question as the women expressed the feeling of people reading the meters with binoculars, if the meter has abnormal behavior or is in a different place of the house. Have there been situations where someone sees the person looking at someone house with binoculars, and they might not have gotten notified. Or the meter might be on the opposite side of where they are looking. Are they getting background checks? Or are complaints being followed up

- Seattle City Light: Yes all city employees have background checks, and if a complaint gets called in they will go through disciplinary actions
- What are the average times for disciplinary actions. How long is the process for a full investigation
- Seattle City Light: It's a multiple step process in terms of different levels. There are warnings, and if there was undo actions. Timeline really depends, I'm not sure
- Cause I think that people who go through the different nuances of how privacy can be breach that is just the end all be all of how privacy can breach so I think there needs to be policy put in place so that people don't have their privacy breach and they are being monitored by a pedophile

4. What recommendations would you give policy makers at the City about this technology?
    0. When I look at the Seattle city of light they do a lot of estimated guesses and as a consumer they might give you a $500 fee based off of the estimated guesses so I think it is important to have some sort of device that better clearly shows how much you use

5. Can you imagine another way to solve the problem this technology solves?
    0. My other question is if its actually not efficient why do you get the option to opt out (of the new automated system). If there is an old school way of doing it that involves a breach of privacy because these are human beings using the binoculars, so If this other option is better why are people having the ability to opt out.
6. Other comments: (Many comments were discussed over Seattle City Light's upcoming change from binocular use to automated meter readers)
    0. Who opted out was it home owners?
    1. When we go to a place with 12 tenements do all 12 of them have the ability to opt out or in, or just the owners of the building?
    2. Each home owner has a schedule provided to them and it is a 3 day period which they can come in and look at the system
    3. Is there a cost to them to have the new meter.
        - Seattle City Light: There is no cost with getting the new meter, but there is still a cost If we have to send someone out there to read it
        - What I don't understand is why the new practice is not to just use the new system since that is more accurate and it is doesn't require binoculars
        - What is the cost of opting out
        - Seattle City Light: There is a flat rate
    - I was gonna reiterate when we talk about equity and equitable practices. You can opt out (of the automated system) but there is a fee. And it makes me think

how much of It is a choose if one of these you have to pay for and the other one is free. So that sounds a little problematic when looking at choices of equity. I think choices are great, but also people need to be well informed. Like people within the community need to have more clear information to make the best decision for themselves

- Going back to people who make the decision. I want the person who are living in the house to know what decision is being made. So not just the person who owns the house, but the person living in the home. And not everyone it literate and not everyone speaks English. And its really important that you are giving them information they can actually consume. Instead of giving them notices they cant read

Council on Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington
Thursday, Feb. 21, 2019
Technology Discussed: Acyclica

1. Do you have concerns about this specific technology or how it's used?
    - Where does this data go? Does it go to SDOT? Google maps?
    - My other question is, it said whatever is being transferred is encrypted. All encrypted means to me is getting data from one device to another will be transferred without it being intercepted. What I don't know is, how much information are people getting
    - My concern is related to data, yeah we like to use gps. But what is the perimeter, what is the breach of access. Where is the data being used, and what can that turn into. we might be okay if the data is only being used for traffic related updates, but they might use it for more
    - I also would like to see how acyclica actually does what they do. They are using a lot of words that normally don't know. So I want to know how exactly they are hashing and salting. So for them to be clear about how they doing it. like when whatsapp encrypted they didn't give us the exact code but told us how they are doing it
    - Asking for a greater transparency for how they are doing this
    - I think the purpose of it is really important but the biggest concern is collecting all of this information without consent of passersby.
    - So the specific identifier that acyclica uses it mac addresses? You could potentially use that number to track that phone for the lifetime of the phone, for as long as that phone is on and being used. And that is very concerning.
    - Also I want to understand more where is this data going, and I want to know if this data is going to be used for future projects.
    - I want to ask is this something people opt into
    - People don't even know this is being used

2. What value do you think this brings to our city?
    - I like getting places and I like getting traffic information.
3. What worries you about how this is used?
    - What I don't like is you using my phone to get that information. I want whatever is in my cellphone to be protected. And I wanna know what you can access
    - I think based on Seattle and Seatac's higher up wanting to monitor and map out Muslims and where they are, and I don't like people being able to use our phone to track our location or actions they might think is violent. So based off of Seattle's track record and law enforcement agencies I don't like it
    - People who live outside of Seattle are also being impacted by it anytime they drive in Seattle
    - Could someone "opt out" by having wifi disabled on their device? I don't know if this covers cell towers. Because if it covers cell towers the only thing you could is having your phone on airplane mode

4. What recommendations would you give policy makers at the City about this technology?
    - I think the big question is why aren't we using other vendors, like I mentioned google maps, or waze, in fact komo 4 uses ways. Where other options we're looked at, and what were the trade off there's. And I want to see some transparency between the decision-making processes
    - I don't think this data should be shared with other private agencies, or other interagency programs
    - If all you're looking at is traffic flow, why are you not using the sensors in the road to give traffic flow updates.
    -
5. Can you imagine another way to solve the problem this technology solves?
    - I don't know if this already exists but something that makes it that data can't be used from one technology and use it for a different purposes
    - I think speaking from an industry perspective that is really important to have a processes for. Because all of this data is being used regardless of if you live in Seattle, or people live in different countries even who are visiting. That data is being collected. My understanding is that SDOT doesn't get the data directly. So my concern is how long can acyclica keep this data, use this data. Why wasn't a different option used, one in which some sort of consent can be used, so something like waze, google maps where people can opt in can get that information.
    - Road sensors or ways to count cars
    - I think its better to count cars than phones, because there is some expectation that your car will be monitored.
    - Using vehicle level granularity

City of Seattle

Entre Hermanos

Please select which technology you wish to comment on:

☐SCL: Binoculars	☐SCL: Sensorlink Transformer Meter (TMS)	☐SFD: Computer-Aided Dispatch	☐SPD:9-11 Call Recorder
☐SCL: Sensorlink Ampstik	☒SDOT: Acyclica	☐SPD: Computer-Aided Dispatch	☐SPD: CopLogic

1) What concerns, if any, do you have about the use of this technology?

El uso de wifi en Acyclica porque pueden obtener toda la información de los teléfonos.

Si vale la pena la inversión

Enfocando al grupo: La tecnología ya está instalada. que les preocupa de su uso?

El tráfico sigue igual.

Quien usa o almacena la información.

La preocupación es la colección de data.

Colección y almacenamiento de información es la mayor preocupación.

No es la colección de data lo alarmante sino los recursos (dinero utilizado) ya que o la tecnología no están funcionando porque el tráfico sigue igual. No hay cambio con la nueva tecnología, esos gastos no son válidos ya que no hay resultados. Esos gastos pudieran ser utilizados para la comunidad.

También tienen que ver si la tecnología emite radiación o alguna otra cosa dañina; perjudicial a la salud.

El gobierno tiene todos los datos.

No necesitan esta tecnología para tener los datos porque ya existen métodos para eso, incluso aplicaciones o alguna otra cosa.

La otra preocupación del grupo es que no haya un cambio al problema que se quiere resolver. En el caso de Acrylica sería el mejorar el tráfico.

- Tecnologías como esta necesitan recolectar más opiniones de expertos.
- Sería bueno que la información sea compartida con la comunidad. (Transparencia en fines y objetivos de la tecnología y datos guardados, tácticas implementadas.)

2) What do you want City leadership to consider about the use of this technology?

Hay lugares donde no se necesitan. En algunas partes de Magnolia, Queen Anne, Northgate, no se ocupan.

Seguimiento de pregunta: En las comunidades donde viven los latinos que tanto se ocupa Acyclica?

Participante no cree que allí se ocupan.

Hablaron sobre la necesitad de puntos estratégicos y calles con más necesidad de ayuda por causa del tráfico.

What do you think about this technology in particular ?

Bien, la tecnología ayuda con la velocidad o el movimiento de los coches.

La información se guarda y analizan por donde viajas o cuantas veces cruzas este rastreo.

Si es solo para ver el tráfico está bien.

Está bien en algunas partes. Puede que sea algo bueno. Pero puede que esta tecnología pueda compartir información personal que puede ser utilizada de otra forma en especial si hay Hacking (forma negativa, uso de datos).

La tecnología en sí no es tan grande (de tamaño) para ser algo visualmente desagradable. La información captada a través de estos medios puede que ayude a conducir el tráfico de mejor manera pero también puede que tome información personal.

Are there any questions you have, or areas you would like more clarification? ●

La tecnología no es un router, sino colección de data para planeaciones urbanas.

Participante: “quiero creer” “convencerme” que los sensores están allí para ayudar con el tráfico.

No se sabe cuándo las instalaron, los resultados deberían de ser públicos. Si la tecnología es para aliviar el flujo de tráfico entonces por qué no extienden el programa? O por qué no hay mejoramiento del tráfico?

Alternatives to this technology

- Alguna pantalla que indique cuáles vías son alternativas puede reemplazar esto.
- Cambios al límite de velocidad puede que alivie el flujo del tráfico.
- Dejar de construir tanto.
- Rediseño de calles ayudaría flujo de tráfico.
- El rediseñar las vías servirá para las futuras generaciones.

City of Seattle

Entre Hermanos

Please select which technology you wish to comment on:

☒SCL: Binoculars	☒SCL: Sensorlink Transformer Meter (TMS)	☐SFD: Computer-Aided Dispatch	☐SPD:9-11 Call Recorder
☐SCL: Sensorlink Ampstik	☐SDOT: Acyclica	☐SPD: Computer-Aided Dispatch	☐SPD: CopLogic

1) What concerns, if any, do you have about the use of this technology?

Los binoculares son preocupantes si la persona no tiene ética. Es preocupante que una persona vea a través de binoculares a que una tecnología mida el uso de la electricidad

Al grupo le incomoda el uso de binoculares

Sensorlynk específicamente la preocupación sería que le quita el trabajo a una persona.

Si es para detectar robo el grupo cree que hay otras maneras de saber quien roba

que no tan solo será para leer la electricidad sino para obtener otros tipos de información si cámaras fueran usadas

2) What value, if any, do you see in the use of this technology?

Ahorro de energía

Record y datos mas precisos

Oportunidad de trabajo a quien utiliza los binoculares

Estabiliza los precios de la electricidad

3) What do you want City leadership to consider about the use of this technology?

: Usar background check, uso de uniforme por trabajadores, cámara en binoculares.

What do you think about this technology in particular ?

Sensorlink Si

Binoculares son invasivos

Are there any questions you have, or areas you would like more clarification? ●

La confianza en estos medidores serán confiables? Serán efectivos?

El uso de binoculares se puede acompañar de una cámara añadida

Alternatives to this technology

Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad

City of Seattle

Entre Hermanos

Please select which technology you wish to comment on:

☐SCL: Binoculars	☐SCL: Sensorlink Transformer Meter (TMS)	☐SFD: Computer-Aided Dispatch	☐SPD:9-11 Call Recorder
☐SCL: Sensorlink Ampstik	☐SDOT: Acyclica	☐SPD: Computer-Aided Dispatch	☒SPD: CopLogic

1) What concerns, if any, do you have about the use of this technology?

Las fallas electrónicas son preocupantes especialmente en reportes policiacos.

Las preocupaciones es que el reporte no salió, no llegó por cualquier razón.

No todos podrán o saben usar las computadoras.

Fallas de los algoritmos de cada demanda es alarmante.

Que y cuando determina la urgencia de respuesta

Las personas le temen a los policías. Y este medio puede ayudar a que el miedo disminuya.

La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

2) What value, if any, do you see in the use of this technology?

La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

El uso de computadora está bien para las denuncias.

Si personas usan esta tecnología y es analizada en tiempo real por otras personas no hay problema.

Es otro método para denunciar

Está de acuerdo con el uso de computadoras para denunciar solo que no todos son capaz de usar este método/tecnología.

3) What do you want City leadership to consider about the use of this technology?
Que sea multi-idioma, implementar audio, implementar sistemas que ayuden a múltiples personas con diversas capacidades/necesidades

Si es usada de manera adecuada y como han dicho está bien.

El uso de la tecnología es bueno para dar respuesta para todas las cosas y personas

What do you think about this technology in particular ?

Grupo están de acuerdo con su uso.

Puede salvar una vida.

Los riesgos y acciones determinan la urgencia de la intermisión policiaca.

Alguna gente se siente más capaz de presentar una queja a través de este sistema, la tecnología en uso tiene validez.

Bueno para la violencia doméstica.

Are there any questions you have, or areas you would like more clarification?

La computadora decidirá la importancia/urgencia del reporte/emergencia dando a llevar acciones de emergencia.

Gravedad de emergencia es determina por tecnología.

La definición de emergencia es diferente con cada persona.

Cada uno tiene la definición de vigilancia, pero ¿que tal la definición de emergencia?

SITUATIONS TO APPLY ITS USE

Una pelea en la calle, un malestar corporal, cuestiones de vida, abuso doméstico

Si nos basamos en la definición de emergencia sólo en cuanto estemos en peligro inmediato o en tiempos mínimos/ de transcurrencia alarmante/peligrosa el uso de será implementado o limitado solo a instantes inmediatos de peligro.

Para reportar algo que ya sucedió o que son recurrentes.

Basado en el concepto de emergencia, las personas pueden tomar el método adecuado para reportar su caso y a través del medio necesario.

Los reportes no son anónimos.

Los datos son recolectados aun, a pesar de la opción escogida.

Alternatives to this technology

Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad

Entre Hermanos

City of Seattle
Surveillance

Inicio

Resumen: El departamento de vecindarios quiere saber la opinión de este grupo. Ellos verán videos de un minuto y medio y encontrarán folletos en sus mesas donde encontraran más información sobre lo visto.

Demográficos:

Ocho personas participaron, una de West Seattle, una de First Hill, dos de Ravenna/Laurelhurst y cuatro de King County (outside Seattle).

Cuatro personas se consideraron hispano o latino, una como india americana o nativa de Alaska, y tres no opinaron.

Cinco personas marcaron 18-44 como su rango de edad, dos marcaron 45-64 como el suyo y una no opinó.

Cinco personas marcaron masculino como género, una como transgénero, una como femenino, y otra no opinó.

Otra Información Importante:

- Preguntas serán hechas.
- Habrá una hoja para poder conversar sobre videos de interés
- Se les agradeció por venir.
- El concepto de vigilancia será manejado como la ciudad de Seattle lo maneja.
- Tom: Agradeció a los invitados por venir

Surveillance. In 2017 city council passed an ordinance to see what technology fit the definition of surveillance. The information gathered by these surveillance technologies are as follows: to “observe or analyze the movements, behaviors, or actions of identifiable individuals in a manner” which "is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice.”

Presentador: Preguntó si la conversación en inglés fue entendida.

Grupo: Concordó.

Tom: Do not let information on videos stop you from making comments or raising questions.

Presentador: Dio a entender el concepto de vigilancia como ha sido interpretada por la ciudad de Seattle. Fue analizada de esta manera: “La vigilancia es definida como tecnologías que observan o analizan los movimientos, comportamientos, o acciones de individuales identificables de una manera que razonablemente levanta inquietudes sobre libertades civiles, la libertad de expresión o asociación, igualdad racial o justicia social.”

- Los movimientos de la gente son observados a través de esta tecnología y puede que para algunas personas esto sea incómodo.
- Las cámaras de policía no califican como tecnologías de vigilancia en este tema.
- La presentación mostrada en la pantalla a través de los videos será transmitida en inglés.
- Se pidió que todos se traten con respeto y que opinen y que su nombre sea mencionado e incluso la vecindad donde viven.

El Grupo

Participante vino porque quiere obtener más información y dar su opinión. Es de Seattle.

Participante viene de Shoreline/Seattle para ver cuánto la tecnología entra afecta

Participante vino porque quiere saber qué información es colectada por el gobierno y para qué usan esa información. Puede que la información obtenida a través de la tecnología sea usada para perseguir a personas de color/minorías/personas marginadas.

Participante vino de First Hill, porque quiere ver el punto de vista de la ciudad y ver que opiniones surgirán.

Participante viene de Seatac porque tiene interés en el tema y porque la seguridad es importante y quiere saber a dónde llega la información.

Participante vine en Ravenna/Northgate, quiere ver que tan confiable es la tecnología y para qué es utilizada. Perjudicial o beneficial?

Participante vine en Seatac y vino porque es un tema muy interesante ya que se tiene que saber/mantener informado de lo que hacen los gobernantes.

Participante vino de Burien por la importancia del tema y la privacidad.

Presentador: La tecnología no es nueva. Ya está siendo usada. Y quieren saber el formato para que las futuras tecnologías tengan.

El video de Seattle Department of Transportation de Acyclica fue mostrado

Esta tecnología es un sensor que detecta el wifi. Es un sensor que detecta la tecnología wifi.

Seattle Metering Tool fue mostrada

Nadie del grupo sabe del tema más el presentador no hablará a fondo de esto para no influenciar opiniones.

Video de Fire Department's Computer Aided Dispatch fue mostrado

El 9-1-1 logging recorder video fue mostrado

Aclaración: Información impresa fue entregada explicando cada una de las tecnologías.

Video de Coplogic fue mostrado

El grupo no conocía que se puede reportar a la policía a través de su página/en línea.

El video de Seattle Police Computer Aided Dispatch fue mostrado

Esta tecnología es similar a la de los bomberos.

Se preguntó cuál video era de interés para analizar

Se acordó el análisis de Acyclica, Binoculares/Sensorlink, y Coplogic

Las Preguntas que sea harán serán las siguientes:

¿Qué piensan de este sistema de tecnología en específico y el motivo de usarla?
¿Cuál creen que sea el aporte de esta tecnología a la cuidad?
¿Qué preocupación les causa el uso que se le dará a este sistema?
¿Qué recomendarían a el grupo de políticos de la cuidad responsables de tomar las decisiones de implementar estas tecnologías?
¿Qué otra manera habría de resolver el problema que esta tecnología esta designada a resolver?

La Acyclica

Pregunta: ¿Qué piensan de este sistema de tecnología en específico y el motivo de usarla? (Como se usa y cuál es el uso)

- Bien, la tecnología ayuda con la velocidad o el movimiento de los coches.
- La información se guarda y analizan por donde viajas o cuantas veces cruzas este rastreo.

- Si es solo para ver el tráfico está bien.

- Está bien en algunas partes. Puede que sea algo bueno. Pero puede que esta tecnología pueda compartir información personal que puede ser utilizada de otra forma en especial si hay Hacking (forma negativa, uso de datos).

- La tecnología en sí no es tan grande (de tamaño) para ser algo visualmente desagradable. La información captada a través de estos medios puede que ayude a conducir el tráfico de mejor manera pero también puede que tome información personal.

Pregunta: Qué es lo que aporta esta tecnología a la ciudad?

- Seria algo bueno el aporte por la agilidad del tráfico solo si la tecnología está sincronizada con los semáforos, de otra manera no es útil si no aporta para el mejoramiento del tráfico.

- Participante dice que hay alternativas para esquivar el tráfico.

- Participante opina que la tecnología es interesante ya que usa google maps y está de acuerdo con el mejoramiento del tráfico.

- Si el objetivo es de mejorar el tráfico está de acuerdo. Pero también quiere saber en qué lugar(es) estarán los aparatos, si algunas personas serán beneficiadas más que otras.

Pregunta: Qué preocupaciones tienen con posible uso/uso potencial de esta tecnología?

- Le preocupa el uso de wifi en Acyclica porque pueden obtener toda la información de los teléfonos.

- Si el potencial puede ser aplicada a la inversión.

Enfocando al grupo: La tecnología ya está instalada, que les preocupa de su uso?

- El tráfico sigue igual.

- Quien usa o almacena la información.

- La preocupación es la colección de data.

Más de la mitad de grupo opina que esa (el almacén y colección de información) es la preocupación.

- Participante no está de acuerdo. No es la colección de data lo alarmante sino los recursos (dinero utilizado) ya que o la tecnología no están funcionando porque el tráfico sigue igual. No hay cambio con la nueva tecnología, esos gastos no son válidos ya que no hay resultados. Esos gastos pudieran ser utilizados para la comunidad.

- También tienen que ver si la tecnología emite radiación o alguna otra cosa dañina; perjudicial a la salud.

- El gobierno tiene todos los datos.

- Opinión de otro participante: No necesitan esta tecnología para tener los datos porque ya existen métodos para eso, incluso aplicaciones o alguna otra cosa.

La otra preocupación del grupo es que no haya un cambio al problema que se quiere resolver. En el caso de Acrylica sería el mejorar el tráfico.

- Tecnologías como esta necesitan recolectar más opiniones de expertos.

- Sería bueno que la información sea compartida con la comunidad. (Transparencia en fines y objetivos de la tecnología y datos guardados, tácticas implementadas.)

Pregunta: Le dirían algo a los políticos algo del lugar donde se encuentran estos aparatos?

- Hay lugares donde no se necesitan. En algunas partes de Magnolia, Queen Anne, Northgate, no se ocupan.

Seguimiento de pregunta: En las comunidades donde viven los latinos que tanto se ocupa Acyclica?

- Participante no cree que allí se ocupan.

Hablaron sobre la necesitad de puntos estratégicos y calles con más necesidad de ayuda por causa del tráfico.

Presentrador: Crees que Acylica es como el router de google?

- La tecnología no es un router, sino colección de data para planeaciones urbanas.

- Participante: “quiero creer” “convencerme” que los sensores están allí para ayudar con el tráfico.

- No se sabe cuándo las instalaron, los resultados deberían de ser públicos. Si la tecnología es para aliviar el flujo de tráfico entonces por qué no extienden el programa? O por qué no hay mejoramiento del tráfico?

Otra pregunta: Alguna otra tecnología que pueda ser utilizada en vez de Acyclica?

Alternativas:

- Alguna pantalla que indique cuáles vías son alternativas puede reemplazar esto.
- Cambios al límite de velocidad puede que alivie el flujo del tráfico.
- Dejar de construir tanto.
- Rediseño de calles ayudaría flujo de tráfico.
- El rediseñar las vías servirá para las futuras generaciones.

Tecnologia #2

Sensorlink/Binoculares

Pregunta: Que opina el grupo de la tecnología?

- Los binoculares son preocupantes si la persona no tiene ética. Es preocupante que una persona vea a través de binoculares a que una tecnología mida el uso de la electricidad.

- Un sensor que detecta la electricidad sería mejor.

- Al grupo le incomoda el uso de binoculares.

Pregunta: Qué opinas sobre la tecnología medidora de electricidad (sensorlink) y que sea usada en tu casa?

- No le incomoda o afecta a dos participantes.

- La preocupación sería que le quita el trabajo a una persona.

- Los binoculares son invasivos.

- Para que usar binoculares si es que se puede llegar a el hogar y ver el medidor en persona, pidiendo permiso? Si la tecnología es usa para ver que las personas se roban la electricidad, creen que no saben quiénes roban?

- El grupo cree que si saben.

Pregunta: Cual creen que sea el aporte que esta tecnología?

- El video dice que 3 millones de dólares son ahorrados.

Pregunta: De qué manera beneficia esto a la cuidad/ciudadanos/comunidad?

- El robo de la luz es preocupante.
- Si ya llevan el record y datos y le hacen saber a la comunidad puede que ahorren dinero.
- Uso de binoculares puede dar trabajo a una persona y dinero puede ser ahorrado con esta tecnología.
- La tecnología trae gasto de electricidad para poder ver gastos de luz? Si pretende evitar el robo entonces los gastos de la factura eléctrica deberían de seguir estables.

Pregunta: La confianza en estos medidores serán confiables? Serán efectivos?

- Ayuda a la precisión, a bajar precios.
- Que quiten los binoculares sería una sugerencia, o usar binoculares que graban con video.
- Si ya tienen récord sobre la energía (consumo, gastos, etc.), el robo de energía no es suficiente para establecer este tipo de tecnología ya que puede ser identificado el robo o alguna otra anomalía dependiendo en el nivel alto o bajo o repentino analizado/visto/detectado por métodos convencionales ya establecidos.
- Otra recomendación: Usar background check, uso de uniforme por trabajadores, cámara en binoculares.
- Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad
- .La preocupación es que no tan solo será para leer la electricidad sino para obtener otros tipos de información si cámaras fueran usadas.

Tecnologia #3 Coplogic

- Esta tecnología no solo el ahorro de tiempo, sino el ahorro de tiempo policial ya que ellos trabajarían en otras cosas
- El uso de computadora está bien para las denuncias.

- Si personas usan esta tecnología y es analizada en tiempo real por otras personas no hay problema.

Enfoque: Lo que estamos queriendo dialogar es el uso del internet y las denuncias.

- Es otro método para denunciar
- Está de acuerdo con el uso de computadoras para denunciar solo que no todos son capaz de usar este método/tecnología.

Pregunta: En que ayuda a la comunidad?

- Por qué usar estos métodos?
- Grupo están de acuerdo con su uso.
- Puede salvar una vida.
- Los riesgos y acciones determinan la urgencia de la intermisión policiaca.
- Alguna gente se siente más capaz de acudir a través de este sistema la tecnología en uso tiene validez.
- Bueno para la violencia doméstica.
- Las fallas electrónicas son preocupantes especialmente en reportes policiacos.
- Las preocupaciones es que el reporte no salió, no llegó por cualquier razón.
- No todos podrán o saben usar las computadoras.
- Fallas de los algoritmos o cuando o que promueve urgencia de cada demanda es alarmante.
- Criterio de demandas y que clase de preocupación de parámetros son confiables tienen que ser cuestionados/analizados, y que/quien es digno de prioridad o importancia o de ayuda.

Pregunta: De qué manera este uso beneficiaria a la comunidad?

- Personas pueden ser discriminadas

- Las personas le temen a los policías. Y este medio puede ayudar a que el miedo disminuya.

- La computadora decidirá la importancia/urgencia del reporte/emergencia dando a llevar acciones de emergencia.

- Gravedad de emergencia determina uso de tecnología.

Pregunta: Alguna inquietud sobre el uso de esta tecnología?

- La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

Pregunta: En qué situación usarán esta tecnología?

- Una pelea en la calle, un malestar corporal, cuestiones de vida, abuso doméstico
- Cada uno tiene la definición de vigilancia, pero que tal la definición de emergencia?
- La definición de emergencia es diferente con cada persona.
- Si nos basamos en la definición de emergencia sólo en cuanto estemos en peligro inmediato o en tiempos mínimos/ de transcurrencia alarmante/peligrosa el uso de será implementado o limitado solo a instantes inmediatos de peligro

Pregunta: Para qué sirve el reporte de la computadora?

- Para reportar algo que ya sucedió o que son recurrentes.
- Basado en el concepto de emergencia, las personas pueden tomar el método adecuado para reportar su caso y a través del medio necesario.
- Los reportes no son anónimos.
- Los datos son recolectados aun, a pesar de la opción escogida.

Pregunta: Qué les recomendarían a los políticos?

- Que sea multi-idioma, implementar audio, implementar sistemas que ayuden a múltiples personas con diversas capacidades/necesidades

Pregunta: Algún otro comentario en general sobre la tecnología de vigilancia?

- Si es usada de manera adecuada y como han dicho está bien.

- El uso de la tecnología es bueno para dar respuesta para todas las cosas y personas.

Consejo:

- Den información más información sobre lo que están haciendo. (transparencia/divulgación de información)

- Que haya más transparencia.

Ser transparentes sobre la colección de datos, para que haya discusiones y decisiones Informadas, en todas las tecnologías implementadas/por implementar.

Byrd Barr Place

2/28/2019 Surveillance Technology Focus Group

Thursday, February 28, 2019
1:42 PM

Disclaimer: some of these notes are written in first-person. These should not be considered direct quotes

Videos:

- Acyclica: sensors recognize when a wifi enabled device is in range of it. Attached to street lights
- 911 recorder: records the conversation with the person calling 911, and conversation with the dispatched officers
- CopLogic: Online police report, treated as a regular policy report
- Computer Aided Dispatch
- Seattle City Light: Binoculars for meter readers; sensor to see if someone is stealing electricity

Tom: Read definition of surveillance

Craig: invasion of privacy?

- Electric one: I never even know they had the sensor one.

Community Member: used to be in the tech industry for thirty years. Writing a book about surveillance and technology
Wanda: I like the online police report. If someone is experiencing a crisis or trauma, you can go ahead and report it.

- Surveillance, I understand the concern, but overall I think it's a good thing. There is good and bad in any location, you'll find people who are taking advantage of it, but hopefully there are systems in place.
- Used to work nights, and catching the bus at night is scary. Having the cameras and police out when catching the bus helps, I appreciate that. No one likes to be watched, but if it's gonna keep people safe, that's a good thing.

Mercy: security is a great safety issue
Craig: there are some parts of the neighborhood/city that need to be watched, and some that need to be left alone
Wanda: as long as it's even
Craig: Sometimes it's not even
Both: There are hot spots though

Which of the surveillance technologies do you think could be abused to pinpoint specific communities?

IG: The Computer Aided Dispatch

Talking about the International District:

- Lots of businesses and residential crammed together in a larger space
- Talking about a great community member who died; if they had surveillance technology them, maybe they would have found his killer

"Some neighborhoods need to be watched"

- Gangs; drug use

Tom: getting back to CAD, how do we feel about the information that is stored

- Craig: there are concerns, but who is allowed to see it, how is it stored? That's a concern
    - Is it used for BOLOs? Is it everyone who is in the area, all of the police officers? Or is there some discretion as to which police officers would be given the information?
- Wanda: plenty of people are arrested who "fit a description"
    - Discussion about the racial discrimination: how people who think that "all [insert race here] look alike".
    - Individuals may think like that, but police officers have the capability to ruin someone's life.
- Marjorie: just recently got a smart phone, and it's new to me that someone could know where I'm going and I wouldn't be aware of it
    - Without my consent.
- Mercy: grew up with the idea that big brother is watching you
    - Tracking how many times I go to the library seems like a waste of money
    - People who are not law abiding citizens, they are the ones to be worried
- Craig: What about selling weed, coke, etc. Should they be worried?
    - Mercy: well at least in Seattle, it's ok to sell
- Mercy: big brother is watching. We already know that, it's just more obvious now
- There is a lot of technology that we are not made aware of

Tom: So acyclica, is it worth it? Some people worried it's tracking, is it something that we can live without?

- Should we put up signs that this road is tracked?
    - Viron: Maybe
    - Mercy: let people out there know that you're on camera.
    - Viron: does it work if your device is not turned on?

Tom: what do you want to tell the city council about tech that is collecting personal information?

- Wanda: they should get our individual consent

- Martha: putting it on the ballot doesn't mean that you are getting individual consent, because if you vote no but it still passes, you didn't give your consent
- Deana: there are some places around Capitol Hill that I don't feel safe at at night
    - Talking about fire department responding to a fire in her building: when one building alarm system goes off, it goes directly to the fire department - affects multiple buildings.
        - Response time is very good.
    - I choose to turn off the GPS tracking, because I don't need people to know where I'm at
        - If others are watching where I'm at, that's an invasion of privacy. I should be able to walk out my front door and go wherever I want without anyone knowing.
- Location privacy: you can tell a lot about a person based on where they go, and tracking that can build a pretty extensive profile of who you are
- IG: now that I know they are tracking, I will turn it off.

Mr. Surveillance: Surveillance is always secret, and it's an aggressive act. It's meant to exert power over others.

Do you think any individual could raise enough concern that it would change anything?

- Resounding no
- Maybe with a larger group
    - Maybe with the whole city

SCL binoculars:

- Craig: they should warn their customers and let them know they are coming into their yard/looking through binoculars.
- Wanda: as long as they aren't looking in people's windows.
    - When we're walking down the street, it's a little different. Certain neighborhoods do need more surveillance than others

Regarding being watched in public:

- Eydie: in public, it depends on how long. If it's a short period of time, that's one thing, but if you're tracked the whole time you're out, it's unreasonable.
    - I don't know what the solutions would be.
    - Even when the meter read just walks into your yard, it's unnerving.
    - What’s the purpose of tracking it this way?
- Mercy: (referring to the acyclica) Why are they doing it all the time? Have they not gotten the information yet?
    - They should already know what the traffic flow would be.
    - We lost a lane to the bicyclist
- Craig: facial recognition used on the street is bad.
- Vyron: sometimes you can't walk down the street and shake someone's hand without getting in trouble

- Mr. Surveillance: The technology has gotten ahead of the law, and it means they have to pay less people

Tom: Are we willing to accept more technology to have less police?

- Craig: how about just making it even? Police have an image to people of color; they are afraid of why they are going to be there. We can police ourselves
- Wanda: I disagree. There are some who think there should be less, but there are also a lot of people who worry about walking down the street
    - As a woman and DV survivor, I appreciate the police and appreciate living in a country where I can call a number for help.
    - I have a big problem with the shooting of unarmed black men, but as an individual I still appreciate the police.
    - But I have a problem being tracked, and I have a problem being watched in my home.
- General comment: The number of police being on the corner is a touchy situation
    - Knowing the police that are on your corner makes a difference. They can police the community better if there is more of a relationship between the two.
- Craig: it has to be both, even. You can't trade off the technology for the police.
- Mr. Surveillance: The trend is they want to go to more technology and less police.

Tom: If right now we have lots of technology, and we want a balance, then how do we do that?

- Craig: keep it the way it is but clean up the police department. Make sure the people who are working there are good at their jobs, not biased or discriminating

CopLogic: making police reports online

- Craig: I think it's stupid.
    - Would use that technology for stupid crimes
- Mercy: you could report your neighbor for silly things
    - Anonymous reporting of crimes that could target people for things they might not call 911 for
- Wanda: there were some lines of traffic where I saw cars lined up with their windows smashed in; nothing taken, but glass all over the place.
    - Police response when called: maybe you should get a cheaper type of car
    - Would he have said that to us if we were a different skin color, or lived in a different neighborhood?
- IG: I think it's a bad thing: someone could make up a story and the officer didn't have to check it.
- Marjorie: I think the online reporting could be abused

City of Seattle

Appendix E: All Comments Received from Members of the Public

ID: 10617663909
Submitted Through: Survey Monkey
Date: 3/25/2019 1:19:54 PM
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SPD: 911 Logging Recorder
What concerns, if any, do you have about the use of this technology?
Medium Concerns: 1) Accidental release of private information of victims via PRA requests. While SPD does normally redact information that is legally exempt from disclosure via PRA request, audio recordings would be logistically more difficult on humans to do the redaction as compared to only text. With text, it's easier to search for known keywords/phrases; whereas with audio (given SPD doesn't have access to reliable voice-to-text technology, per email thread with SPD) if Public Disclosure Officers happen to have their attention slip from the audio momentarily, they may miss an important blip of content that should be redacted. 2) NICE911 supports passive logging (sniffing the local network for SIP traffic) or active logging (NG911 makes a conference call to the voice logger). Based on discussion at the tech fair, it's my understanding that SPD's telephone system is analog only, no VoIP, therefore no SIP traffic therefore SPD must be using active logging. This is fine. However, if in the future SPD does transition over to VoIP and switches to NICE911 passive call logging, then effort must be placed into correctly segmenting that section of the network otherwise all calls (even those not intended to be logged) will be logged, since passive logging means NICE911 will log ALL VoIP traffic it is able to sniff. Lesser Concern: 1) No 2-step-verification/2-factor-authentication (2SV/2FA) for login to NICE; however, an individual would need to first logon to an SPD workstation and then login to NICE. NICE isn't accessible externally to the SPD local network. That being said, page 13 of the SIR implies that 2FA is in place.
What value, if any, do you see in the use of this technology?
It meets a legal requirement; and could be used to help improve the handling of calls by staff.
What do you want City leadership to consider about the use of this technology?
Ensure proper care is taken both when SPD Public Disclosure Officers are listening to recordings to redact personal information that is exempt from disclosure via PRA requests; and if/when SPD ever considers moving to using VoIP, special care would need to be taken regarding the segmentation and security of that network.
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

ID: 10617425376
Submitted Through: Survey Monkey
Date: 3/25/2019 11:44:57 AM
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SPD: 911 Logging Recorder
What concerns, if any, do you have about the use of this technology?
My only concern is the valuable information that would be lost if this is NOT done.
What value, if any, do you see in the use of this technology?
Verification of information, useful for training, QC, and evidence in court cases.
What do you want City leadership to consider about the use of this technology?
This is vital information that needs to be gathered and kept.
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

ID: 3
Submitted Through: Focus Group
Date: 2/27/2019
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars, SCL: CheckMeter, SCL: AmpFork, SFD: CAD, SPD: CAD, SPD: 911 Logging Recorder
What concerns, if any, do you have about the use of this technology?
That would be good with advanced technology
What value, if any, do you see in the use of this technology?
Yes, around the city.
What do you want City leadership to consider about the use of this technology?
Need good train to people who use new technologies
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

ID: 10554344108
Submitted Through: Survey Monkey
Date: 2/25/2019
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SPD: 911 Logging Recorder
What concerns, if any, do you have about the use of this technology?
I think it should be widely used.
What value, if any, do you see in the use of this technology?
to speed up the efficiency of SPD
What do you want City leadership to consider about the use of this technology?
KEEP ON DOING THE GOOD WORK.
Do you have any other comments?
NOT YET
Are there any questions you have, or areas you would like clarification?

Appendix F: Department Responses to Public Inquiries

No public inquiries were received for this technology.

Appendix G: Letters from Organizations or Commissions

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

March 12th, 2019

Seattle City Council
600 4th Ave
Seattle, WA 98104

Re: Surveillance Ordinance Group 2 Public Comment

We would like to first thank City Council for passing one of the strongest surveillance technology policies in the country, and thank Seattle IT for facilitating this public review process.

These public comments were prepared by volunteers from the Community Technology Advisory Board (CTAB) Privacy & Cybersecurity Committee, as part of the surveillance technology review defined in Ordinance 125376. These volunteers range from published authors, to members of the Seattle Privacy Coalition, to industry experts with decades of experience in the information security and privacy sectors.

We reviewed and discussed the Group 2 Surveillance Impact Reports (SIRs) with a specific emphasis on privacy policy, access control, and data retention. Some recurring themes emerged, however, that we believe will benefit the City as a whole, independent of any specific technology:

- **Interdepartmental sharing of privacy best practices**: When we share what we've learned with each other, the overall health of the privacy ecosystem goes up.
- **Regular external security audits**: Coordinated by ITD (Seattle IT), routine third-party security audits are invaluable for both hosted-service vendors and on-premises systems.
- **Mergers and acquisitions**: These large, sometimes billion-dollar ownership changes introduce uncertainty. Any time a vendor, especially one with a hosted service, changes ownership, a thorough review of any privacy policy or contractual changes should be reviewed.
- **Remaining a Welcoming City**: As part of the Welcoming Cities Resolution, no department should comply with a request for information from Immigration and Customs Enforcement (ICE) without a criminal warrant. In addition, the privacy of all citizens should be protected equally and without consideration of their immigration status.

Sincerely,

Privacy & Cybersecurity Committee volunteers
Torgie Madison, Co-Chair
Smriti Chandashekar, Co-Chair
Camille Malonzo
Sean McLellan
Kevin Orme
Chris Prosser
Rabecca Rocha
Adam Shostack
T.J. Telan

Community Technology Advisory Board
Steven Maheshwary, CTAB Chair
Charlotte Lunday, CTAB Co-Vice Chair
Torgie Madison, CTAB Co-Vice Chair
Smriti Chandashekar, CTAB Member
Mark DeLoura, CTAB Member
John Krull, CTAB Member
Karia Wong, CTAB Member

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SFD: Computer-Aided Dispatch (CAD)

Comments

The use of a centralized Computer-Aided Dispatch (CAD) system is essential to protecting the health and safety for all Seattle citizens. The National Fire Protection Association (NFPA) standards outline specific alarm answering, turnout, and arrival times[1] that could only be accomplished in a city of this size with a CAD system.

In addition, with over 96,000 SFD responses per year (2017)[2], only a computerized system could meet the state's response reporting guidelines established in RCW 35A.92.030[3].

CentralSquare provides the dispatch service used by SFD. CentralSquare is a new entity resulting from the merger of Superion, TriTech, Zuercher, and Aptean[4] in September 2018.

Recommendations

- Tritech, the underlying technology supplying SFD with CAD services, has been in use since 2003 [SIR 4.3], making it 16 years old. As with any technology, advancements in security, speed, usefulness, and reliability come swiftly. Due to the age of the technology, we recommend conducting a survey into the plausibility of replacing Tritech as SFD's CAD solution.

- Tritech was merged very recently into CentralSquare in one of the largest-ever government technology mergers to date. Due diligence should be exercised to ensure that this vendor is keeping up to date with industry best practices for security and data protection, and that their privacy policies are still satisfactory after the CentralSquare merger. We recommend ensuring that the original contracts and privacy policies have remained unchanged as a result of this merger.

---

[1] "NFPA Standard 1710." https://services.prod.iaff.org/ContentFile/Get/30541
[2] "2017 annual report - Seattle.gov." https://www.seattle.gov/Documents/Departments/Fire/FINAL%20Annual%20Report_2017.pdf
[3] "RCW 35A.92.030: Policy statement—Service ... - Access WA.gov." https://app.leg.wa.gov/rcw/default.aspx?cite=35A.92.030
[4] "Superion, TriTech, Zuercher, and Aptean's Public Sector Business to " 5 Sep. 2018, https://www.tritech.com/news/superion-tritech-zuercher-and-apteans-public-sector-business-to-form-centra

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SDOT: Acyclica

Comments

Traffic congestion is an increasingly major issue for our city. Seattle is the fastest-growing major city in the US this decade, at 18.7% growth, or 114,00 new residents[5]. Seattle ranks sixth in the nation for traffic congestion[6]. The need for intelligent traffic shaping and development has never been greater. Acyclica, a service provided by Western Systems and now owned by FLIR[7], is an implementation of surveillance technology specifically designed to address this problem.

We were happy to see the 2015 independent audit of Acyclica's systems [SIR 8.2]. This is an excellent industry best practice, and one that we'll be recommending to other departments throughout this document.

In addition, we are pleased to see the hashing function's salt value rotated every 24-hours [SIR 4.10]. This ensures that even the 10-year retention policy [SIR 5.2] cannot be abused to correlate multiple commute sessions and individually identify a person.

Recommendations

- FLIR Systems' acquisition of Acyclica is a recent development (September 2018). We recommend verifying that the Western Systems terms [SIR 3.1] still apply. If they have been superseded by new terms from FLIR Systems, those should be subject to an audit by SDOT and Seattle IT. Specifically, section 2.5.1 of Western Systems' terms must still apply:

  > 2.5.1. It is the understanding of the City that the data gathered are encrypted to fully eliminate the possibility of identifying individuals or vehicles. In no event shall City or Western Systems and its subcontractors make any use of the data gathered by the devices for any purpose that would identify the individuals or vehicles included in the data.

- FLIR Systems is known primarily as an infrared technology vendor. Special care should be taken if FLIR/Acyclica attempt to couple IR scanning with WiFi/MAC sniffing. Implementation of an IR system would necessitate a new public surveillance review.

---

[5] "114,000 more people: Seattle now decade's fastest-growing big city in ...." 24 May. 2018, https://www.seattletimes.com/seattle-news/data/114000-more-people-seattle-now-this-decades-fastest-growing-big-city-in-all-of-united-states/
[6] "INRIX Global Traffic Scorecard." http://inrix.com/scorecard/
[7] "FLIR Systems Acquires Acyclica | FLIR Systems, Inc.." 11 Sep. 2018, http://investors.flir.com/news-releases/news-release-details/flir-systems-acquires-acyclica

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SCL: Binoculars, Check Meter, SensorLink

Comments

As these three technologies are serving the same team and mission objectives, we will review them here in a combined section.

The mission of the Current Diversion Team (CDT) is to investigate and gather evidence of illegal activity related to the redirection and consumption of electricity without paying for its use. As such, none of these technologies surveil the public at large. They instead target specific locations and equipment, albeit without the associated customer's knowledge.

It appears as though all data collected through the Check Meter Device and SensorLink Amp Fork are done without relying on a third-party service, so the usual scrutiny of a vendor's privacy policies does not apply.

Recommendations

- **Binoculars**: We have no recommendations for the use of binoculars.
- **Check Meter Device & SensorLink Amp Fork**: As noted in the comments above, we have no further recommendations for the use of the Check Meter Device and SensorLink Amp Fork technologies.
- **Racial Equity**: As with any city-wide monitoring practice, it can be easy to more closely scrutinize one neighborhood over another. Current diversion may be equally illegal (and equally prevalent) across the city, but the enforcement of this law may be unevenly applied. This could introduce racial bias by disproportionately burdening specific neighborhoods with a higher level of surveillance.

  As described, DPP 500 P III-416 section 5.2[8] asserts that all customers shall receive uniform consideration [SIR RET 1.7]. To ensure this policy is respected, we encourage City Light to track and routinely review the neighborhoods where CDT performs investigations, with a specific emphasis on racial equity. This information should be made publicly available.

  When asked at the February 27th Surveillance Technology public meeting, SDOT indicated that no tracking is currently being done on where current diversion is enforced.

[8] "SCL DPP 500 P III-416 Current Diversion - Seattle.gov." 11 Jan. 2012, http://www.seattle.gov/light/policies/docs/III-416%20Current%20Diversion.pdf

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: 911 Logging Recorder

Comments

This is a technology that the general public would likely already assume is in place. Some of the more sensational 911 call logs have been, for example, played routinely on the news around the country. Since it would not alarm the public to know that 911 call recording is taking place, our recommendations will focus primarily on data use, retention, and access control.

Call logging services are provided by NICE Ltd., an Israeli company founded in 1986. This vendor has had a troubling history with data breaches. For example, a severe vulnerability discovered in 2014 allowed unauthorized users full access to a NICE customer's databases and audio recordings[9]. Again, in 2017, a NICE-owned server was set up with public permissions, exposing phone numbers, names, and PINs of 6 million Verizon customers[10].

Recommendations

- SIR Appendix K includes a CJIS audit performed in 2017. SIR section 4.10 also mentions that ITD (Seattle IT) periodically performs routine monitoring of the SPD systems.

  However, given the problematic history with the quality of the technology vendor, if any of the NICE servers, networks, or applications were installed by the vendor (or installation was overseen/advised by the vendor), we recommend an external audit of the implementation of the call logging technology.

- SIR sections 3.3 and 4.2 outline the SPD-mandated access control and data retention policies, however it is not apparent if there is a policy that strictly locks down the use of this technology to a well-defined list of allowed cases. We recommend formally documenting the allowed 911 Logging use cases, and creating a new SIR for any new desired applications of this technology.

  With a 90-day retention policy [SIR 4.2], and with SPD receiving 900,000 calls per year[11], there are about 220,000 audio recordings existing at any given time. This is enough for a data mining, machine learning, or voice recognition project.

---

[9] "Backdoor in Call Monitoring, Surveillance Gear — Krebs on Security." 28 May. 2014, https://krebsonsecurity.com/2014/05/backdoor-in-call-monitoring-surveillance-gear/
[10] "Nice Systems exposes 14 million Verizon customers on open AWS ...." 12 Jul. 2017, https://www.techspot.com/news/70106-nice-systems-exposes-14-million-verizon-customers-open.html
[11] "9-1-1 Center - Police | seattle.gov." https://www.seattle.gov/police/about-us/about-policing/9-1-1-center

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: Computer-Aided Dispatch (CAD)

Comments

As mentioned in the section "SFD: Computer-Aided Dispatch (CAD)" and the section "SPD: 911 Logging Recorder", these dispatch technologies are mandatory for functional emergency services of a city this size. No other system would be able to meet the federal- and state-mandated response times and reporting requirements.

SIR section 4.10 mentions that ITD (Seattle IT) performs routine inspections of the Versaterm implementation.

Versaterm, founded in 1977, provides the technology used by SPD's CAD system. SPD purchased this technology in 2004. In September of 2016, there was a legal dispute between Versaterm and the City of Seattle over a Public Records Act (PRA) disclosure of certain training and operating manuals[12]. The court ruled in favor of Versaterm.

Recommendations

- It is not immediately clear what use cases are described in SIR 2.5 describing data access by "other civilian staff whose business needs require access to this data". All partnerships and data flows between SPD and businesses should be explicitly disclosed.

- This system has been in place for 15 years. As with any technology, advancements in security, speed, usefulness, and reliability come swiftly. Due to the age of the technology, and the potential damaged relationship between Seattle and Versaterm due to the aforementioned legal dispute, we recommend conducting a survey into the plausibility of replacing Versaterm as SPD's CAD solution.

- As mentioned in the introduction to this document, Seattle has adopted the Welcoming Cities Resolution[13]. In honoring this resolution, we recommend that SPD never disclose identifying information, from CAD or any system, to Immigrations and Customs Enforcement (ICE) without a criminal warrant.

---

[12] "Versaterm Inc. v. City of Seattle, CASE NO. C16-1217JLR | Casetext." 13 Sep. 2016, https://casetext.com/case/versaterm-inc-v-city-of-seattle-2
[13] "Welcoming Cities Resolution - Council | seattle.gov." http://www.seattle.gov/council/issues/past-issues/welcoming-cities-resolution

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: CopLogic

Comments

Track 1 - Public reporting of no-suspect, no-evidence, non-emergency crimes

CTAB understands that in cases where no evidence or suspect is available, a crime should be reported (for statistical or insurance purposes) but does not require the physical appearance of an SPD officer.

Track 2 - Retail Loss Prevention

This track is more problematic, as it could be used by retailers as a method to unreasonably detain, intimidate, or invade the privacy of a member of the public accused of, but not proven guilty of, shoplifting.

Recommendations

- **Track 2**: If not already done, retailers should be trained and informed that having a CopLogic login does not allow them to act as if they are law enforcement officers. Members of the public suspected of shoplifting need to have an accurate description of their rights in order to make informed decisions before providing identifying information. Retailers are also held to a lower standard than SPD regarding racial bias. It is virtually guaranteed that people of color are disproportionately apprehended and entered into the retail track of CopLogic.

  We recommend discontinuing Track 2 entirely.

- **Track 1 & 2**: If not already done, SPD, in coordination with Seattle IT, should perform or hire a company to perform an audit of the vendor's systems. If this audit has not been performed in the 8 years since purchasing this system, it should absolutely be done before the 10-year mark in 2020.
- **Track 1 & 2**: It is not immediately clear in the SIR or LexisNexis's Privacy Policy what CopLogic does with these records long-term, after SPD has imported them into their on-premises system. A written statement from LexisNexis on how this data is used, mined, or sold to affiliates/partners should be acquired by SPD.
- **Track 1 & 2**: We recommend migrating CopLogic to an on-premises solution. We found the LexisNexis privacy policy to be obfuscated and vague[14]. Such sensitive information should not be protected by trust alone.

[14] "Privacy Policy | LexisNexis." 7 May. 2018, https://www.lexisnexis.com/en-us/terms/privacy-policy.page

City of Seattle

March 20, 2019

RE: ACLU-WA Comments Regarding Group 2 Surveillance Technologies

Dear Seattle IT:

On behalf of the ACLU of Washington, I write to offer our comments on the surveillance technologies included in Group 2 of the Seattle Surveillance Ordinance process. We are submitting these comments by mail and electronically because they do not conform to the specific format of the online comment form provided on the CTO's website, and because the technologies form groups in which some comments apply to multiple technologies.

These comments should be considered preliminary, given that the Surveillance Impact Reports (SIR) for each technology leave a number of significant questions unanswered. Specific unanswered questions for each technology are noted in the comments relating to that technology, and it is our hope that those questions will be answered in the updated SIR provided to the Community Surveillance Working Group and to the City Council prior to their review of that technology. In addition to the SIR, our comments are also based on independent research relating to the technology at hand.

The 8 technologies in Group 2 are covered in the following order.

I. Acyclica (SDOT)

II. CopLogic (SPD)

III. Computer-Aided Dispatch & 911 Logging Recorder Group

1. Computer-Aided Dispatch (SPD)
2. Computer-Aided Dispatch (SFD)
3. 911 Logging Recorder (SPD)

IV. Current Diversion Technology Group

1. Check Meter Device (Seattle City Light)
2. SensorLink Amp Fork (Seattle City Light)
3. Binoculars/Spotting Scope (Seattle City Light)

ACLU
AMERICAN CIVIL LIBERTIES UNION
Washington

901 Fifth Ave, Suite #630
Seattle, WA 98164
(206) 624-2184
aclu-wa.org

Tana Lin
Board President

Michele Storms
Executive Director

Shankar Narayan
Technology & Liberty Project Director

I. Acyclica - SDOT

Background

Acyclica technology is a powerful location-tracking technology that raises a number of civil liberties concerns because of its ability to uniquely identify individuals and their daily movements. Acyclica (via its hardware vendor, Western Systems), manufactures Intelligent Transportation System (ITS) sensors called RoadTrend that are used by the Seattle Department of Transportation for the stated purpose of traffic management. These RoadTrend sensors collect encrypted media access control (MAC) addresses, which are transmitted by any Wi-Fi enabled device including phones, cameras, laptops, and vehicles. Collection of MAC addresses, even when hashed (a method of de-identifying data irreversibly),[1] can present locational privacy challenges.

Experts analyzing a dataset of 1.5 million individuals found that just knowing four points of approximate spaces and times that individuals were near cell antennas or made a call were enough to uniquely identify 95% of individuals.[2] In the case of Acyclica's operation in Seattle, the dataset is comprised of MAC addresses recorded on at least 301 intersections,[3] which allows Acyclica to generate even more precise location information about individuals. Not only do the RoadTrend sensors pick up the MAC addresses of vehicle drivers and riders, but these sensors can also pick up the MAC addresses of all nearby individuals, including pedestrians, bicyclists, and people in close structures (e.g., apartments, offices, and hospitals). Acyclica technology's location tracking capabilities means that SDOT's use of Acyclica can not only uniquely identify individuals with ease, but can also create a detailed map of their movements. This raises privacy concerns for Seattle residents, who may be tracked without their consent by this technology while going about their daily lives.

These location-tracking concerns are exacerbated by the lack of clarity around whether SDOT has a contract with Acyclica (see below). Without a contract, data ownership and scope of data sharing and repurposing by Acyclica is unclear. For example, without contractual restrictions, Acyclica

[1] Hashing is a one-way function that scrambles plain text to produce a unique message digest. Unlike encryption—which is a two-way function, allowing for decryption—what is hashed cannot be un-hashed. However, hashed location data can still be used to uniquely identify individuals. While it is infeasible to compute an input given only its hash output, pre-computing a table of hashes is possible. These types of tables consisting of pre-computed hashes and their inputs are called rainbow tables. With a rainbow table, if an entity has a hash, then they only need to look up that hash in their table to then know what the original MAC address was.
[2] Montjoye, Y., Hidalgo, C., Verleysen, M., and Blondel, V. 2013. Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports.* 3:1375.
[3] The SIR states that SDOT has 301 Acyclica units installed throughout the City. However, an attached location excel sheet in Section 2.1 lists 389 Acyclica units, but only specifies 300 locations.

would be able to share the raw data (i.e., the non-aggregated, hashed data before it is summarized and sent to SDOT) with any third parties, and these third parties would be able to use the data in any way they see fit, including combining the data with additional data such as license plate reader or facial recognition data. Acyclica could also share the data with law enforcement agencies that may repurpose the data, as has happened with other City data. For example, in 2018, U.S. Immigration and Customs Enforcement (ICE) approached Seattle City Light with an administrative subpoena demanding information on a particular customer location, including phone numbers and information on related accounts.[4] ICE also now has agency-wide access to a nationwide network of license plate readers controlled by Vigilant Solutions,[5] indicating the agency may seek additional location data for immigration enforcement purposes in the future. Data collected via Acyclica should never be used for law enforcement purposes.

The uncertainty around the presence or absence of a contract contributes to two key issues: (1) lack of a clearly defined purpose of use of Acyclica technology; and (2) lack of clear restrictions on the use of Acyclica technology that track that purpose. With no contract, SDOT cannot enforce policies restricting the use of Acyclica technology to the intended purpose.

There are also a number of contradictory statements in the SIR concerning the operation of Acyclica technology,[6] as well as discrepancies between the SIR, the information shared at the technology fair (the first public meeting to discuss the Group 2 technologies),[7] and ACLU-WA's conversation with the President of Acyclica, Daniel Benhammou. All these leave us with concerns over whether SDOT fully understands (and the SIR reflects) the capabilities of the technology. In addition, there remain a number of critical unanswered questions that the final SIR must address (set forth below).

Of additional concern is the recent acquisition of Acyclica by FLIR Systems, an infrared and thermal imaging company funded by the U.S. Department of Defense.[8] As of March 2019, FLIR has discontinued Acyclica RoadTrend sensors.[9] Neither the implications of the FLIR acquisition nor the discontinuation of the RoadTrend sensors are mentioned in the SIR—but if the sensors used will change, the SIR should make clear how that will impact the technology.

a. Specific Concerns

- *Inadequate Policies Defining Purpose of Use.* Policies cited in the SIR are vague,

[4] https://crosscut.com/2018/02/immigration-officials-subpoena-city-light-customer-info
[5] https://www.theverge.com/2018/3/1/17067188/ice-license-plate-data-california-vigilant-solutions-alpr-sanctuary
[6] Explained in further detail in 1. Acyclica – SDOT *Major Concerns* below.
[7] http://www.seattle.gov/tech/initiatives/privacy/events-calendar#/?i=3
[8] https://www.crunchbase.com/acquisition/flir-systems-acquires-acyclica--e6043a1a#section-overview
[9] https://www.flir.com/support/products/roadtrend#Specifications

short, and impose no meaningful restrictions on the purposes for which Acyclica devices may be used.[10] Section 1.1 of the abstract set forth in the SIR states that Acyclica is used by over 50 agencies to "to help to monitor and improve traffic congestion." Section 2.1 is similarly vague, providing what appear to be examples of some types of information the technology produces (e.g., calculated average speeds) in order to facilitate outcomes (correcting traffic signal timing, providing information to travelers about expected delays, and allowing SDOT to meet traffic records and reporting requirements)—but it's not clear this list is exhaustive. Section 2.1 fails to describe the purpose of use, all the types of information Acyclica provides, and all the types of work that Acyclica technology facilitates. All these must be clarified.

- *Lack of Clarity on Whether Acyclica and SDOT have a Written Contract.* The SIR does not state that any contract exists, and in the 2018 conversation ACLU-WA had with Benhammou, he stated that there was no contract between the two parties. However, at the 2019 technology fair, the SDOT representative affirmatively stated that SDOT has a contract with Acyclica. As previously mentioned, the lack of a contract limits SDOT's ability to restrict the scope of data sharing and repurposing. The only contractual document provided appears to be a terms sheet in Section 3.0 detailing SDOT's terms of service with Western Systems (the hardware vendor that manufactures the Acyclica RoadTrend sensors), which states that Western Systems only deals with the maintenance and replacement of the hardware used to gather the data, and not the data itself.

- *Lack of Clarity on Data Ownership.* At the technology fair, the SDOT representative stated that SDOT owns all the data collected (including the raw data), but the SIR only states that the aggregated traffic data is owned by SDOT. In the 2018 conversation, Benhammou stated that Acyclica owns all the raw data. There is an apparent lack of clarity between SDOT and Acyclica concerning ownership of data that must be addressed.

- *Data Retention Periods are Unclear.* Section 5.2 of the SIR states that there is a 10-year internal deletion requirement for the aggregated traffic data owned by SDOT, but pg. 37 of the SIR states that "the data is deleted within 24 hours to prevent tracking devices over time." In the 2018 interview, Benhammou stated that Acyclica retains all non-aggregated data indefinitely. It is unclear whether the different retention periods stated in the SIR are referring to different types of data. The lack of clarity on data retention periods also relates to the lack of clarity on data ownership given that data retention periods may depend on data ownership.

[10] As noted in 1. Acyclica – SDOT *Background* above.

- *Inaccurate Descriptions of Anonymization/Data Security Practices.* The SIR appears to use the terms "encryption" and "hashing" interchangeably in some parts of the SIR, making it difficult to clearly understand Acyclica's practices in this area. For example, Section 7.2 states: "Contractually, Acyclica guarantees that the data gathered is encrypted to fully eliminate the possibility of identifying individuals or vehicles." But by design, encryption allows for decryption with a key, meaning anyone with that key and access to the data can identify individuals. (Also, if there is no contract between SDOT and Acyclica, the use of 'contractually' is misleading). This language is also used in the terms sheet detailing SDOT's contract with Western Systems (in Section 2.5.1 in the embedded contract). The SIR compounds this confusion with additional contradictory statements. For example, the SIR states in multiple sections that the data collected by the RoadTrend sensors are encrypted and hashed on the actual sensor. However, according to a letter from Benhammou provided by SDOT representatives at the technology fair,[11] the data is never hashed on the sensor—the data is only hashed after being transmitted to Acyclica's cloud server. These contradictory descriptions cause concern.

- *No Restrictions on Non-City Data Use.* Section 6.3 of the SIR states that there are no restrictions on non-City data use. However, there are no policies cited making clear the criteria for such use, any inter-agency agreements governing sharing of Acyclica data with non-City parties, or why the data must be shared in the first place.

- *Not All Locations of Acyclica Devices are Specified.* Section 2.1 of the SIR states that there are 301 Acyclica locations in Seattle. However, in the embedded excel sheet detailing the serial numbers and specific intersections in which Acyclica devices are installed, there are 389 serial numbers, but only 300 addresses/locations specified. The total number and the locations of Acyclica devices collecting data in Seattle is unclear. This gives rise to the concern that there are unspecified locations in which Acyclica devices are collecting MAC addresses.

- *No Mention of RoadTrend Sensor Discontinuation.* As noted in the background,[12] Acyclica has been acquired by FLIR, an infrared and thermal imaging company. As of March 2019, FLIR's product webpage states that the Acyclica RoadTrend sensors (those currently used by SDOT) have been discontinued.[13] From the information we have, it is unclear if SDOT will be able to continue using the RoadTrend sensors described in the 2019 SIR. Given that FLIR sensors, such as the TrafiOne, have capabilities that go much farther than those of the

[11] Included in Appendix 1.
[12] As noted in 1. Acyclica – SDOT *Background* above.
[13] https://www.flir.com/support/products/roadtrend#Specifications

RoadTrend sensors (e.g., camera technology and thermal imaging)[14] as well as potentially different technical implementations, their use would give rise to even more serious privacy and misuse concerns. Neither the implications of the FLIR acquisition nor the discontinuation of the RoadTrend sensors are mentioned in the SIR.

- *No Mention of Protecting MAC Addresses of Non-Drivers/Riders (e.g., people in nearby buildings).* The Acyclica sensors will pick up the MAC addresses of all nearby individuals, regardless of whether they are or are not driving or riding in a vehicle. The SIR does not mention any steps taken to reduce the privacy infringements on non-drivers/riders.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- For what specific purpose or purposes will Acyclica be used, and what policies state this?
- Does SDOT have a contract with Acyclica, and if so, why is the contract not included in the SIR?
- Who owns the raw, non-aggregated data collected by Acyclica devices?
- What is the retention period for the different types of collected data (aggregated and non-aggregated)—for both SDOT and Acyclica?
- Provide accurate descriptions of Acyclica's data security practices, including encryption and hashing, consistent with the letter from Daniel Benhammou, including any additional practices that prevent reidentification.
- What third parties will access Acyclica's data, for what purpose, and under what conditions?
- Why are 89 locations not specified in the embedded Acyclica locations sheet in Section 2.1 of the SIR?
- Will SDOT continue to use Acyclica RoadTrend Sensors, and for how long? If SDOT plans to switch to other sensors, which ones, and how do their capabilities differ from the RoadTrend Sensors?
- Did SDOT consider any other alternatives when deciding to acquire Acyclica? Did SDOT consider other, more privacy protective traffic management tools in use (for example, inductive-loop detectors currently used by the Washington State Department of Transportation and the US

[14] https://www.flir.com/support/products/trafione#Resources

Department of Transportation)?[15]

- How does SDOT plan to reduce the privacy infringements on non-drivers/riders?

c. Recommendations for Regulation:

At this stage, pending answers to the questions set forth above, we can make only preliminary recommendations for regulation of Acyclica. We recommend that the Council adopt, via ordinance, clear and enforceable rules that ensure, at a minimum, the following:

- There must be a binding contract between SDOT and Acyclica.
- The contract between SDOT and Acyclica must include the following minimum provisions:
  - A data retention period of 12 hours or less for any data Acyclica collects, within which time Acyclica must aggregate the data, submit it to SDOT, and delete both non-aggregated and aggregated data.
  - SDOT receives only aggregated data.
  - SDOT owns all data, not Acyclica.
  - Acyclica cannot share the data collected with any other entity besides SDOT for any purpose.
- The ordinance must define a specific purpose of use for Acyclica technology, and all use of the tool and its data must be restricted to that purpose. For example: Acyclica may only be used for traffic management purposes, defined as activities concerning calculating average travel times, regulating traffic signals, controlling traffic disruptions, determining the placement of barricades or signals for the duration of road incidents impeding normal traffic flow, providing information to travelers about traffic flow and expected delays, and allowing SDOT to meet traffic records and reporting requirements.
- SDOT must produce an annual report detailing its use of Acyclica, including details how SDOT used the data collected, the amount of data collected, and for how long it was retained and in what form.

II. CopLogic – SPD

[15] https://www.fhwa.dot.gov/publications/research/operations/its/06108/03.cfm

Background

CopLogic (LexisNexis's Desk Officer Reporting System-DORS)[16] is a technology owned by LexisNexis and used by the Seattle Police Department to allow members of the public and retailers to submit online police reports regarding non-emergency crimes. Members of the public and retailers can submit these reports through an online portal they can access via their phone, tablet, or computer. Community members can report non-emergency crimes that have occurred within the Seattle city limits, and retail businesses that participate in SPD's Retail Theft Program may report low-level thefts that occur in their businesses when they have identified a suspect. This technology is used by SPD for the stated purpose of freeing up resources in the 9-1-1 Center, reducing the need for a police officer to be dispatched for the sole purpose of taking a police report.

This technology gives rise to potential civil liberties concerns because it allows for the collection of information about community members, unrelated to a specific incident, and without any systematic method to verify accuracy or correct inaccurate information. In addition, there is lack of clarity surrounding data retention and data sharing by LexisNexis, and around how CopLogic data will be integrated into SPD's Records Management System.

a. Concerns

- *Lack of Clarity on CopLogic/LexisNexis Data Collection and Retention.* There is no information in the SIR or in the contract between SPD and LexisNexis detailing the data retention period by LexisNexis (Section 5.2 of the SIR). This lack of clarity stems in part from an unclear description of what's provided by LexisNexis—it's described as an online portal, but the SIR and the contract provided appears to contemplate in Section 4.8 that LexisNexis will indeed access and store collected data. If true, the nature of that access should be clarified, and data restrictions including clear access limitations and retention periods should accordingly be put in place. Once reports are transferred over to SPD's Records Management System (RMS), the reports should be deleted by CopLogic/LexisNexis.

- *Lack of Clarity on LexisNexis Data Sharing with Other Agencies or Third Parties.* If LexisNexis does access and store data, it should do so only for purposes of fulfilling the contract, and should not share that data with third parties. But the contract between SPD and LexisNexis does not make clear whether LexisNexis is prohibited entirely from sharing data with other entities (it does contain a restriction on "transmit[ting]" the data, but without reference to third parties.

[16] https://risk.lexisnexis.com/products/desk-officer-reporting-system

- *No Way to Correct Inaccurate Information Collected About Community Members.* Community members or retailers may enter personally-identifying information about third parties without providing notice to those individuals, and there is no immediate, systematic method to verify the accuracy of information that individuals provide about third parties. There are also no stated measures in the SIR to destroy improperly collected data.

- *Lack of clarity on how the CopLogic data will be integrated with and analyzed within SPD's RMS.* At the technology fair, SPD stated that completed complaints will go into Mark43[17] when it is implemented. ACLU-WA has previously raised concerns about the Mark43 system, and it should be made clear how CopLogic data will enter that system, including to what third parties it will be made available.[18]

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What data does LexisNexis collect and store via CopLogic? What are LexisNexis's data retention policies for CopLogic data?

- Are there specific policies restricting LexisNexis from sharing CopLogic data with third parties? If so, what are they?

- Is there any way to verify or correct inaccurate information collected about community members?

- How will CopLogic data be integrated with Mark43?

c. Recommendations for Regulation:

Pending answers to the questions set forth above, we can make only preliminary recommendations for regulation of CopLogic. SPD should adopt clear and enforceable policies that ensure, at a minimum, the following:

- After CopLogic data is transferred to SPD's RMS, LexisNexis must delete all CopLogic data.

- LexisNexis is prohibited from using CopLogic data for any purpose other than those set forth in the contract, and from sharing CopLogic data with third parties.

[17] https://www.aclu-wa.org/docs/aclu-letter-king-county-council-regarding-mark-43
[18] A Records Management System (RMS) is the management of records for an organization throughout the records-life cycle. New RMSs (e.g., Mark43) may have capabilities that allow for law enforcement agencies to track and analyze the behavior of specific groups of people, leading to concerns of bias in big data policing, particularly for communities of color.

- Methods are available to the public to correct inaccurate information entered in the CopLogic portal.
- Measures are implemented to delete improperly collected data.

III. Computer-Aided Dispatch & 911 Logging Recorder Group

Overall, concerns around the Computer-Aided Dispatch (CAD) and 911 Logging Recorder technologies focus on use of the technologies and/or collected data them for purposes other than those intended, over-retention of data, and sharing of that data with third parties (such as federal law enforcement agencies). Therefore, for all of these technologies as appropriate, we recommend that the responsible agency should adopt clear and enforceable rules that ensure, at a minimum, the following:

- The purpose of use must be clearly defined, and its operation and data collected must be explicitly restricted to that purpose only.
- Data retention must be limited to the time needed to effectuate the purpose defined.
- Data sharing with third parties, if any, must be limited to those held to the same restrictions.
- Clear policies must govern operation, and all operators should be trained in those policies.

Specific comments follow:

1. Computer-Aided Dispatch – SPD

Background

CAD is a software package (made by Versaterm) utilized by the Seattle Police Department's 9-1-1 Center that consists of a set of servers and software deployed on dedicated terminals in the 9-1-1 center, in SPD computers, and as an application on patrol vehicles' mobile data computers and on some officers' smart phones. The stated purpose of CAD is to assist 9-1-1 Center call takers and dispatchers with receiving requests for police services, collecting information from callers, and providing dispatchers with real-time patrol unit availability. Concerns include lack of clarity surrounding data retention and data sharing with third parties.

a. Concerns:

- *Lack of clarity on data retention within CAD v. RMS.* While the SIR makes clear that at some point, CAD data is transferred to SPD's RMS, it is unclear what data, if any, the CAD system itself retains and for how long. If the CAD system does retain some data (for example, call logs)

independent of the RMS, and that data is accessible to the vendor, appropriate data protections should be put in place. But because the SIR usually references "data collected by CAD," it is unclear where that data resides.

- *Lack of a policy defining purpose of the technology and limiting its use to that purpose*: Unlike SFD's similar system, SPD appears to have no specific policy defining the purpose of use for CAD and limiting its use to that purpose.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- Does the CAD system itself store data? If so, what data and for how long? Who can access that data?

c. Recommendations for Regulation:

Depending on the answer to the question above, appropriate data protections may be needed as described above. In addition, SPD should adopt a policy similar to SFD's, clearly defining purpose and limiting use of the tool to that purpose.

2. Computer-Aided Dispatch – SFD

Background

Computer Aided Dispatch (CAD) is a suite of software packages used by SFD and made by Tritech that provide unit recommendations for 911 emergency calls based on the reported problem and location of a caller. The stated purpose of CAD is to allow SFD to manage emergency and non-emergency call taking and dispatching operations. The technology allows SFD to quickly enable personnel to execute rapid aid deployment.

Generally and positively, SFD clearly defines the purpose of use, restricts CAD operation and data collection to that purpose only, limits sharing with third parties, and specifies policies on operation and training. However, SFD must clarify what data is retained within CAD, data retention policies, and provide information about its data sharing partners.

d. Concerns

- *Lack of clarity on data retention within CAD*. It is unclear what data, if any, the CAD system itself retains and for how long. If the CAD system does retain some data (for example, call logs) and that data is accessible to the vendor, appropriate data protections should be put in place.
- *Lack of clarity on data retention policies*. At the technology fair, we learned that CAD data is retained indefinitely. It is not clear what justifies indefinite retention of this data.

- *Lack of clarity on data sharing partners.* In Section 6.3 of the SIR, SFD states that in rare case where CAD data is shared with partners other than those specifically named in the SIR, a third-party nondisclosure agreement is signed. However, there are no examples or details of who those partners are and the purposes for which CAD data would be shared.

e. Outstanding Questions That Must be Addressed in the Final SIR:

- Does the CAD system itself store data? If so, what data and for how long? Who can access that data?
- Who are SFD's data sharing partners? For what purpose is data shared with them?

f. Recommendations for Regulation:

Depending on the answer to the question regarding if the CAD system itself stores data, appropriate data protections may be needed as described above. SFD should adopt a clear policy requiring deletion of CAD data no longer needed. In addition, depending on how data is shared, SFD should adopt a policy that clearly limits what for what purposes CAD data would be shared, and with what entities.

3. 911 Logging Recorder – SPD

Background

The NICE 911 logging recorder is a technology used by SPD to audio-record all telephone calls to SPD's 9-1-1 communications center and all radio traffic between dispatchers and patrol officers. The stated purpose of the 9-1-1 Logging Recorder is to allow SPD to provide evidence to officers and detectives who investigate crimes and the prosecutors who prosecute offenders. These recordings also provide transparency and accountability for SPD, as they record in real time the interactions between 9-1-1 call takers and callers, and the radio traffic between 9-1-1 dispatchers and police officers. The NICE system also supports the 9-1-1 center's mission of quickly determining the nature of the call and getting the caller the assistance they need as quickly as possible with high quality, consistent and professional services.

Concerns include lack of clarity surrounding data retention schedules and data sharing with third parties.

a. Concerns

- *Lack of clarity on data retention.* Section 4.2 of the SIR states: "Recordings

requested for law enforcement and public disclosure are downloaded and maintained for the retention period related to the incident type." Similar to other technologies noted above, it is unclear whether the 9-1-1 system itself stores these recordings, or if they are stored on SPD's RMS. If the former, it should be made clear how the technology vendor accesses these recordings and for what purpose, if at all.

- *More clarity needed on data sharing with third parties.* There are no details or examples of the "discrete pieces of data" that are shared outside entities and individuals as referenced in Section 6.0 of the SIR.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What is SPD's data retention schedule for data stored in the NICE system, if any?
- What "discrete pieces of data" does SPD share with third parties?

c. Recommendations for Regulation:

SPD should adopt a clear policy requiring deletion of data no longer needed. In addition, depending on how data is shared, SPD should adopt a policy that clearly limits what for what purposes data would be shared, and with what entities.

IV. Current Diversion Technology Group – Seattle City Light

The technologies in this group—the Check Meter device (SensorLink TMS), the SensorLink Amp Fork, and the Binoculars/Spotting Scope raise civil liberties concerns primarily due to lack of explicit, written policies imposing meaningful restrictions on use of the technologies. While the purpose of the current diversion technologies appears clear—to assess whether suspected diversions of current have occurred and/or are continuing to occur—there are no explicit policies in the SIR detailing restrictions on what can and cannot be recorded by these technologies.

Below are short descriptions of the technologies, followed by concerns and recommendations.

Background

1. Check Meter Device (SensorLink TMS)

The SensorLink TMS device measures the amount of City Light-provided electrical energy flowing through the service-drop wire over time, digitally capturing the instantaneous information on the device for later retrieval by the Current Diversion Team via the use of a secure wireless protocol.

The stated purpose of use is to allow Seattle City Light to maintain the integrity of its electricity distribution system, to determine whether suspected current diversions have taken place, and to provide the valuation of the diverted energy to proper authorities for cost recovery.

2. SensorLink Amp Fork

The SensorLink Amp Fork is an electrical device mounted on an extensible pole allowing a circular clamp to be placed around the service-drop wire that provides electrical service to a customer location via its City Light-provided meter. The device then displays instantaneous readings of the amount of electrical energy (measured in amperage, or "amps") that the Current Diversion Team may compare against the readings displayed on the meter, allowing them to determine if current is presently being diverted.

The stated purpose of use of the Amp Fork is to allow Seattle City Light to assess whether suspected diversions of current have occurred and/or are continuing to occur. The Amp Fork allows the Utility to determine the valuation of the energy illegally diverted, which supports City Light's mission of recovering this value for ratepayers via a process called "back-billing."

3. Binoculars/Spotting Scope

The binoculars are standard, commercial-grade, unpowered binoculars. They do not contain any special enhancements requiring power (e.g., night-vision or video-recording capabilities). They are used to read a meter from a distance when the Current Diversion Team is otherwise unable to access physically the meter for the purpose of inspection upon suspected current diversion.

The stated purpose of the binoculars is to allow Seattle City Light to inspect meters and other implicated electrical infrastructure at a distance. If a determination of diversion is sustained, data may be used to respond to lawful requests from the proper law enforcement authorities for evidence for recovering the value of the diverted energy.

a. Concerns Regarding all Three Current Diversion Technologies

- *Absence of explicit, written policies imposing meaningful restrictions on use.* At the technology fair, a Seattle City Light representative stated that these technologies are used only for the purpose of checking current diversions, but could not confirm that Seattle City Light had clear, written policies for what data could and could not be recorded (e.g., an employee using the binoculars to view non-meter related information). The absence of written, specific policies increases the risk of unwarranted surveillance of individuals. There is also no mention in the SIRs of

specific data protection policies in place to safeguard the data (e.g., encryption, hashing, etc.).

- *Seattle City Light's records retention schedule is mentioned in the SIRs, but details about it are omitted.* It is unclear how long Seattle City Light retains data collected, and for what reason.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What enforceable policies, if any, apply to use of these three technologies?
- What is Seattle City Light's data retention schedule?

c. Recommendations for Regulation:

Seattle City Light must create clear, enforceable policies that, at a minimum:

- Define purpose of use for each technology and restrict its use to that purpose.
- Clearly state what clear data protection policies exist to safeguard stored data, if any, and ensure the deletion of data collected by the technology immediately after the relevant current diversion investigation has closed.

Thank you for your consideration, and please don't hesitate to contact me with questions.

Best,

Shankar Narayan
Technology and Liberty Project Director

Jennifer Lee
Technology and Liberty Project Advocate

Appendix 1: Benhammou Letter

16

City of Seattle

Acyclica

February 6th, 2015

RE: Acyclica data privacy standards

To whom it may concern:

The purpose of this letter is to provide information regarding the data privacy standards maintained by Acyclica. Acyclica is a traffic information company specializing in traffic congestion information management and analysis. Among the various types of data sources which make of Acyclica's traffic data portfolio including GPS probe data, video detection and inductive loops, Acyclica also utilizes our own patent-pending technology for the collection of Bluetooth and Wifi MAC addresses. MAC or Media Access Control addresses are unique 48-bit numbers which are associated with devices with Bluetooth and/or Wifi capable devices.

While MAC addresses themselves are inherently anonymous, Acyclica goes to great lengths to further obfuscate the original source of data through a combination of hashing and encryption to all but guarantee that information derived from the initial data bears no trace of any individual.

Acyclica's technology for collecting MAC addresses for congestion measurement operates by detecting nearby MAC addresses. The MAC addresses are then encrypted using GPG encryption before being transmitted to the cloud for processing. Encrypting the data prior to transmission means that no MAC addresses are ever written where they can be retrieved from the hardware. Once the data is received by our servers, the data is further anonymized using a SHA-256 algorithm which makes the raw MAC address nearly impossible to decipher from the hashed output. Furthermore, any customer seeking to download data for further investigation or integration through our API can only ever view the hashed MAC address.

Acyclica occasionally provides data to partners to help enhance the quality of congestion information. The information which is provided to such partners is received through API calls which only return aggregated information about traffic data over a given period such as the average travel-time over a 5-minute period. Aggregating the data provides a final layer of anonymization by reporting on the collective trend of all vehicles rather than the specific behavior of a single vehicle.

As always questions, comments and concerns are welcome. Please do let me know if we can provide further clarity and transparency on our internal operations with regards to data processing and privacy standards. We take the privacy of the public very seriously and always treat our customers and the data with the utmost respect.

Regards,

Daniel Benhammou
President
Acyclica Inc.

Appendix H: Comment Analysis Methodology

Overview

The approach to comment analysis includes combination of qualitative and quantitative methods. A basic qualitative text analysis of the comments received, and a subsequent comparative analysis of results, were validated against quantitative results. Each comment was analyzed in the following ways, to observe trends and confirm conclusions:

1. Analyzed collectively, as a whole, with all other comments received
2. Analyzed by technology
3. Analyzed by technology and question

A summary of findings are included in Appendix B: Public Comment Demographics and Analysis. All comments received are included in Appendix E: All Individual Comments Received.

Background on Methodological Framework

A modified Framework Methodology was used for qualitative analysis of the comments received, which "*…approaches [that] identify commonalities and differences in qualitative data, before focusing on relationships between different parts of the data, thereby seeking to draw descriptive and/or explanatory conclusions clustered around themes" (Gale, N.K., et.al, 2013).* Framework Methodology is a coding process which includes both inductive and deductive approaches to qualitative analysis.

The goal is to classify the subject data so that it can be meaningfully compared with other elements of the data and help inform decision-making. Framework Methodology is "not designed to be representative of a wider population, but purposive to capture diversity around a phenomenon" (*Gale, N.K., et.al, 2013).*

Methodology

Step One: Prepare Data

1. Compile data received.
    a. Daily collection and maintenance of 2 primary datasets.
        i. Master dataset: a record of all raw comments received, questions generated at public meetings, and demographic information collected from all methods of submission.
        ii. Comment analysis dataset: the dataset used for comment analysis that contains coded data and the qualitative codebook. The codebook contains the qualitative codes used for analysis and their definitions.
2. Clean the compiled data.
    a. Ensure data is as consistent and complete as possible. Remove special characters for machine readability and analysis.

b. Comments submitted through SurveyMonkey for "General Surveillance" remained in the "General Surveillance" category for the analysis, regardless of content of the comment. Comments on surveillance generally, generated at public meetings, were categorized as such.
c. Filter data by technology for inclusion in individual SIRs.

Step Two: Conduct Qualitative Analysis Using Framework Methodology

1. Become familiar with the structure and content of the data. This occurred daily compilation and cleaning of the data in step one.
2. Individually and collaboratively code the comments received, and identify emergent themes.
   I. Begin with deductive coding by developing pre-defined codes derived from the prescribed survey and small group facilitator questions and responses.
   II. Use clean data, as outlined in Data Cleaning section above, to inductively code comments.
      A. Each coder individually reviews the comments and independently codes them.
      B. Coders compare and discuss codes, subcodes, and broad themes that emerge.
      C. Qualitative codes are added as a new field (or series of fields) into the Comments dataset to derive greater insight into themes, and provide increased opportunity for visualizing findings.
   III. Develop the analytical framework.
      A. Coders discuss codes, sub-codes, and broad themes that emerge, until codes are agreed upon by all parties.
      B. Codes are grouped into larger categories or themes.
      C. The codes are be documented and defined in the codebook.
   IV. Apply the framework to code the remainder of the comments received.
   V. Interpret the data by identifying differences and map relationships between codes and themes, using R and Tableau.

Step Three: Conduct Quantitative Analysis

1. Identify frequency of qualitative codes for each technology overall, by questions, or by themes:
   I. Analyze results for single word codes.
   II. Analyze results for word pair codes (for context).
2. Identify the most commonly used words and word pairs (most common and least common) for all comments received.

I. Compare results with qualitative code frequencies and use to validate codes.
II. Create network graph to identify relationships and frequencies between words used in comments submitted. Use this graph to validate analysis and themes.

3. Extract CSVs of single word codes, word pair codes, and word pairs in text of the comments, as well as the corresponding frequencies for generating visualizations in Tableau.

Step Four: Summarization

1. Visualize themes and codes in Tableau. Use call out quotes to provide context and tone.
2. Included summary information and analysis in the appendices of each SIR.

Appendix I: Supporting Policy Documentation

Management Control Agreement

Management Control Agreement Between
Seattle Police Department and
City of Seattle Information Technology Department

The City of Seattle Police Department ("SPD"), also referred to as the Criminal Justice Agency, and the City of seattle Information Technology Department (''ITD") are departments of the municipal corporation of the City of Seattle.

Pursuant to Seattle Municipal Code ("SMC") 3.23, ITD provides information technology systems, services, and support to SPD and is therefore required to support, enable, enforce, and comply with SPD policy requirements, including the FBl's Criminal Justice Information Services ("CJIS") Security Policy.

Pursuant to the CJIS Security Policy, it is agreed that with respect to the administration of computer systems, network infrastructure, devices, and services interfacing directly or indirectly with A Central Computerized Enforcement System ("ACCESS") for the exchange of criminal history/criminal justice information, the Criminal Justice Agency shall have the authority, via managed control, to set and enforce:

Priorities that guarantee the priority, integrity, and availability of service needed by the criminal justice community.

Requirements for the selection, authorization, supervision, and termination of physical and logical access to Criminal Justice Information ("CJI").

Policy governing operation of justice systems, data, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a communications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.

Restriction of unauthorized physical and logical access to or use of systems and equipment accessing CJI.

Compliance with all rules and regulations of the Criminal Justice Agency policies and CJIS Security Policy in the operation of, access to, or control over any CJI systems, data, or infrastructure.

The responsibility for management control of the criminal justice function remains solely with the Criminal Justice Agency. ITD will not enter into any agreements or allow any access to, possession of, or control over any SPD CJI systems, data, or infrastructure without explicit authorization from at least one SPD Authorized Party. SPD Authorized Parties must be SPD employees and include:
Chief of Police
Chief Operating Officer

This agreement covers the overall supervision of all Criminal Justice Agency systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, administration, and maintenance of any Criminal Justice Agency system to include NCIC Programs that may be subsequently designed and/or implemented within the Criminal Justice Agency.

Additional agreements, such as a Memorandum of Agreements, Service Level Agreements, and/or Continuity Plans, may be established and maintained to further delineate, define, and assign roles, responsibilities, and requirements of and agreements between SPD and ITD, and other City of Seattle Departments and/or agencies.

Tracye Cantrell

Tracye Cantrell
Interim Chief Technology Officer
Seattle Information Technology Department

Date Feb 2, 2018

Carmen Best

Carmen Best
Interim Chief of Police |
Seattle Police Department

Date 2-7-2018

Reference: CJIS Security Policy, Version 5.5, dated June 1, 2016 (CJISD-ITS-DOC-08140-5 .5)

IT Support Services for City Technology

Engineering and Operations

This division designs, implements, operates, and supports technology solutions and resources in accordance with city wide architecture and governance. Responsibilities for this division include:

- Primary communications networks that provide public safety and constituent access to and from City government; the telephone system, the data network, and Public Safety Radio System. Responsible for sustaining all three systems operating as close to 100% availability as possible 24 hours a day, seven days a week.
- Design, acquisition, installation, maintenance, repair and management of fiber optic cables on behalf of City departments and approximately 20 other local, state and federal agencies.
- Procurement requests, allocation, operation and maintenance of city wide and departmental servers, virtual enterprise computing and SAN storage environments for large scale mission critical applications in a secure, reliable, 24/7 production environment for enterprise computing.
- Allocation, operation and maintenance of enterprise level services like messaging services, web access, file sharing, user management and remote access solutions.
- Collaborate with Enterprise Architecture team to develop standards for information technology equipment and software.
- Service Desk and technical support services for City's computers, peripherals, electronic devices and mobile device management.
- Centralized IT asset management to include research, procurement request, surplus and asset transfer.
- Facility management for a reliable production computing environment to the City departments.
- Support for other enterprise services and tools.

Compute System Technologies

This team manages the operations and maintenance of computing infrastructure, including servers, storage, backup and recovery, and enterprise support systems (e.g., Active Directory, VPN, etc.). The team is also responsible for safeguarding systems and data by performing required security patches, updates, and backups to ensure systems operate at as close to 100% availability as possible 24x7. Units within this group include:

Systems Operations. The team is focused on delivering the computing environment across multiple departments. The team has technical expertise to design, integrate, and operate a secure, reliable computing environment. Key technologies include Windows, Solaris, IBM AIX, and Linux.

Enterprise Services. Enterprise Services (ES) are large scale infrastructure and application services used by the City of Seattle end user community. This includes both SaaS and NGDC hosted infrastructure and application services. The team is responsible for EA vendor management, system administration, upgrades and technical support. Key technologies includes Microsoft Active Directory (AD), Distributed File System (DFS), Exchange Online, Office 365 and SharePoint Online infrastructure.

Infrastructure Tools. The team provides a single focus for the design, planning, deployment and maintenance of standard enterprise infrastructure monitoring and management tools. This includes system performance (Solarwinds, SCOM), configuration management (SCCM, WSUS), and monitoring and system management (Trend Micro, CRM, Vipre).

Virtual and Data Infrastructure. This team engineers and operates reliable, flexible, performant virtualized Windows, UNIX and Linux platforms and their related technologies in direct support of critical business applications. Key technologies include Solaris, Unix, Linux, Windows, and vmWare, and the associated virtualization Nutanix, IBM LPAR, and Solaris hardware.

The team also engineers and operates reliable, flexible, performant storage and data protection solutions to host and protect critical business data of all types, leveraging SAN, NAS, object, and cloud technologies. Key technologies include Dell Compellent, Quantum, Hitachi, NetApp, Cloud storage, Brocade fiber channel switching, and Commvault.

Network And Communications Technologies

This team is responsible for designing, installing, operating, and maintaining data, voice, radio, fiber optic, and structured cabling infrastructure that integrates with other technologies to provide access to resources used by City departments and the public we serve. Units within this group include:

Network Engineering & Operations. The Network Services team engineers, operates and maintains the City's data network, including data center core networks, the internet perimeter, the network backbone, and local area networks that support systems and users across the City. This group designs, acquires, installs, maintains, repairs, and manages an enterprise data network that aligns with City architectures and standards. This group also participates in development of those standards and provides tier 2 and 3 end user support. This team supports technologies that include routing, switching, load balancing, enterprise Wi-Fi, DNS/DHCP/NTP, and network security (including firewalls, VPN appliances, certificate infrastructure, network access control, and web filtering.)

Telecommunication Engineering & Operations. The Telecommunications Services team engineers, operates, and maintains a highly-reliable enterprise telephone and contact center infrastructure. This group supports end user move and change activity and provides tier 2 and 3 support. The Telecommunication Services team acquires, installs, maintains, and repairs telecommunications equipment and manages commercial telephony circuits. It supports technologies that include VoIP, circuit-switched telephony, voice mail, contact center services (including call routing scripts), audio conference bridges, commercial telephony services, SONET, and WDM.

Radio & Communications Infrastructure. This team delivers radio services for public safety and other government departments. It provides extremely reliable infrastructure and support for end user mobile and portable radio equipment. The group installs and maintains communications equipment inside 911 dispatch centers and City vehicles, with primary support to SPD and SFD. The team also supports regional planning, maintenance, interoperability testing, and projects (including PSERN and Washington OneNet) in partnership with other local, state, and federal agencies. This team also

designs, acquires, installs, maintains, repairs, and manages in-building structured cabling systems and outside plant fiber optic and copper cable infrastructure for the City and approximately 20 external public agency partners. Technologies include trunked and conventional land mobile radio, microwave radio and other wireless communications systems (including point-to-multipoint and mesh networks,) distributed antenna systems, routing/MPLS, DS3/T1/DACS, outside plant cable infrastructure (including fiber and copper,) and structured cabling infrastructure.

End User Support

This team is responsible for providing a single point of contact for IT technical support, trouble ticket and service request resolution and referral services to other IT workgroups, and for communication for all changes, patches, upgrades and standards changes. The team is also responsible for providing technical support for the City's desktop computers, peripherals, electronic devices and mobile devices. Units within this group include:

Service Desk. The Service Desk team provides a single point of contact for Seattle IT services, promptly resolving incidents and service requests when first contacted whenever possible, escalating issues accurately and efficiently, and keeping users and partners aware of service status and changes.

Device Support. This team provides direct customer support for end user computing to all departments within the City and tier 2 escalation support and management of centralized end user computing applications and hardware. requests.

Device Engineering. This team engineers and deploys software packages for end user applications, device drivers, patches, security updates and custom packages as required. This team evaluates and recommends hardware and software for end user standards. In addition, this team provides tier 3 escalation support and management of centralized end user computing applications and hardware.

Asset Management. This team is responsible tracking and inventory controls for city wide IT assets including desktops, laptops, printers, servers, switches, and miscellaneous Information Technology infrastructure. In addition to inventory control, the team will be forecasting replacement cycles for equipment based on City standards to promote a stable computing environment.

IT Operations Support

The IT Operations Support team is responsible for management of Information Technology facilities (including data centers and communications equipment rooms), and installation and cabling equipment within those facilities. This team provides the enterprise Network Operations Center (NOC) that monitors alerts, performs initial incident analysis, dispatches tier 2 and 3 technical support, and provides initial incident communication for network infrastructure and computing systems managed by Engineering and Operations. Units within this group include:

Installation Management. This team installs networking and computing equipment in data centers, communications rooms and wiring closets; installs and maintains network cabling within data centers and equipment rooms according to City standards; and supports repair and end user move and change activity (including telephone move projects).

IT Operations Center. This team manages facilities which support City computing and communications services. This includes managing access to facilities, coordinating vendors, maintaining records (including data center inventory management), and, where applicable, monitoring facility systems (including CRUs, fire alarms, water detection sensors, UPS systems, and power consumption). This team also staffs the NOC that monitors alerts from network infrastructure and computing systems, performs initial problem analysis, dispatches appropriate tier 2 and 3 technical support team(s), and provides initial incident communication.

Application Services

This division designs, develops, integrates, implements, and supports application solutions in accordance with city wide architecture and governance. Its teams are organized to support business functions or service groups**.** The integration of application services will be completed gradually in 2017, with details of the organization and integration process still under development.

Applications

These teams will provide development and support for applications that include customer relationship management, billing, finance, human resources, work and asset management and records management.

Shared Platforms

These teams will provide development and support for applications that include engineering, spatial analysis, business intelligence, analytics, SharePoint Online and document management.

Cross Platform Services

These teams will provide support to application teams, including quality assurance, change control, database administration, integration services, and access management activities.

City of Seattle

Technical Security Audit

Technical Security Audit

Agency Information: Seattle PD - (WASPD0000)

Submitted By: Pepper Bojang-Jackson - On: March 22, 2017 Compliance Report with Agency Responses

Compliance Report

NCIC compliance standards must be improved and a response submitted to the WSP ACCESS Section.

Item:	1
Section Name:	Personnel Security
Question:	Are you maintaining a record of all your agency and/or county/city IT personnel that must receive a state of residency fingerprint background check within 30 days of employment? *(CJIS Security Policy, Version 5.5, Section 5.12.1.1)* Yes Please provide the SID numbers for all the IT personnel.
Agency Response:	List emailed 05/16/17

Item:	2
Section Name:	Personnel Security
Question:	Have all your agency and/or county/city IT personnel viewed the technical security awareness training (Level 4) in CJIS Online? *(CJIS Security Policy, Version 5.5, Section 5.2)* Yes All technical staff must view the technical security training - level 4 once every two years. Please provide a list of names of who viewed the training. The training is available at the following address: https://www.cjisonline.com/
Agency Response:	Sent email 05/16/17

Item:	3

City of Seattle

Section Name: Personnel Security

Question: Does your agency use an IT vendor for any IT needs?

Sub Question(s)

Item: 3.1

Section Name: Personnel Security

Question: Have all IT *vendors* had a Washington State fingerprint background check completed? *(CJIS Security Policy, Version 5.5, Section 5.12.1.1 and 5.12.1.2)*

User Answer: Yes

Compliance Response: All IT vendors must have a Washington State fingerprint background check completed.

Agency Response: List emailed 05/16/17

Sub Question(s)

Item: 3.2

Section Name: Personnel Security

Question: Please send a copy of the security addendum signed by each employee of the vendor company to CJISAudits@wsp.wa.gov

User Answer: I have read and will comply.

Compliance Response: Please provide a copy of the signed security addendum for each employee of the vendor company. I am missing security addendums for the following vendors:

1. 4quarters
2. Advantage Factory
3. Dorsey Consulting
4. Gartner
5. Genetec Corp
6. Sabey
7. Sysorex Consulting
8. TASER
9. TEKsystems
10. Versaterm - only a few

Agency Response:

1. 4quarters - Emailed 05/08/17
2. Advantage Factory - All Advantage Factory accounts are

inactive
3. Dorsey Consulting - DOJ Monitoring Team - Should be CJIS Level 2, not 4 (deactivated all accounts)
4. Emailed 05/22/17
5. Genetec Corp - All accounts are inactive.
6. Adashi - Adashi employees are working in an environment that does not currently have CJIS data. Future plans do include CJIS data so they are in the process of completing the Security Addendums.
7. Sysorex Consulting - All accounts are inactive

8. TASER - Emailed 05/18/17
9. TEKsystems - Contractor is now City IT w/updated information.
10. Versaterm - Emailed 05/08/17

Item: 4
Section Name: System and Communications Protection and Information Integrity
Question: Does your agency email CJI? *(CJIS Security Policy, Version 5.5, Section 5.10.1.2)*

Sub Question(s)

Item: 4.1
Section Name: System and Communications Protection and Information Integrity
Question: Is the email that contains CJI encrypted? *(CJIS Security Policy, Version 5.5 Section 5.10.1.2)*
User Answer: No
Compliance Response: CJI that is emailed is required to be encrypted. Please advise when you will have this in place.
Agency Response: Seattle is utilizing Office 365 for email and email is encrypted

Is the email encrypted in transit? https://products.office.com/en-us/business/office-365-trust-center-security

Outlook client to O365 - SSL/TLS connection is established between Outlook client and O365

O365 to OME server - SSL / TLS connection between EXO Transport servers and OME server. "Office 365 uses Transport Layer Security (TLS) to encrypt the connection, or session, between two servers." https://support.office.com/en-us/article/Email-encryption-in-Office-365- c0d87cbe-6d65-4c03-88ad-5216ea5564e8

Is the email encrypted at rest when it sits on the server? https://support.office.com/en-us/article/Email-encryption-in-Office-365-c0d87cbe-6d65-4c03-88ad-5216ea5564e8

What about encryption for data at rest?

"Data at rest" refers to data that isn't actively in transit. In Office 365, email data at rest is encrypted using BitLocker Drive Encryption.
BitLocker encrypts the hard drives in Office 365 datacenters to provide enhanced protection against unauthorized access. To learn more, see BitLocker Overview.

What level of encryption does OME use? - Microsoft attests that they meet and/or exceed FBI CJIS requirements

The CJIS Security Policy defines 13 areas that private contractors such as cloud service providers must evaluate to determine if their use of cloud services can be consistent with CJIS requirements. These areas correspond closely to NIST 800-53, which is also the basis for the Federal Risk and Authorization Management Program (FedRAMP), a program under which Microsoft has been certified for its Government Cloud offerings

Item: 5

Section Name: Event Logging

Question: Does your agency have an established audit trail capable of monitoring the following:

- Successful and unsuccessful log on attempts
- Successful and unsuccessful password changes
- Successful and unsuccessful attempts to access, create, write, delete or change permissions on a user account, file, directory or other system resources
- Successful and unsuccessful actions by privileged accounts
- Successful and unsuccessful attempts for users to access, modify, or destroy audit log files

(CJIS Security Policy, Version 5.5, Section 5.4.1.1)

User Answer: No

Compliance Response: Please advise when your agency will have an established audit trail capable of monitoring the following:

- Successful and unsuccessful log on attempts
- Successful and unsuccessful password changes
- Successful and unsuccessful attempts to access, create, write, delete or

change permissions on a user account, file, directory or other system resources

- Successful and unsuccessful actions by privilegedaccounts
- Successful and unsuccessful attempts for users to access, modify, or destroy audit log files

Agency Response:

Seattle PD has established an audit trail capable of monitoring the following:

- Successful and unsuccessful log on attempts
- Successful and unsuccessful password changes
- Successful and unsuccessful attempts to access, create, write, delete or change permissions on a user account, file, directory or other system resources
- Successful and unsuccessful actions by privilegedaccounts
- Successful and unsuccessful attempts for users to access, modify, or destroy audit log files

Item: 6

Section Name: Identification and Authentication

Question: Does your agency and/or county/city IT department employee perform remote assistance from a non-secure location? Example employees home or coffee shop etc.

(CJIS Security Policy, Version 5.5, Section 5.6.2.2)

User Answer: Yes

Compliance Response: IT has the ability to remote in the system from a non-secure location. Please advise once Advanced Authentication will be in place or when a remote session will be virtually escorted at all times.

Agency Response:

Full policy emailed to ACCESS on 04/23/18:

This policy applies to employees, contractors, or vendors who have a need to remotely access the CJI (Criminal Justice Information) in-scope systems for maintenance and operations. All access both remote and within the Seattle network (except for the SPD network) is through bastion hosts protected by two-factor Advanced Authentication (AA).

*All non-law enforcement personnel who perform criminal justice functions or have access to Criminal justice data shall acknowledge, via signing of the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS

Security Addendum. Seattle Information Technology employees are not required to sign the Security Addendum provided there is a CJIS Management Control Agreement (MCA) between Seattle Information Technology and Seattle Police/Fire.

*CJIS Security Awareness Training shall be required upon initial assignment, and biennially thereafter, for all personnel who have access to CJI.

Verify Identification: a state of residency and national fingerprint-based record checks shall be conducted (prior to) assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.

*All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All designees shall be from an authorized criminal justice agency.

*VPN access must be approved by the requesting department prior to activation.

*Users must not:

Type remote access passwords while someone is watching. Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. (CJIS Security Policy Section 5.5.5) A session lock is not a substitute for logging out of the information system or from disconnecting a remote session.

Be connected to other network connections during remote access sessions into CJI data in-scope (e.g., no split tunnels are allowed).

*Users must maintain current virus protection and a host firewall on remote systems to protect from viruses and other remote attacks.

*Vendors must:

Be provided with the minimum access required to perform the necessary duties while the VPN session is active. Other access and privileges will be limited to the specific function performed by each vendor or service provider.

Be monitored by a City of Seattle CDE administrator during an assisted remote control session using Skype for Business or other current City of Seattle Enterprise standard for remote control sessions. The CDE administrator must have the ability to end the session at any time and the session must be terminated as soon as their work has finished.

Item: 6.1

Section Name: Identification and Authentication

Question: Describe the type of Advanced Authentication (AA) that is being used while the remote session is in process or advise if the session is being virtually escorted at all times. Virtually escorting is permitted when the following conditions are met:

- The session shall be monitored at all times by an authorized escort.
- The escort shall be familiar with the system/area in which the work is being performed.
- The escort shall have the ability to end the session at any time.
- The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.
- The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.

(CJIS Security Policy, Version 5.5, Section 5.5.6)

User Answer: Certificate on the workstation. RSA is being implemented for network equipment.

Rarely workstations are remotely accessed. If they are, an SPD computer would be used to do the support work.

Compliance Response: Please advise when AA will be in place for IT staff that conducts remote assistance on applications or networks that access CJI or when all personnel will be virtually escorted or a policy prohibiting remote access from an unsecure location is established.

Agency Response: See #6

City of Seattle

Item: 7

Section Name: Cloud Computing

Question: Does the agency utilize a cloud provider to host or store CJI related systems, applications or data? *(CJIS Security Policy, Version 5.5, Section 5.10.1.5)*

Sub Question(s)

Item: 7.1

Section Name: Cloud Computing

Question: Is the CJI encrypted prior to entering the cloud?

User Answer: No

Compliance Response: Please advise when the CJI that goes to the cloud will be encrypted.

Agency Response: Seattle is utilizing Office 365 and CJI is encrypted

Report Summary: The Federal Bureau of Investigation (FBI) assigned the Washington State Patrol (WSP) as the Criminal Justice Information Services (CJIS) Systems Agency (CSA) for the state of Washington. The CSA is responsible for establishing and administering an information technology security program throughout the CSA user community, to include the local levels. All standards set forth in the audit questionnaire originate

from the CJIS Security Policy which provides Criminal Justice Agencies (CJA) with a minimum set of security requirements for access to FBI CJIS Division systems and information to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

Remote Access Policy

City of Seattle

CJIS Remote Access Policy

June 1st, 2018

Overview

The CJI Remote Access Policy defines the necessary controls for remote access to Criminal Justice Information Services (CJIS) in scope systems.

Purpose

This policy ensures proper measures are taken when granting remote access to any employee, contractor, or vendor, to Criminal Justice Information (CJI) in-scope systems.

Definition

CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, decimation, storage, and destruction of CJI.

Scope and Applicability

This policy applies to personnel at City of Seattle, including those affiliated with third parties who remotely access City of Seattle systems to include CJI data. The policy applies to all systems owned by and/or administered by City of Seattle, including network to network VPN tunnels.

Policy

This policy applies to City of Seattle employees, City of Seattle Police Department employees, contractors, or vendors who have a need to remotely access the CJI (Criminal Justice Information) in-scope systems for maintenance and operations. All access both remote and within the City of Seattle network or Public network, are required to utilize two factor authentication & VPN tunnel on City of Seattle workstation OR through a jump-box protected by two-factor Advanced Authentication (AA). Contractors, Vendors and City employees accessing in-scope systems from non-city computers are required to utilize the jump-box AA solution.

All non-law enforcement personnel who perform criminal justice functions or have access to Criminal justice data shall acknowledge, via signing of the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. Seattle Information Technology employees are not required to sign the Security Addendum provided there is a CJIS Management Control Agreement (MCA) between Seattle Information Technology and Seattle Police/Fire.

- CJIS Security Awareness Training shall be required upon initial assignment, and biennially thereafter, for all personnel who have access to CJI.
- Verify Identification: a state of residency and national fingerprint-based record checks shall be conducted (prior to) assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.
- All requests for access shall be made as specified by the CSO (CJIS Systems Officer). The CSO, or their designee, is authorized to approve access to CJI. All designees shall be from an authorized criminal justice agency.
- VPN access must be approved by the requesting department prior to activation.
- Users must not:
    - Type remote access passwords while someone is watching. Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. (CJIS Security Policy Section 5.5.5) A session lock is not a substitute for logging out of the information system or from disconnecting a remote session.
    - Be connected to other network connections during remote access sessions into CJI data in-scope (e.g., no split tunnels are allowed).
- Users must maintain current virus protection and a host firewall on remote systems to protect from viruses and other remote attacks.
- Vendors must:
    - Be provided with the minimum access required to perform the necessary duties while the VPN session is active. Other access and privileges will be limited to the specific function performed by each vendor or service provider.
    - Be monitored by a City of Seattle CDE administrator during an assisted remote control session using Skype for Business or other current City of Seattle Enterprise standard for remote control sessions. The CDE administrator must have the ability to end the session at any time and the session must be terminated as soon as their work has finished.

Applicability of other Policies

January 17, 2016 1 The City of Seattle has an existing Remote Access Policy that must be adhered to and can be found here.

Enforcement

Enforcement of this policy will be led by the Chief Technology Officer (CTO). Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment or vendor contract termination. Where illegal activities or loss of City of Seattle assets are known or suspected, the City of Seattle must report activities to the appropriate authorities, City of Seattle is obliged to adhere to breach reporting by statutory limitation and must notify the Terminal Agency Coordinator (TAC) of any potential violations. All potential violations that involve CJI must be report to the Washington State Patrol ACCESS Section.

Implementation

This Policy is implemented by the ITD Security, Risk, and Compliance Director and applies to the City of Seattle access to CJI.

Document Control

Version	Content	Contributors	Approval Date
1.0	Initial Draft	Reviews: Denise Mendoza; Pepper Bojang-Jackson Approvers: CISO Andrew Whitaker CTO	
1.1	Initial Draft	Reviews: Denise Mendoza; Pepper Bojang-Jackson	
1.2	Initial Draft	Reviews: Denise Mendoza Bruce Hills Pepper Bojang-Jackson	
1.3	Review	Andrew Whitaker	6/5/18
1.4	Approved	Tracye Cantrell	6/12/18

CJIS Security Policy

The CJIS Security Policy may be found below.

Appendix J: CTO Notification of Surveillance Technology

Thank you for your department's efforts to comply with the new Surveillance Ordinance, including a review of your existing technologies to determine which may be subject to the Ordinance. I recognize this was a significant investment of time by your staff; their efforts are helping to build Council and public trust in how the City collects and uses data.

As required by the Ordinance (SMC 14.18.020.D), this is formal notice that the technologies listed below will require review and approval by City Council to remain in use. This list was determined through a process outlined in the Ordinance and was submitted at the end of last year for review to the Mayor's Office and City Council.

The first technology on the list below must be submitted for review by March 31, 2018, with one additional technology submitted for review at the end of each month after that. The City's Privacy Team has been tasked with assisting you and your staff with the completion of this process and has already begun working with your designated department team members to provide direction about the Surveillance Impact Report completion process.

Please let me know if you have any questions.

Thank you,

Michael Mattmiller

Chief Technology Officer

Technology	Description	Proposed Review Order
Automated License Plate Recognition (ALPR)	ALPRs are computer-controlled, high-speed camera systems mounted on parking enforcement or police vehicles that automatically capture an image of license plates that come into view and converts the image of the license plate into alphanumeric data that can be used to locate vehicles reported stolen or otherwise sought for public safety purposes and to enforce parking restrictions.	1
Booking Photo Comparison Software (BPCS)	BCPS is used in situations where a picture of a suspected criminal, such as a burglar or convenience store robber, is taken by a camera. The still screenshot is entered into BPCS, which runs an algorithm to compare it to King County Jail booking photos to identify the person in the picture to further investigate his or her involvement in the crime. Use of BPCS is governed by SPD Manual §12.045.	2
Forward Looking Infrared Real-time video (FLIR)	Two King County Sheriff's Office helicopters with Forward Looking Infrared (FLIR) send a real-time microwave video downlink of ongoing events to commanders and other decision-makers on the ground, facilitating specialized radio tracking equipment to locate bank robbery suspects and provides a platform for aerial photography and digital video of large outdoor locations (e.g., crime scenes and disaster damage, etc.).	3

Technology	Description	Proposed Review Order
Undercover/ Technologies	The following groups of technologies are used to conduct sensitive investigations and should be reviewed together. • **Audio recording devices**: A hidden microphone to audio record individuals without their knowledge. The microphone is either not visible to the subject being recorded or is disguised as another object. Used with search warrant or signed Authorization to Intercept (RCW 9A.73.200). • **Camera systems**: A hidden camera used to record people without their knowledge. The camera is either not visible to the subject being filmed or is disguised as another object. Used with consent, a search warrant (when the area captured by the camera is not in plain view of the public), or with specific and articulable facts that a person has or is about to be engaged in a criminal activity and the camera captures only areas in plain view of the public. • **Tracking devices**: A hidden tracking device carried by a moving vehicle or person that uses the Global Positioning System to determine and track the precise location. U.S. Supreme Court v. Jones mandated that these must have consent or a search warrant to be used.	4
Computer-Aided Dispatch (CAD)	CAD is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field.	5

Technology	Description	Proposed Review Order
CopLogic	System allowing individuals to submit police reports on-line for certain low-level crimes in non-emergency situations where there are no known suspects or information about the crime that can be followed up on. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.	6
Hostage Negotiation Throw Phone	A set of recording and tracking technologies contained in a phone that is used in hostage negotiation situations to facilitate communications.	7
Remotely Operated Vehicles (ROVs)	These are SPD non-recording ROVs/robots used by Arson/Bomb Unit to safely approach suspected explosives, by Harbor Unit to detect drowning victims, vehicles, or other submerged items, and by SWAT in tactical situations to assess dangerous situations from a safe, remote location.	8
911 Logging Recorder	System providing networked access to the logged telephony and radio voice recordings of the 911 center.	9
Computer, cellphone and mobile device extraction tools	Forensics tool used with consent of phone/device owner or pursuant to a warrant to acquire, decode, and analyze data from smartphones, tablets, portable GPS device, desktop and laptop computers.	10
Video Recording Systems	These systems are to record events that take place in a Blood Alcohol Concentration (BAC) Room, holding cells, interview, lineup, and polygraph rooms recording systems.	11
Washington State Patrol (WSP) Aircraft	Provides statewide aerial enforcement, rapid response, airborne assessments of incidents, and transportation services in support of the Patrol's public safety mission. WSP Aviation currently manages seven aircraft equipped with FLIR cameras. SPD requests support as needed from WSP aircraft.	12

Technology	Description	Proposed Review Order
Washington State Patrol (WSP) Drones	WSP has begun using drones for surveying traffic collision sites to expedite incident investigation and facilitate a return to normal traffic flow. SPD may then request assistance documenting crash sites from WSP.	13
Callyo	This software may be installed on an officer's cell phone to allow them to record the audio from phone communications between law enforcement and suspects. Callyo may be used with consent or search warrant.	14
I2 iBase	The I2 iBase crime analysis tool allows for configuring, capturing, controlling, analyzing and displaying complex information and relationships in link and entity data. iBase is both a database application, as well as a modeling and analysis tool. It uses data pulled from SPD's existing systems for modeling and analysis.	15
Parking Enforcement Systems	Several applications are linked together to comprise the enforcement system and used with ALPR for issuing parking citations. This is in support of enforcing the Scofflaw Ordinance SMC 11.35.	16
Situational Awareness Cameras Without Recording	Non-recording cameras that allow officers to observe around corners or other areas during tactical operations where officers need to see the situation before entering a building, floor or room. These may be rolled, tossed, lowered or throw into an area, attached to a hand-held pole and extended around a corner or into an area. Smaller cameras may be rolled under a doorway. The cameras contain wireless transmitters that convey images to officers.	17
Crash Data Retrieval	Tool that allows a Collision Reconstructionist investigating vehicle crashes the opportunity to image data stored in the vehicle's airbag control module. This is done for a vehicle that has been in a crash and is used with consent or search warrant.	18

Technology	Description	Proposed Review Order
Maltego	An interactive data mining tool that renders graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the internet.	19

Please let me know if you have any questions.

Thank you,

Michael

POWERFUL TECHNOLOGY SOLUTIONS
FOR THE CITY AND PUBLIC WE SERVE

2018 Surveillance Impact Report

PARKING ENFORCEMENT SYSTEMS (INCLUDING ALPR)

SEATTLE POLICE DEPARTMENT

January 31, 2019

Seattle
Information Technolog

CONTENTS

SUBMITTING DEPARTMENT SIR RESPONSE 4

2019 POLICY UPDATE 7

SURVEILLANCE IMPACT REPORT OVERVIEW 8

PRIVACY IMPACT ASSESSMENT 9

FINANCIAL INFORMATION 29

EXPERTISE AND REFERENCES 31

RACIAL EQUITY TOOLKIT AND ENGAGEMENT FOR PUBLIC COMMENT WORKSHEET 33

PRIVACY AND CIVIL LIBERTIES ASSESSMENT 43

CTO RESPONSE 50

APPENDIX A: GLOSSARY 57

APPENDIX B: PUBLIC COMMENT DEMOGRAPHICS AND ANALYSIS 60

APPENDIX C: PUBLIC MEETING NOTICE(S) 64

APPENDIX D: MEETING SIGN-IN SHEET(S) 72

APPENDIX E: ALL INDIVIDUAL COMMENTS RECEIVED 100

APPENDIX F: LETTERS FROM ORGANIZATIONS 153

APPENDIX G: EMAILS & LETTERS FROM THE PUBLIC 165

APPENDIX H: PUBLIC COMMENT ANALYSIS METHODOLOGY 171

APPENDIX I: POLICIES AND PROCEDURES GOVERNING ALPR 173

APPENDIX J: CTO NOTICE OF SURVEILLANCE TECHNOLOGY 330

SUBMITTING DEPARTMENT SIR RESPONSE

Seattle
Police Department

Memo

Date: 11/27/2018
To: City Council
From: Deputy Chief Marc Garth Green, Seattle Police Department
Subject: ALPR Parking Enforcement

Description

Automated License Plate Readers (ALPRs) are vehicles equipped with high definition infrared digital cameras that are mounted on the vehicle. The Seattle Police Department has eight parking enforcement vehicles equipped with ALPRs. Three of ALPR vehicles utilized by parking enforcement are designated for scofflaw enforcement (these boot vans carry boot devices that can be mounted to immobilize vehicles in violation of scofflaw) and five parking enforcement vehicles are designated for parking enforcement in time-restricted zones and residential parking zones. The ALPRs, when activated, continuously capture photos of vehicles and license plates and then filter those "reads" through software to determine whether they system will "hit" on the license plate. A hit may come from a HotList that is uploaded daily and is managed by the Washington State Patrol. This list contains national stolen vehicle and license plate data, along with information about license plates connected with criminal investigations. A hit may also come from the Seattle Municipal Court's system, identifying a scofflaw vehicle. Or a hit may come from a vehicle that has been parked beyond the designated maximum time or is parked in a Restricted Parking Zone without the required permit. When the software hits on a license plate, the parking enforcement officer must verify that the hit was accurate. Only after verification may the officer take further action, such as issuing a parking ticket or booting the vehicle. If the ALPR hits for a reason other than parking or scofflaw enforcement, parking enforcement officers request assistance from patrol officers then return to focusing on parking enforcement purposes.

Parking enforcement vehicle reads are destroyed at the end of the shift. Scofflaw enforcement vehicle reads are stored, maintained, and managed on SPD's premises. Retention is automated and will be automatically deleted after 90 days per department retention policy unless a record is identified as being related to a parking violation or criminal investigation and exported in support of that citation or investigation (see ALPR: Patrol SIR for further detail).

Purpose

The Seattle Police Department (SPD) facilitates the flow of traffic, assists with the collection of revenue related to parking violations in the City of Seattle, and recovers stolen vehicles through a variety of tools.

610 Fifth Avenue | PO Box 34986 | Seattle, WA 98124-4986 | 206-684-5485 | seattle.gov/police

Among these is Parking Enforcement Systems technology, which is used by SPD as a necessary tool to enforce parking such as the Scofflaw Ordinance, time-restricted parking areas, and restricted parking zones. Parking citations are a significant source of revenue for the City. In 2016 and 2017, parking citations generated approximately $20 million in revenue collected each year.

Benefits to the Public

Drivers in Seattle spend almost 60 hours per year looking for parking in the City. This contributes to congestion and traffic flow concerns. Traffic congestion has increased with population growth and development, and is likely to continue to increase with Viaduct demolition and other future development. Parking Enforcement systems assist the City in managing traffic flow and parking assets, and recouping revenue lost to parking violations (Scofflaw, time-restricted parking enforcement, RPZ violations, and metered parking).

Our primary concern as a law enforcement agency is to reduce crime and disorder. SPD uses ALPR to help achieve this goal. Parking Enforcement ALPR assist the City in locating stolen vehicles. In 2017, 3613 motor vehicle thefts were reported in the City of Seattle. Using ALPR, Parking Enforcement identified 318 confirmed stolen vehicles. During the first nine months of 2018, 2600 motor vehicle thefts were reported in the City of Seattle. Using ALPR, Parking Enforcement identified 349 confirmed stolen vehicles during that period.

Privacy and Civil Liberties Considerations

During the public comment period, SPD heard concerns about privacy and civil liberties from community members. They raised concerns around the perceived overcollection of data, data-sharing with other agencies, policies that may need updating, and a 90-day retention period for data that is stored onsite at SPD.

SPD recognizes the privacy concerns most correlated with ALPR are related to the data collected while enforcing parking and traffic laws. Because ALPRs collect license plate information from vehicles, that information could be correlated with other information to personally identify innocent individuals, determine where they were parked at a given time, track their movements, or be pooled with ALPR data from other agencies. To attempt to mitigate these concerns, SPD requires its officers to follow SPD and City policies, and the laws of the city, state, and federal government. SPD also audits usage of the ALPR systems and access to stored ALPR data, and welcomes independent audits from the Office of the Inspector General. To address specific concerns, please see below:

- **Data-sharing policies**: SPD does not pool its ALPR data with any other agency's data. SPD limits data-sharing with other law enforcement agencies for official law enforcement purposes and requires an audit-trail whenever an SPD officer accesses the ALPR data. Further, SPD complies with the Mayoral Directive dated February 6, 2018, requiring all City departments to seek approval from the Mayor's Office before sharing data and information with ICE. However, individuals may request ALPR data through a public records request, and no court has determined whether ALPR data is

exempt from disclosure under the Washington State Public Records Act. Individuals also have the right to inspect their criminal history record information maintained by the department.

- **Overcollection of data**: Parking enforcement ALPR vehicles do not save the data they collect beyond the end of the parking enforcement officer's shift. Scofflaw ALPR vehicles only collect data about vehicles and license plates and then download that data into SPDs' onsite storage. The ALPR vehicles do not automatically link that data to private data such as Department of Licensing information about the registered owner or the driver. Any link between the vehicle and the driver or owner must be instigated by an officer who is investigating a specific crime. Further, SPD continues to comply with the City's intelligence ordinance (SMC 14.12) which only permits "the collection and recording of information for law enforcement purposes, so long as these police activities do not unreasonably: (a) infringe upon individual rights, liberties, and freedoms guaranteed by the Constitution of the United States or of the State—including, among others, the freedom of speech, press, association, and assembly; liberty of conscience; the exercise of religion; and the right to petition government for redress of grievances; or (b) violate an individual's right to privacy."

- **Ninety-day retention period**: SPD maintains the downloaded data collected by Scofflaw enforcement vehicles for 90 days and then automatically deletes it, which is commensurate with the Washington Secretary of State's retention policy for 911 audio recordings, in-car video recordings unrelated to specific incidents, and recordings of radio transmissions between law enforcement and dispatch staff. SPD investigators use the retained ALPR data to help solve serious offenses such as robberies, shootings, and kidnappings. SPD investigators also use ALPR data to help find vulnerable people, such as with "silver alerts" or at the request of family members concerned about a suicidal loved-one. By maintaining the data for 90 days, SPD balances the privacy concerns of the community with the needs of victims to have their cases solved. Every officer who uses the ALPR vehicles or accesses the ALPR data must comply with SPD policies and city, state, and federal laws.

- **New policies**: SPD recognizes that its current ALPR policy needs updating and anticipates that an updated ALPR policy will be in place by January 31, 2019. In addition, SPD has recently updated its policy related to Foreign Nationals, emphasizing that SPD has no role in immigration enforcement and will not inquire about any person's immigration status. In addition, SPD welcomes the OIG to audit its use of ALPR technologies and data.

Summary

ALPR technology is an effective tool for assisting SPD with a variety of responsibilities, from enforcing parking laws to addressing scofflaw vehicles to solving serious crimes. SPD utilizes this resource thoughtfully and efficiently by deploying ALPR vehicles to specific areas where parking enforcement is important to the community. SPD remains committed to complying with laws, policies, and procedures, and sharing data with law enforcement agencies only for law enforcement purposes.

2019 POLICY UPDATE

Through the course of the completion of this Surveillance Impact Report, SPD recognized the need to update the existing ALPR Policy and on February 1, 2019 the new SPD ALPR policy went into effect. This new policy expanded on the previous by adding definitions of the terms used in the operation of the technology, expanding on the required training for employees prior to access and use of ALPR, detailing authorized and prohibited uses of ALPR, defining response to alerts, detailing how ALPR equipment is to be handled, detailing ALPR administrator roles, defining ALPR data storage and retention, and detailing policy around the release or sharing of ALPR data.

In the interest of transparency, the original SIR documents policy as it stood at the time of completion of the SIR (including public engagement and Working Group review). References to the new policy are placed next to original policy references and will be indicated underneath the section where they originally appeared.

SURVEILLANCE IMPACT REPORT OVERVIEW

The Seattle City Council passed Ordinance 125376, also referred to as the "Surveillance Ordinance", on September 1, 2017. This Ordinance has implications for the acquisition of new technologies by the City, and technologies that are already in use that may fall under the new, broader definition of surveillance.

SMC 14.18.020.B.1 charges the City's Executive with developing a process to identify surveillance technologies subject to the Ordinance. Seattle IT, on behalf of the Executive, developed and implemented a process through which a privacy and surveillance review is completed prior to the acquisition of new technologies. This requirement, and the criteria used in the review process, are documented in Seattle IT Policy PR-02, the "Surveillance Policy".

HOW THIS DOCUMENT IS COMPLETED

As Seattle IT and department staff complete the document, they should keep the following in mind.

- Responses to questions should be in the text or check boxes only; all other information (questions, descriptions, etc.) should **NOT** be edited by the department staff completing this document.
- All content in this report will be available externally to the public. With this in mind, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.

PRIVACY IMPACT ASSESSMENT

PURPOSE

A Privacy Impact Assessment ("PIA") is a method for collecting and documenting detailed information collected in order to conduct an in-depth privacy review of a program or project. A PIA asks questions about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. It also requests information about policies, training and documentation that govern use of the technology. The PIA responses are used to determine privacy risks associated with a project and mitigations that may reduce some or all of those risks. In the interests of transparency about data collection and management, the City of Seattle has committed to publishing all PIAs on an outward facing website for public access.

WHEN IS A PRIVACY IMPACT ASSESSMENT REQUIRED?

A PIA may be required in two circumstances.

1) When a project, technology, or other review has been flagged as having a high privacy risk.
2) When a technology is required to complete the Surveillance Impact Report process. This is one deliverable that comprises the report.

1.0 ABSTRACT

1.1 Please provide a brief description (one paragraph) of the purpose and proposed use of the project/technology.

Seattle Police Department (SPD) facilitates the flow of traffic, assists with the collection of revenue related to parking violations in the City of Seattle, and recovers stolen vehicles through a number of means. Among these is Parking Enforcement Systems technology, which is used by SPD as a necessary tool in the following ways:

1. Scofflaw – SPD employs three vehicles (two vans, and one truck) with ALPR systems to identify parked vehicles in violation of the City Scofflaw Ordinance. Vehicles in violation are subject to booting, pending payment of past due balances.
2. Time-Restricted Parking Areas – 47 sedans, 54 scooters, 2 vans, and 1 truck are utilized to monitor time-restricted parking within the City. Five of the sedans are equipped with ALPR systems and operated by civilian employees to digitally "chalk" vehicles parked in time-restricted zones. Utilizing GPS location and stem-valve comparison technology, the system alerts on those vehicles that are in violation of the time zone restriction upon a second pass. The remaining vehicles are used in traditional pay to park enforcement, and for manually chalking vehicle tires in time-restricted locations.
3. Restricted Parking Zones ("RPZ") means a portion of the street commonly used for vehicular parking where vehicles properly displaying a permit or other authorization are exempt from the posted RPZ. Seattle Department of Transportation provides SPD with a list of vehicles permitted to park in an RPZ. Parking Enforcement Officers may use ALPR to determine that a vehicle does not have the appropriate permit or authorization to park in an RPZ.
4. Parking Enforcement Officers may use ALPR using a list of vehicles reported stolen or sought in connection with criminal investigation to identify those vehicles and report their location to Dispatch.
5. Parking in the City is also monitored by Parking Enforcement officers on bicycles, foot, and scooters. ALPR is not used in this capacity.

SPD has nineteen vehicles equipped with Automated License Plate Readers (ALPR). Eight of these are Parking Enforcement and eleven are Patrol vehicles. Although ALPR use for Parking Enforcement differs from ALPR use by Patrol in some respects as described in this Surveillance Impact Report and in the ALPR (Patrol) Surveillance Impact Report, all rules and policies that govern ALPR use by SPD as mentioned in the Surveillance Impact Report for ALPR (Patrol) are applicable in the same manner as they are when ALPR is utilized by Parking Enforcement.

The actual surveillance technology in this Surveillance Impact Report (SIR) is Genetec's AutoVu ALPR hardware, which may only be used for the distinctly different purpose of parking enforcement when used with combined with the following (non-surveillance) technologies:

1. **Genetec's Patroller software**, the interface and backend server through which retention periods are set (and auditable), user permissions are managed, user activity is tracked and logged, and camera "read" and "hit" data is accessible.

Continued on next page…

1.1 Continued…

2. **Samsung devices** allow Officers to access the software required to write tickets and enter ticket information.
3. **Gtechna software** prints citations for vehicles found in violation of scofflaw, overtime zone parking, and metered parking.

1.2 Explain the reason the project/technology is being created or updated and why the PIA is required.

Among parking enforcement technologies, privacy concerns are probably most correlated with ALPR data collection in pursuit of parking enforcement. ALPR collects license plate information from vehicles, which could be correlated with other information to personally identify individuals' vehicles and determine where they were parked at a given time, track the movements of innocent individuals, or be pooled with ALPR data from other agencies. Parking enforcement technologies also have the potential to affect individuals residing in vehicles who park in areas where parking regulations apply.

2.0 PROJECT / TECHNOLOGY OVERVIEW

Provide an overview of the project or technology. The overview gives the context and background necessary to understand the purpose, mission and justification for the project / technology proposed

2.1 Describe the benefits of the project/technology.

Drivers in Seattle spend almost 60 hours per year looking for parking in the City. This contributes to congestion and traffic flow concerns. Traffic congestion has increased with population growth and development, and is likely to continue to increase with Viaduct demolition and other future development. Parking Enforcement systems assist the City in managing traffic flow, parking assets, and recouping revenue lost to parking violations (Scofflaw, time-restricted parking enforcement, RPZ violations, and metered parking).

Patrol and Parking Enforcement ALPR assist the City in locating stolen vehicles. In 2017, 3613 motor vehicle thefts were reported in the City of Seattle. Using ALPR, Parking Enforcement identified 318 confirmed stolen vehicles. During the first nine months of 2018, 2600 motor vehicle thefts were reported in the City of Seattle. Using ALPR, Parking Enforcement identified 349 confirmed stolen vehicles during that period.

2.2 Provide any data or research demonstrating anticipated benefits.

Revenue collected from parking citations for two years:
2016: $19,705,640
2017: $20,909,278

2.3 Describe the technology involved.

SPD parking enforcement technologies include: Genetec's AutoVu ALPR hardware, Genetec's Patroller software, Paylock's Bootview software, Samsung handhelds, and Gtechna software. Parking Enforcement ALPR data collected by Scofflaw enforcement boot vans is stored with Patrol ALPR data in the Neology Back Office System Software (BOSS). (See ALPR: Patrol SIR for more detailed description of BOSS).

Parking enforcement ALPR hardware consists of high definition infrared digital cameras that are mounted on three vehicles designated for scofflaw enforcement (these boot vans carry boot devices that can be mounted to immobilize vehicles in violation of scofflaw), and five Parking Enforcement vehicles – for a total of eight ALPR-equipped vehicles that are utilized for Parking Enforcement. The other 39 ticketing vehicles are not equipped with ALPR.

In Time-Limited, no pay parking areas, the ALPR systems in the five sedans digitally "chalk" parked vehicles using GPS location and stem-valve comparison technology. The system alerts on those vehicles that are in violation of the time zone restriction upon a second pass. In RPZs, ALPR can be used to determine whether a vehicle is permitted to park in the RPZ based on the Seattle Department of Transportation-issued list of vehicles currently permitted to park in the RPZ.

The City contracts with Genetec for the AutoVu ALPR system used by Parking Enforcement. Genetec provides Patroller software that works in tandem with cameras, installed by PCS Mobile, Genetec's hardware and install partner. Patroller is the interface and backend server through which retention periods are set (and auditable), user permissions are managed, user activity is tracked and logged, and camera "read" and "hit" data is accessible.

Twice a day, the License Plate Reader File (known as the HotList) is uploaded from the State of Washington into the ALPR system. The license plate numbers compiled on the HotList "may be stolen vehicles, vehicles wanted in conjunction with felonies, wanted persons, and vehicles subject to seizure based on federal court orders" (WSP Memorandum of Understanding No. C141174GSC; March 11, 2014). While ALPR-equipped Parking Enforcement vehicles will receive notifications of any license plate "hits" on the HotList, Parking Enforcement officers radio these in to Dispatch and take no action themselves (see the Surveillance Impact Report for ALPR: Patrol for further information).

In addition to AutoVu, Parking Enforcement uses Paylock's Bootview software to assist SPD and Seattle Municipal Court enforce the ScofflawOrdinance, mandating the booting of vehicles in scofflaw (four or more unpaid violations). Municipal Court contracts with Paylock to assist with tracking the status of vehicles in violation of Scofflaw through its Bootview software program. SPD does not contract with Paylock or Bootview. Parking Enforcement Officers use the City of Seattle Municipal Court's scofflaw list - indicating those vehicles with four or more unpaid parking tickets subject to booting. Parking Enforcement Officers enforcing Scofflaw use this software to verify the current status of vehicles that are identified as being in violation of Scofflaw and to assist in determining whether a ticket should be issued.

Each configuration is designed so that the cameras capture the images and filter the reads through the linked software to determine if/when a hit occurs.

Continued on next page…

2.3 continued…

When the software identifies a hit, it issues an audible alert, and a visual notification informs the user as to what list the hit comes from –Scofflaw, time-restricted over time parking, or HotList.

1) If the user is utilizing the system to enforce Scofflaw violations, the user visually confirms the match and then verifies with Paylock's Bootview (in-vehicle software linked to the Scofflaw list managed by Municipal Court) that the identified vehicle is in Scofflaw before taking further action.
2) In time-restricted parking enforcement, users rely on hits triggered by vehicles that have been digitally chalked and remain in time-restricted zones beyond allotted time. Once the user receives this hit, s/he visually verifies that the license plate read is accurate and, if so, does an image comparison of the tire to determine if the vehicle has moved since it was chalked at an earlier time before taking further action. Autovu's patented tire valve stem technology assists users to make an accurate determination before issuing a violation. Hand-held devices, manufactured by Samsung, are used to 1) check the web-based Pay-by-Phone (contracted with SDOT) application, and parking meter data, to determine if vehicles in metered parking are in violation of their time limits, and 2) to issue citations for all parking infractions. Gtechna prints citations for vehicles found in violation of scofflaw, overtime zone parking, and metered parking.
3) If a Parking Enforcement Officer receives notification of any license plate "hit" on the HotList, s/he radios it in to Dispatch and takes no further action themselves. SPD patrol or detectives assume responsibility for following up (see the SIR for ALPR: Patrol for further information).

2.4 Describe how the project or use of technology relates to the department's mission.

Seattle Police Department utilizes Parking Enforcement Systems to uphold the law including Seattle's Traffic Code and Seattle's Scofflaw Ordinance and to ensure public safety by facilitating the flow of traffic and locating stolen vehicles.

2.5 Who will be involved with the deployment and use of the project / technology?

Parking Enforcement manages and oversees the deployment of ALPR-equipped vehicles for Scofflaw booting and time-restricted parking enforcement. Trained civilian Parking Enforcement Officers (PEOs) are authorized to operate the 101 vehicles, including the eight Parking Enforcement vehicles equipped with ALPR (3 boot vans; five sedans). A Parking Enforcement Supervisor monitors and manages access to the AutoVu ALPR system for parking enforcement purposes. Each shift, the Parking Enforcement Supervisor assigns deployment to Parking Enforcement Officers. Officers monitoring time-restricted parking focus their efforts solely on time-restricted zones (e.g., digital chalking), while officers enforcing Scofflaw with the boot vans canvas the City (these vehicles do not chalk).

Parking Enforcement ALPR data collected by Scofflaw enforcement boot vans is stored with Patrol ALPR data in the Neology Back Office System Software (BOSS). The BOSS ALPR administrator is a member of the Technical and Electronic Support Unit (TESU), a unit within SPD that maintains administrative control of much of SPD's physical technology. The unit staff is knowledgeable about investigative and forensic technology. (See ALPR: Patrol SIR for more detailed description of BOSS).

3.0 USE GOVERNANCE

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities are bound by restrictions specified in the Surveillance Ordinance and Privacy Principles and must provide written procedures for how the entity will comply with any restrictions identified.

3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

Prior to gaining access to the ALPR system, potential users must be trained by other trained SPD Parking Enforcement officers. Once this training has been verified with the Parking Enforcement Supervisor, users are given access and must log into the system with unique login and password information whenever they employ the technology. They remain logged into the system the entire time that the ALPR system is in operation. The login is logged and auditable.

Parking Enforcement Officers are assigned the vehicles to use while on-shift, as well as a specific zone to monitor for time-restricted parking violations.

3.2 List the legal standards or conditions, if any, that must be met before the project / technology is used.

For example, the purposes of a criminal investigation are supported by reasonable suspicion.

Parking Enforcement systems, including ALPR, can be used at any time.

Parking enforcement is governed by Seattle's Traffic Code and Seattle's Scofflaw Ordinance. SPD ALPR systems can be used during routine patrol or specific to a criminal investigation (i.e., to locate a stolen vehicle), as per SPD Policy 16.170. The policy specifies that the ALPR system administrator will be a member of the Technical and Electronic Support Unit (TESU). It further requires that users must be trained; they must be certified in A Central Computerized Enforcement Service System (ACCESS) – a computer controlled communications system maintained by Washington State Patrol that extracts data from multiple repositories, including Washington Crime Information Center, Washington State Identification System, the National Crime Information Center, the Department of Licensing, the Department of Corrections Offender File, the International Justice and Public Safety Network, and PARKS - and trained in the proper use of ALPR. In addition, the policy limits* use of the technology to strictly routine patrol or criminal investigation. Further, the policy clarifies that users may only access ALPR data when that data relates to a specific criminal investigation**. Records of these requests are purged after 90 days.

Policy Update

*the policy limits use of ALPR to the "search of specific or partial plate(s) and/or vehicle identifiers as related to: a crime in progress, a search of a specific area as it relates to a crime in-progress, a criminal investigation, a search for a wanted person, or community caretaking functions such as locating an endangered or missing person."

** and will complete a "Read Query" justification form documenting the search and applicable case number.

3.3 Describe the policies and training required of all personnel operating the project / technology, and who has access to ensure compliance with use and management policies.
Include links to all policies referenced.

SPD Policy 16.170 addresses Automatic License Plate Readers. The policy requires that users must be trained; they must be certified in A Central Computerized Enforcement Service System (ACCESS) – a computer controlled communications system maintained by Washington State Patrol (WSP) that extracts data from multiple repositories, including Washington Crime Information Center, Washington State Identification System, the National Crime Information Center, the Department of Licensing, the Department of Corrections Offender File, the International Justice and Public Safety Network, and PARKS - and trained in the proper use of ALPR.

Parking Enforcement officers are trained in the use of parking enforcement systems by trained Parking Enforcement Officers.

Compliance oversight is conducted by the Parking Enforcement supervisor.

Policy Update

By policy, SPD instruction on ALPR technology will include the appropriate use and collection of ALPR data with emphasis on the requirement to document the reason for any data inquiry. The training will also include any Surveillance Impact Reporting regarding ALPR adopted by the City Council.

THE ALPR Administrators will update access for approved, trained users. Also the ALPR administrator will assist the Office of Inspector General in conducting periodic audits of the Department's ALPR systems.

4.0 DATA COLLECTION AND USE

Provide information about the policies and practices around the collection and use of the data collected.

4.1 Provide details about what information is being collected from sources other than an individual, including other IT systems, systems of record, commercial data aggregators, publicly available data and/or other city departments.

Data collected from ALPR include license plate image, computer-interpreted read of the license plate number, date, time, and GPS location. ALPR on Parking Enforcement vehicles, takes a burst of 26 pictures of each parked vehicle, for visual photo comparison when the same vehicle is later examined for time zone violation.

All ALPR-equipped vehicles upload a daily HotList that contains only license plate numbers, with the associated states, of stolen vehicles from NCIC and WASIC. The information downloaded will come from the NCIC hot file via ACCESS, currently managed by the Washington State Patrol (WSP). NCIC contains national stolen vehicle and plate data published daily by the FBI. The WSP places the NCIC file on a server available through ACCESS to those agencies that have a specific and signed agreement with WSP to access and use the information. SPD may supplement the list with additional information, such as vehicles sought in connection with an SPD criminal investigation.

Parking Enforcement vehicles equipped with ALPR are linked to the HotList; however, they take no action on hits generated from the list and request assistance from sworn officer(s). The Parking Enforcement Officer then returns to focusing on vehicles in violation of parking ordinances.

Boot van users connect to Bootview, a software program that contains information about individuals in Scofflaw. This list is created, and provided to Bootview, by Seattle Municipal Court. To be in scofflaw violation, a vehicle must have acquired four or more overdue, unpaid parking tickets and they must be found in the public-right-of-way. Booting is required whether a car is found parked illegally or legally.

When a user in a boot van receives a hit that a vehicle is in violation of scofflaw, s/he accesses Bootview to determine the most updated information about the scofflaw status. This system reports identifying information about the vehicle (license plate number, make, model, color) and information about past violations, as well as current information as to whether prior warnings or tickets have been issued. The hit from the Scofflaw list, coupled with the supporting information from Bootview helps users to determine whether to take action, which could include issuing a warning or booting a vehicle. Parking Enforcement also manages the Scofflaw Mitigation Program, in which officers assess scofflaw vehicles that appear to be lived-in vehicles and, in lieu of booting, provide contact information to assist individuals with payment of past-due fines, so as not to exacerbate a difficult situation.

4.2 What measures are in place to minimize inadvertent or improper collection of data?

When the ALPR system registers a hit, the user must verify accuracy before taking any action. In Parking Enforcement, users verify first that a vehicle hit for Scofflaw violation is still actively in violation by checking for updated information in Bootview before booting a vehicle. Parking Enforcement Officers then visually verify that a vehicle suspected of time-zone restriction or metered parking violation is, in fact, in violation prior to issuing a ticket. Images captured serve as "evidence" that the system and the user are not in error.

Unless a hit has been exported for investigation and exported from the database for this purpose, all data captured by the five ALPR-equipped parking enforcement sedans is retained in the same database as ALPR data collected by ALPR-equipped patrol vehicles and is retained until automatically deleted after 90 days, per department retention policy (see ALPR Surveillance Impact Report).

Unless a hit has been exported for booting or investigation and exported for this purpose, all data captured by boot van ALPR is deleted when the Parking Enforcement Officer logs off the system at the end of shift.

4.3 How and when will the project / technology be deployed or used? By whom? Who will determine when the project / technology is deployed and used?

Parking Enforcement is in operation Monday-Saturday, and with limited staffing on Sundays, for the purposes outlined above (see 1.0).

4.4 How often will the technology be in operation?

This technology may be used at any time, and on any day, during any given year.

Policy Update

***Policy 16.170 has been significantly updated and updates are reflected below:**

16.170-POL – 3 ALPR Equipment
1. ALPR Operators Will Ensure ALPR Cameras Are Properly Affixed to the Assigned Police Vehicle Prior to the Start of Their Shift
Operators will inspect cameras for damage or excessive wear.
2. Operators Will Notify the ALPR Administrator Upon Discovery of any Damaged or Inoperable ALPR Equipment
Operators will document the damage/issue on the Vehicle Damage Report form 1_35 found in Word Templates.
3. Operators Will Activate the ALPR Software and Receive the Automatic Updated Hot List at the Start of Each Shift
ALPR units installed on marked patrol and PEO vehicles will be activated and used at all times unless the operator of the vehicle has not been trained.
4. Operators Will Ensure that the ALPR System is Operational by Confirming all Three Cameras and GPS are Functioning Properly at the Beginning of Their Shift
Operators will alert Seattle ITD and the ALPR administrator of any equipment defects.
5. Operators Will Upload, Their ALPR Data Accumulated from Their Shift to the BOSS Server Prior to Shutting Down Their Computer

4.5 What is the permanence of the installation? Is it installed permanently, or temporarily?

Temporary – while in operation.

4.6 Is a physical object collecting data or images visible to the public? What are the markings to indicate that it is in use? What signage is used to determine department ownership and contact information?

In Parking Enforcement vehicles, ALPR cameras are in plain view, and the vehicle itself is advertised as a Parking Enforcement vehicle.

4.7 How will data that is collected be accessed and by whom?

Please do not include staff names; roles or functions only.

All data collected for Parking Enforcement systems are hosted on City SPD servers and are not accessible by vendors without knowledge and/or permission of City personnel. Unlike some ALPR systems, SPD's systems do not "pool" SPD's ALPR data with that collected by other agencies.

Only authorized users can access the data collected by ALPR for Parking Enforcement. Also, all activity by users in the AutoVu ALPR system is logged and auditable.

Data removed from the system/technology and entered into investigative files is securely input and used on SPD's password-protected network with access limited to authorized SPD personnel.

All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.

4.8 If operated or used by another entity on behalf of the city, provide details about access, and applicable protocols. Please link memorandums of agreement, contracts, etc. That are applicable.

Access to the Parking Enforcement ALPR system is limited to ALPR-trained parking enforcement officers, the Parking Enforcement Supervisor, authorized SPD administrators, and authorized Seattle City IT administrators.

4.9 What are acceptable reasons for access to the equipment and/or data collected?

Users can only access the equipment and systems for purposes earlier outlined (see 1.0 above) – Scofflaw, parking enforcement, and criminal investigations.

Policy Update

* ALPR systems will only be deployed for official law enforcement purposes. These deployments are limited to:

- Locating stolen vehicles;
- Locating stolen license plates;
- Locating wanted, endangered or missing persons; or those violating protection orders;
- Canvassing the area around a crime scene;
- Locating vehicles under SCOFFLAW; and
- Electronically chalking vehicles for parking enforcement purposes.

ALPR data maintained on BOSS will only be accessed by trained, SPD employees for official law enforcement purposes. This access is limited to:

- Search of specific or partial plate(s) and/or vehicle identifiers as related to:
- A crime in-progress;
- A search of a specific area as it relates to a crime in-progress;
- A criminal investigation; or
- A search for a wanted person; or
- Community caretaking functions such as, locating an endangered or missing person.

Officers/detectives conducting searches in the system will complete the Read Query screen documenting the justification for the search and applicable case number.

ALPR will not be used to intentionally capture images in private area or areas where a reasonable expectation of privacy exists, nor shall it be used to harass, intimidate or discriminate against any individual or group.

4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) and to provide an audit trail (viewer logging, modification logging, etc.)?

Individuals can only access the Parking Enforcement AutoVu ALPR system via unique login credentials. Hardware systems can only be accessed in-vehicle (which are assigned by superiors for each shift), and Parking Enforcement software systems can only be accessed in-vehicle or on-site of SPD. As previously noted, all activity in the systems is logged and can be audited.

Further, City IT manages SQL on the system's backend that purges ALPR data at the required intervals (90 days). A record of the purge is generated and accessible at any time for verification of purges.

5.0 DATA STORAGE, RETENTION AND DELETION

5.1 How will data be securely stored?

All data collected from SPD's ALPR systems is stored, maintained, and managed on premises. Retention is automated, so that all ALPR data from the three ALPR-equipped Parking Enforcement boot vans is retained in the same BOSS database as ALPR data collected by ALPR-equipped patrol vehicles and is retained until automatically deleted after 90 days per department retention policy unless a record is identified as being related to a parking violation or criminal investigation and exported in support of that citation or investigation (see ALPR: Patrol SIR for further detail). All data collected from the five ALPR-equipped Parking Enforcement sedans is deleted from the vehicle on-board system when the Parking Enforcement Officer logs off the at the end of the shift.

Unless a record is identified as being related to a parking violation or criminal investigation and exported in support of that matter, all data collected from the five ALPR-equipped Parking Enforcement sedans is deleted from the vehicle on-board system when the Parking Enforcement Officer logs off the at the end of the shift. No data from those sedans is retained by SPD except for records identified as being related to a parking violation or criminal investigation and exported during the shift it was captured.

Parking Enforcement systems that are contracted by SPD include only PCS Mobile's Patroller and Gtechna. Data collected by Patroller and Gtechna are hosted on City SPD servers.

5.2 How will the owner allow for departmental and other entities, to audit for compliance with legal deletion requirements?

Systems utilized by Parking Enforcement keep logs of access and action. The Office of Inspector General may access all data and audit for compliance at any time.

5.3 What measures will be used to destroy improperly collected data?

Any citations issued by a Parking Enforcement Officer or booting for scofflaw violation can be contested by individuals. Users may make notes in records about license plate data captured that reflects that the hit is a misread, or that the hit was in error.

All information must be gathered and recorded in a manner that is consistent with SPD Policy 6.060, such that it does not reasonably infringe upon "individual rights, liberties, and freedoms guaranteed by the Constitution of the United States and the State of Washington, including freedom of speech, press, association, and assembly; liberty of conscience the exercise of religion; the right to petition government for redress of grievances; and the right to privacy."

All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

5.4 Which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

Seattle City IT, in conjunction with SPD's Enforcement Supervisor, are responsible for ensuring compliance with data retention requirements. Additionally, external audits by OIG can review and ensure compliance, at any time.

6.0 DATA SHARING AND ACCURACY

6.1 Which entity or entities inside and external to the city will be data sharing partners?

Data obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law. Seattle's Scofflaw Ordinance and Traffic Code require that SPD share information with Seattle Municipal Court.

Data may be shared without outside entities in connection with criminal prosecutions:

- Seattle City Attorney's Office
- King County Prosecuting Attorney's Office
- King County Department of Public Defense
- Private Defense Attorneys
- Seattle Municipal Court
- King County Superior Court
- Similar entities where prosecution is in Federal or other State jurisdictions

Data may be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

Discrete pieces of data collected by the parking enforcement systems may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by SPD Policy 12.050 and 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayor's Directive, dated February 6, 2018.

SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the parking enforcement systems.

6.2 Why is data sharing necessary?

Data sharing is necessary for SPD to fulfill its mission as a law enforcement agency and to comply with legal requirements.

6.3 Are there any restrictions on non-city data use?

Yes ☒ No ☐

6.3.1 If you answered Yes, provide a copy of the department's procedures and policies for ensuring compliance with these restrictions.

Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

Once disclosed in response to PRA request, there are no restrictions on non-City data use; however, applicable exemptions will be applied prior to disclosure to any requestor who is not authorized to receive exempt content.

6.4 How does the project/technology review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?

Please describe the process for reviewing and updating data sharing agreements.

Research agreements must meet the standards reflected in SPD Policy 12.055. Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

Following Council approval of the SIR, SPD must seek Council approval for any material change to the purpose or way the parking enforcement systems may be used.

6.5 Explain how the project/technology checks the accuracy of the information collected. If accuracy is not checked, please explain why.

Parking Enforcement systems technologies do not check themselves for errors. This is because the systems are unaware that they are gathering incorrect data. Instead, users are trained to visually verify accuracy (i.e., comparing a license plate hit from the system to the physical plate that the system read before taking any action). If they note a misread, they can enter a note into the system recognizing the read, as such. If they cannot verify visually, no action is taken.

Individuals can challenge citations, alleged scofflaw violations, or criminal charges and provide correct information.

6.6 Describe any procedures that allow individuals to access their information and correct inaccurate or erroneous information.

Individuals would not know that their information is collected inaccurately or erroneously in the normal course of ALPR data reading. This would only come to an individual's attention if a user acts on a hit received.

As it pertains to parking enforcement, individuals may contest booting action or a parking violation, and argue that the action was taken based on inaccurate or erroneous information, through the normal course of municipal proceedings.

Individuals may request records pursuant to the PRA, and individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

7.0 LEGAL OBLIGATIONS, RISKS AND COMPLIANCE

7.1 What specific legal authorities and/or agreements permit and define the collection of information by the project/technology?

ALPR use is not legally constrained at the local, state, or federal level. Instead, retention of data is restricted. Data collected by ALPR-equipped Parking Enforcement sedans other than that related to an alleged scofflaw violation or criminal investigation is deleted at the end of a Parking Enforcement Officer's shift. SPD has designated 90 days as the retention period for ALPR data from the three ALPR-equipped Parking Enforcement boot vans and the eleven ALPR-equipped patrol vehicles data that is not case specific (i.e., related to an investigation).

Parking Enforcement is authorized and mandated by Seattle's Traffic Code and Seattle's Scofflaw Ordinance.

7.2 Describe what privacy training is provided to users either generally or specifically relevant to the project/technology.

Users are trained in how to use the parking enforcement and ALPR systems and how to properly access data by other trained Parking Enforcement Officers. The Parking Enforcement Supervisor confirms the training before providing access to new users.

SPD Policy 12.050 mandates that all employees, including Parking Enforcement Officers, who use terminals that have access to information in WACIC/NCIC files, must be certified by completing complete Security Awareness Training (Level 2) with recertification testing required every two years, and all employees also complete City Privacy Training. Failure to comply with ACCESS/NCIC/WACIC user requirements can result in termination of the right to continue using ACCESS services.

7.3 Given the specific data elements collected, describe the privacy risks identified and for each risk, explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

As it relates to ALPR, each component of data collected, on its own, does not pose a privacy risk. Paired with other known or auditable information, however, an individual may be able to personally identify owners of vehicles, and then use that information to determine, to a certain degree, where specific vehicles have been located. Because SPD's ALPR cameras are not fixed in location, vehicles equipped with ALPR generally do not follow the same routes, and records are only retained for 90 days, this privacy risk is mitigated somewhat, as vehicle patterns more difficult to identify.

Per SPD Policy 16.170, all users of ALPR are restricted from accessing the data, except as it relates to a specific criminal investigation. Appropriate SPD personnel can access the data (assuming it is within the 90-day retention period) as it relates to the active investigation.

Any activity by a user to access this information is logged and auditable. Washington State's Public Records Act requires release of collected ALPR data, however, making it possible for members of the public to make those identification connections on their own if they have access to the information necessary to do so, such as an independent knowledge of an individual's license plate number.

7.4 Is there any aspect of the project/technology that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?

Data collected by ALPR may cause the most concern, as it relates to Parking Enforcement. As mentioned in 7.3, the data could be used to personally identify individuals; however, SPD policy prohibits the use of data collected by ALPR to be used in any capacity by SPD personnel beyond its relation to a specific criminal investigation or parking enforcement action. Additionally, all collected Parking Enforcement from ALPR-equipped sedans is deleted when the Parking Enforcement Officer logs off the system at the end of shift, and all other collected ALPR data that is not relevant to an active investigation is deleted 90 days after collection.

8.0 MONITORING AND ENFORCEMENT

8.1 Describe how the project/technology maintains a record of any disclosures outside of the department.

Data collected by Parking Enforcement Systems is only disclosed pursuant to the public under the PRA. The only data available for disclosure is that data which remains in the system within the 90-day retention window.

Discrete pieces of data collected by ALPR may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by SPD Policy 12.050 and SPD Policy 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayor's Directive, dated February 6, 2018. SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the devices.

Per SPD Policy 12.080, the Crime Records Unit is responsible to receive and record all requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies." Any requests for disclosure are logged by SPD's Crime Records Unit or Legal Unit, as appropriate. Any action taken, and data released subsequently, is then tracked through the request log. Responses to Public Disclosure Requests, including responsive records provided to a requestor, are retained in SPD's GovQA system for two years after the request is completed.

8.2 What auditing measures are in place to safeguard the information, and policies that pertain to them, as well as who has access to the audit data? Explain whether the project/technology conducts self-audits, third party audits or reviews.

Parking Enforcement Systems, including ALPR, do not self-audit. Instead, third party audits exist, as follows: 1) The Parking Enforcement Supervisor has the responsibility of managing the user list and ensuring proper access to the system; 2) The Office of the Inspector General (OIG) can also conduct an audit at any time. Violations of policy may result in referral to Office of Professional Accountability (OPA).

FINANCIAL INFORMATION

PURPOSE

This section provides a description of the fiscal impact of the surveillance technology, as required by the Surveillance Ordinance.

1.0 FISCAL IMPACT

Provide a description of the fiscal impact of the project/technology by answering the questions below.

1.1 Current or potential sources of funding: initial acquisition costs.

Current ☒ Potential ☐

Date of Initial Acquisition	Date of Go Live	Direct Initial Acquisition Cost	Professional Services for Acquisition	Other Acquisition Costs	Initial Acquisition Funding Source
2012/2013 (Genetec)	2012/2013	$18,085.050			SPD Budget
2014 (Gtechna)	2014	$529,769.99			SPD Budget
2016 (PCS Mobile)	2016	$263,123.68			SPD Budget

Notes:

These fiscal totals reflect the invoiced totals for the year of system/technology acquisition.

1.2 Current or potential sources of funding: on-going operating costs, including maintenance, licensing, personnel, legal/compliance use auditing, data retention and security costs.

Current ☒ Potential ☐

Annual Maintenance and Licensing	Legal/compliance, audit, data retention and other security costs	Department Overhead	IT Overhead	Annual Funding Source
$162,628.00				SPD Budget

Notes:

N/A

1.3 Cost savings potential through use of the technology.

These are not quantified; however, potential cost savings may result from enhanced Parking Enforcement Officer efficiency. It may reduce distractions for Parking Enforcement Officers while driving because they do not have to visually scan chalk marks or license plates while driving.

1.4 Current or potential sources of funding including subsidies or free products offered by vendors or governmental entities.

N/A

EXPERTISE AND REFERENCES

PURPOSE

The following information is provided to ensure that Council has a group of experts to reference while reviewing the completed Surveillance Impact Report ("SIR"). Any individuals or agencies referenced must be made aware ahead of publication that their information has been included. All materials must be available for Council to access or review, without requiring additional purchase or contract.

1.0 OTHER GOVERNMENT REFERENCES

Please list any other government bodies that have implemented this technology and can speak to the implementation of this technology.

Agency, Municipality, etc.	Primary Contact	Description of Current Use
Multiple Municipalities utilize different configurations of systems for parking enforcement		

2.0 ACADEMICS, CONSULTANTS, AND OTHER EXPERTS

Please list any experts in the technology under consideration, or in the technical completion of the service or function the technology is responsible for.

Agency, Municipality, etc.	Primary Contact	Description of Current Use
Bryce Newell, PhD	Brycenewell@uky.edu	"Transparent Lives and the Surveillance State: Policing, New Visibility, and Information Policy" – A Dissertation

3.0 WHITE PAPERS OR OTHER DOCUMENTS

Please list any authoritive publication, report or guide that is relevant to the use of this technology or this type of technology.

Title	Publication	Link
Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement	US Department of Justice (federally-funded grant report)	https://www.ncjrs.gov/pdffiles1/nij/grants/239604.pdf
License Plate Readers for Law Enforcement: Opportunities and Obstacles	Rand Corporation	https://www.ncjrs.gov/pdffiles1/nij/grants/247283.pdf
Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information	66 Maine Law Review 398, 2014 Bryce Clayton Newell	https://cpb-us-w2.wpmucdn.com/wpsites.maine.edu/dist/d/46/files/2014/06/03-Newell.pdf

RACIAL EQUITY TOOLKIT AND ENGAGEMENT FOR PUBLIC COMMENT WORKSHEET

PURPOSE

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit ("RET").

1. To provide a framework for the mindful completion of the Surveillance Impact Reports in a way that is sensitive to the historic exclusion of vulnerable and historically underrepresented communities. Particularly, to inform the public engagement efforts Departments will complete as part of the Surveillance Impact Report.
2. To highlight and mitigate any impacts on racial equity from the adoption and the use of the technology.
3. To highlight and mitigate any disparate impacts on individuals or vulnerable communities.
4. To fulfill the public engagement requirements of the Surveillance Impact Report.

ADAPTION OF THE RET FOR SURVEILLANCE IMPACT REPORTS

The RET was adapted for the specific use by the Seattle Information Technology Departments' ("Seattle IT") Privacy Team, the Office of Civil Rights ("OCR"), and Change Team members from Seattle IT, Seattle City Light, Seattle Fire Department, Seattle Police Department, and Seattle Department of Transportation.

RACIAL EQUITY TOOLKIT OVERVIEW

RACIAL EQUITY TOOLKIT: TO ASSESS POLICIES, INITIATIVES, PROGRAMS, AND BUDGET ISSUES

The vision of the Seattle Race and Social Justice Initiative is to eliminate racial inequity in the community. To do this requires ending individual racism, institutional racism and structural racism. The Racial Equity Toolkit lays out a process and a set of questions to guide the development, implementation and evaluation of policies, initiatives, programs, and budget issues to address the impacts on racial equity.

WHEN DO I USE THIS TOOLKIT?

Early. Apply the toolkit early for alignment with departmental racial equity goals and desired outcomes.

HOW DO I USE THIS TOOLKIT?

With inclusion. The analysis should be completed by people with different racial perspectives.

Step by step. The Racial Equity Analysis is made up of six steps from beginning to completion:

Please refer to the following resources available on the Office of Civil Rights' website here: Creating effective community outcomes; Identifying stakeholders & listening to communities of color; Data resources

1.0 SET OUTCOMES

1.1. Seattle city council has defined the following inclusion criteria in the surveillance ordinance, and they serve as important touchstones for the risks departments are being asked to resolve and/or mitigate. Which of the following inclusion criteria apply to this technology?

☐ The technology disparately impacts disadvantaged groups.

☐ There is a high likelihood that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service.

☒ The technology collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection.

☐ The technology raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice.

1.2 What are the potential impacts on civil liberties through the implementation of this technology?

Without appropriate policy, license plate data could be paired with other identifiable information about individuals that could be used to identify individuals without reasonable suspicion of having committed a crime, or to data mine for information that is not incidental to any active investigation. SPD Policy 16.170 mitigates this concern by limiting operation to solely routine patrol, criminal investigations, or community caretaking functions.

An additional potential civil liberties concern is that the SPD would over-surveil vulnerable or historically targeted communities, deploying ALPR to diverse neighborhoods more often than to other areas of the City.

1.3 What does your department define as the most important racially equitable community outcomes related to the implementation of this technology?

Trust in SPD is affected by its treatment of all individuals. Equity in treatment, regardless of actual or perceived race, gender, sex, sexual orientation, country of origin, religion, ethnicity, age, and ability is critical to establishing and maintaining trust.

Per the 2016 Race and Social Justice Initiative Community Survey, measuring "the perspectives of those who live, work, and go to school in Seattle, including satisfaction with City services, neighborhood quality, housing affordability, feelings about the state of racial equity in the city, and the role of government in addressing racial inequities," 56.1% of African American/Black respondents, 47.3% of Multiracial respondents, and 47% of Indian/Alaska Native respondents have little to no confidence in the police to do a good job enforcing the law, as compared with 31.5% of White respondents. Further, while 54.9% of people of color have a great deal or fair amount of confidence in the police to treat people of color and White people equally, 45.1% of people of color have little to no confidence in the police to treat people equitably. This is contrasted with White respondents, of which 67.5% have a great deal or fair amount of confidence in the police to treat people of color and White people equally. This may be rooted in feelings of disparate types of contact with the police, across racial groups. While 14.3% of White respondents, 14.7% of Asian/Pacific Islander respondents, and 16.7% of Latino/Hispanic respondents reported being questioned by the police, charged, or arrested when they had not committed a crime, some communities of color reported much higher rates (American Indian/Alaska Native -52.7%; Black/African American - 46.8%; and Multiracial - 36.8%) of this type of contact with the criminal justice system.

As it relates to ALPR, it is important that SPD continue to follow its policy of limiting use of the technology to strictly routine patrol or criminal investigation, as well as limiting access to ALPR data to only instances in which it relates to a specific criminal investigation. Further, continuing to audit the system on a regular basis, provides a measure of accountability. In doing so, SPD can mitigate the appearance of disparate treatment of individuals based on factors other than true criminal activity.

The desired outcome is to ensure that Parking Enforcement occurs throughout the City equitably in areas where parking restrictions exist, without over-surveilling areas where historically targeted communities reside or congregate.

1.4 What racial equity opportunity area(s) will be affected by the application of the technology?

- ☐ Education
- ☐ Community Development
- ☐ Health
- ☐ Environment
- ☒ Criminal Justice
- ☐ Jobs
- ☐ Housing
- ☐ Other

1.5 Are there impacts on:

- ☐ Contracting Equity
- ☐ Workforce Equity
- ☐ Immigrant and Refugee Access to Services
- ☐ Inclusive Outreach and Public Engagement
- ☐ Contracting Equity
- ☐ Workforce Equity
- ☐ Immigrant and Refugee Access to Services
- ☐ Inclusive Outreach and Public Engagement

☒ Other

2.0 INVOLVE STAKEHOLDERS, ANALYZE DATA

2.1 Departmental conclusions about potential neighborhood impacts of the technology. Are the impacts on geographic areas?

☒ Yes ☐ No

Check all neighborhoods that apply *(see map of neighborhood boundaries in Appendix A: Glossary, under "Seattle Neighborhoods"):*

☒ All Seattle neighborhoods

☐ Ballard
☐ North
☐ Northeast
☐ Central
☐ Lake Union
☐ Southwest
☐ Southeast
☐ Delridge
☐ Greater Duwamish
☐ East District
☐ King County (outside Seattle)

☐ Outside King County. Please describe:

N/A

2.2 What are the racial demographics of those living in the area or impacted by the issue?
(see Stakeholder and Data Resources here.)

The demographics for the City of Seattle: White - 69.5%; Black or African American - 7.9%; Amer. Indian & Alaska Native - 0.8%; Asian - 13.8%; Native Hawaiian & Other Pac. Islander - 0.4; Other race - 2.4%; Two or more races - 5.1%; Hispanic or Latino ethnicity (of any race): 6.6%; Persons of color: 33.7%.

STOP: Department should complete RET questions 2.3 – 6 and Appendices B-I AFTER completing their public comment and engagement requirements.

2.3 Have you completed the following steps to engage the public?
If you have not completed these steps, pause here until public outreach and engagement has been completed. (*See OCR's RET worksheet here for more information about engaging the public at this point in the process to ensure their concerns and expertise are part of analysis.*)

☒ **Create a public outreach plan.** Residents, community leaders, and the public were informed of the public meeting and feedback options via:

- ☒ Email
- ☐ Mailings
- ☐ Fliers
- ☒ Phone calls
- ☒ Social media
- ☐ Other

☐ The following community leaders were identified and invited to the public meeting(s):

- ☒ American Civil Liberties Union (ACLU)
- ☒ CARE
- ☒ Northwest Immigrant Rights
- ☒ OneAmerica
- ☒ JACL
- ☒ For Seattle Police Department only, Community Police Commissions
- ☐ Other:

[Please describe]

☒ **Engagement for Public Comment #1**

Date of meeting: 10/22/18

Location of meeting: Columbia City Branch Library

Summary of discussion:

See Appendix B for an overview of comments received, and demographics on attendees. See Appendix E for the transcript of all comments received for this technology.

☒ **Engagement for Public Comment #2**

Date of meeting: 10/29/18

Location of meeting: Bertha Knight Landes Room

Summary of discussion:

See Appendix B for an overview of comments received, and demographics on attendees. See Appendix E for the transcript of all comments received for this technology.

☒ **Engagement for Public Comment #3 (if applicable)**

Date of meeting: 10/30/18

Location of meeting: Greenlake Branch Library

Summary of discussion:

See Appendix B for an overview of comments received, and demographics on attendees. See Appendix E for the transcript of all comments received for this technology.

☒ **Collect public feedback via mail and email**

Number of feedback submissions received: 2

Summary of feedback: See Appendix B for an overview of comments received, and demographics on attendees. See Appendix E for the transcript of all comments received for this technology.

Open comment period: October 8, 2018 – November 5, 2018

☐ **Community Technology Advisory Board (CTAB) Presentation**

Date of presentation: N/A

Summary of comments:

N/A

☐ Complete meeting minutes and comments are attached an as an appendix to the SIR

☐ Any letters of feedback by CTAB members are attached as an appendix to the SIR

2.4 What does data and conversations with stakeholders tell you about existing racial inequities that influence people's lives and should be taken into consideration when applying/implementing/using the technology?

(See OCR's RET worksheet here for more information; King County Opportunity Maps are a good resource for information based on geography, race, and income.)

SPD has heard concerns that our ALPR data will be shared with other agencies and governments that do not share Seattle's values. Community members have expressed concern that ALPR data will be used for purposes other than law enforcement. SPD has also heard that community members may be concerned that ALPR may be used to track movement of people around sensitive areas, such as local mosques, and may be used to infringe upon people's First Amendment rights.

2.5 What are the root causes or factors creating these racial inequities?

Mitigation strategies will be addressed in 4.1 and 5.3. *Examples: bias in process; lack of access or barriers; lack of racially inclusive engagement.*

Root causes are related to historical over-surveillance and over-enforcement of minor violations in neighborhoods and areas where historically targeted communities reside or congregate.

3.0 DETERMINE BENEFIT AND/OR BURDEN

Provide a description of any potential disparate impact of surveillance on civil rights and liberties on communities of color and other marginalized communities. Given what you have learned from data and from stakeholder involvement…

3.1 How will the technology, or use of the technology increase or decrease racial equity?

What are potential unintended consequences? What benefits may result? Are the impacts aligned with your department's community outcomes that were defined in 1.0?

ALPR is content-neutral; it does not identify the race of the driver or the registered owner of the vehicle. However, SPD must continue to follow its policy of limiting use of the technology to strictly routine parking enforcement as well as continuing to delete all data collected by the parking enforcement ALPR vehicles at the end of a parking enforcement officer's shift. SPD must also continue to ensure that all ALPR data collected by the ALPR scofflaw vehicles is used for legitimate law-enforcement purposes. Further, continuing to audit the system on a regular basis provides a measure of accountability. In doing so, SPD can ensure that parking enforcement occurs throughout the City equitably in areas where parking restrictions exist, without over-surveilling areas where historically targeted communities reside or congregate.

3.2 What benefits to the impacted community/demographic may result?

Parking enforcement systems assist the City in managing traffic flow and parking assets, and in recouping revenue lost to parking violations. Because SPD deploys the parking enforcement ALPRs throughout the City, SPD ensures that parking enforcement is occurring equitably throughout all City neighborhoods.

3.3 What are potential unintended consequences (both negative and positive potential impact)?

SPD does not collect data on the demographics of the vehicle owners or operators, so unintended consequences may be difficult to determine. However, because ALPR is deployed equitably throughout the City, all City neighborhoods benefit from the use of ALPRs. SPD will continue to allocate ALPRs to neighborhoods with RPZ and time-limited parking to ensure that overuse of ALPRs is not occurring in neighborhoods where historically targeted communities reside or congregate.

3.4 Are the impacts aligned with your department's community outcomes that were defined in step 1.0?

Yes. The desired outcome is to ensure that Parking Enforcement occurs throughout the City equitably in areas where parking restrictions exist, without over-surveilling areas where historically targeted communities reside or congregate.

4.0 ADVANCE OPPORTUNITY OR MINIMIZE HARM

Provide a mitigation plan for the impacts described in step 3.

4.1 How will you address the impacts (including unintended consequences) on racial equity?
What strategies address immediate impacts? What strategies address root causes of inequity listed in 2.5? How will you partner with stakeholders for long-term positive change? If impacts are not aligned with desired community outcomes for surveillance technology (see 1a), how will you re-align your work?

Program Strategies:

SPD will ensure that is policies related to ALPR and Foreign Nationals are up-to-date and will ensure that all SPD employees comply with the Mayoral Directive, dated February 6, 2018. SPD will also continue to comply with SMC 14.18, the City's Intelligence Ordinance, and ensure that law enforcement personnel shall not "unreasonably infringe upon individuals, rights, liberties and freedoms guaranteed by the Constitution of the United States."

Policy Strategies:

SPD recognizes that its current ALPR policy needs updating and anticipates that an updated policy will be in place by January 31, 2019*. Further, SPD complies with the Mayoral Directive dated February 6, 2018, requiring all City departments to seek approval from the Mayor's Office before sharing data and information with ICE. In addition, SPD has recently updated its policy related to Foreign Nationals, emphasizing that SPD has no role in immigration enforcement and will not inquire about any person's immigration status. In addition, SPD welcomes the OIG to audit its use of ALPR technologies.

Policy Update

*Through the course of the completion of this Surveillance Impact Report, SPD recognized the need to update the existing ALPR Policy and on February 1, 2019 the new SPD ALPR policy went into effect. This new policy expanded on the previous by adding definitions of the terms used in the operation of the technology, expanding on the required training for employees prior to access and use of ALPR, detailing authorized and prohibited uses of ALPR, defining response to alerts, detailing how ALPR equipment is to be handled, detailing ALPR administrator roles, defining ALPR data storage and retention, and detailing policy around the release or sharing of ALPR data.

Partnership Strategies:

N/A

5.0 EVALUATE, RAISE RACIAL AWARENESS, BE ACCOUNTABLE

The following information must be provided to the CTO, via the Privacy Office, on an annual basis for the purposes of an annual report to the City Council on the equitable use of surveillance technology. For Seattle Police Department, the equity impact assessments may be prepared by the Inspector General for Public Safety.

The following information does not need to be completed in the SIR submitted to Council, unless this is a retroactive review.

5.1 Which neighborhoods were impacted/targeted by the technology over the past year and how many people in each neighborhood were impacted?

☒ All Seattle neighborhoods
☐ Ballard
☐ North
☐ NE
☐ Central
☐ Lake Union
☐ Southwest
☐ Southeast
☐ Greater Duwamish
☐ East District
☐ King County (outside Seattle)
☐ Outside King County. Please describe:

[Respond here, if applicable.]

5.2 Demographic information of people impacted/targeted by the technology over the past year.

To the best of the department's ability, provide demographic information of the persons surveilled by this technology. If any of the neighborhoods above were included, compare the surveilled demographics to the neighborhood averages and City averages.

ALPR does not collect demographic data about the owners or operators of cars that have been captured by the ALPR systems. ALPRs are dispatched throughout the city where parking limits, such as maximum hours or residential parking zones, exist. Because ALPRs are dispatched throughout, SPD ensures all of Seattle's neighborhoods receive the benefit of ALPR cars.

5.3 Which of the mitigation strategies that you identified in step 4 were implemented in the past year?
Specifically, what adjustments to laws and policies should be made to remedy any disproportionate impacts so as to achieve a more equitable outcome in the future.

Type of Strategy (program, policy, partnership)	**Description of Strategy**	**Percent complete of implementation**	**Describe successes and challenges with strategy implementation**
Updated ALPR Policy	Expanding and clarifying SPD's ALPR policies both for Parking Enforcement and Patrol	90%	
Updated Foreign Nationals Policy	Updated SPD policy related to Foreign Nationals	100%	

5.4 How have you involved stakeholders since the implementation/application of the technology began?

☒ Public Meeting(s)
☐ CTAB Presentation
☒ Postings to Privacy webpage seattle.gov/privacy
☒ Other external communications
☐ Stakeholders have not been involved since the implementation/application

5.5 What is unresolved? What resources/partnerships do you still need to make changes?

N/A

6.0 REPORT BACK

Responses to Step 5 will be compiled and analyzed as part of the CTO's Annual Report on Equitable Use of Surveillance Technology.

Departments will be responsible for sharing their own evaluations with department leadership, Change Team Leads, and community leaders identified in the public outreach plan (Step 2c).

PRIVACY AND CIVIL LIBERTIES ASSESSMENT

PURPOSE

This section shall be completed after public engagement has concluded and the department has completed the Racial Equity Toolkit section above. The Privacy and Civil Liberties Assessment is completed by the Community Surveillance Working Group ("Working Group"), per the Surveillance Ordinance which states that the Working Group shall:

> "*[p]rovide to the Executive and the City Council a privacy and civil liberties impact assessment for each SIR that must be included with any departmental request for surveillance technology acquisition or in-use approval. The impact assessment shall include a description of the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities. The CTO shall share with the Working Group a copy of the SIR that shall also be posted during the period of public engagement. At the conclusion of the public engagement period, the CTO shall share the final proposed SIR with the Working Group at least six weeks prior to submittal of the SIR to Council for approval. The Working Group shall provide its impact assessment in writing to the Executive and the City Council for inclusion in the SIR within six weeks of receiving the final proposed SIR. If the Working Group does not provide the impact assessment before such time, the Working Group must ask for a two-week extension of time to City Council in writing. If the Working Group fails to submit an impact statement within eight weeks of receiving the SIR, the department and City Council may proceed with ordinance approval without the impact statement.*"

WORKING GROUP PRIVACY AND CIVIL LIBERTIES ASSESSMENT

The Working Group's Privacy and Civil Liberties Impact Assessment (PCLIA) for this technology is below, and is also included in the Ordinance submission package, available as an attachment.

Please note, the Working Group's PCLIA for SPD's Parking Enforcement was part of a larger report which included reviews of additional retroactive surveillance technologies not applicable to this Council submission. As such, the Working Group's assessment for these technologies has been removed from this report, and will be made available in the appropriate SIRs, to be submitted to Council at a later date.

From: Seattle Community Surveillance Working Group (CSWG)
To: Seattle City Council

Date: April 23, 2019

Re Privacy and Civil Liberties Impact Assessment for ~~Automated License Plate Recognition~~, Parking Enforcement Systems, ~~and License Plate Readers~~

Executive Summary

On March 28th, 2019, CSWG received the Surveillance Impact Reports, or SIRs, for the three Automated License Plate Reader (ALPR) surveillance technologies included in Group 1 of the Seattle Surveillance Ordinance technology review process (Automated License Plate Recognition, Parking Enforcement Systems, and License Plate Readers). This document is CSWG's Privacy and Civil Liberties Impact Assessment for those technologies as set forth in SMC 14.18.080(B)(1), which we provide for inclusion in the final SIRs submitted to the City Councils.

This document first details the civil liberties concerns regarding ALPR surveillance technologies in general, and then provides specific concerns and recommendations for each of the three specific ALPR technologies under review.

Our assessment of the ALPR surveillance technologies focuses on three key issues:

1. The use of these systems and the data collected by them for purposes other than those intended.
2. Over-collection and over-retention of data.
3. Sharing of that data with third parties (such as federal law enforcement agencies).

For all three of these systems, the Council should adopt, via ordinance, clear and enforceable rules that ensure, at a minimum, the following:

1. The purposes of ALPR use must be clearly defined, and operation and data collected must be explicitly restricted to those purposes only.
2. Dragnet, suspicionless use of ALPR must be outlawed.
3. Data collected should be limited to license plate images, and no images of vehicles or occupants should be collected.
4. Data retention should be limited to the time needed to effectuate the purpose defined.
5. Data sharing with third parties must be limited to those held to the same restrictions as agency deploying the system.

Background: Civil Liberties Concerns with ALPR Systems

Automated License Plate Reader (ALPR) systems are powerful surveillance technologies that can significantly chill constitutionally protected activities by allowing the government to create a detailed picture of the movements—and therefore the lives—of a massive number of individuals. At the first public meeting seeking comment on the SPD Patrol ALPRs held on October 22, 2018, SPD stated that the ALPR system collects 37,000 license plates in a 24-hour period—which equates to over *13.5 million* scans over a full year. These drivers are not specifically suspected of any crime, which calls into question the scale and purpose of such data collection.

ALPR use creates a massive database of license plate information that allows agencies to comprehensively track and plot the movements of individual cars over time, even when the driver has not broken any law.[1] Such a database enables agencies, including law enforcement, to undertake widespread, systematic surveillance on a level that was never possible before. These surveillance concerns are exacerbated by long data retention periods because aggregate data becomes increasingly invasive and revealing when it is stored for long periods of time (as acknowledged by the U.S. Supreme Court in the *Carpenter* decision[2]). However, existing law in Seattle places no specific limits on the use of ALPR technology or data, meaning an agency can choose whether and how they want to retain data and track vehicle movements.

Currently, the use of ALPR technology in Seattle chills constitutionally protected activities because they can be used to target drivers who visit sensitive places such as centers of religious worship, protests, union halls, immigration clinics, or health centers. Whole communities can be targeted based on their religious, ethnic, or associational makeup, which is exactly what has happened in the United States and abroad. In New York City, police officers drove unmarked vehicles equipped with license plate readers near local mosques as part of a massive program of suspicionless surveillance of the Muslim community.[3] In the U.K., law enforcement agents installed over 200 cameras and license plate readers to target a predominantly Muslim community suburbs of Birmingham.[4] ALPR data obtained from the Oakland Police Department showed that police disproportionately deployed

ALPR-mounted vehicles in low-income communities and communities of color.[5] And the federal Immigration and Customs Enforcement (ICE) agency has sought access to ALPR data in order to target immigrants for deportation.[6]

The foregoing concerns suggest the Council should ensure strong protections in ordinance against the misuse of this technology, regardless of which agency is deploying it and for what purpose.

---

[1] https://www.eff.org/deeplinks/2013/05/alpr

[2] https://www.scotusblog.com/wp-content/uploads/2017/08/16-402-tsac-Scholars-of-Criminal-Procedure-and-Privacy.pdf

[3] https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques

[4] https://www.theguardian.com/uk/2010/jun/04/surveillance-cameras-birmingham-muslims

[5] https://www.eff.org/pages/automated-license-plate-readers-alpr

[6] https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/documents-reveal-ice-using-driver-location-data

Specific Comments and Recommendations

~~1. Automated License Plate Recognition (ALPR) (Patrol) (SPD)~~

~~The initial October 2018 Surveillance Impact Report (SIR) for this technology did not indicate the existence of clear policies imposing meaningful restrictions on the purposes for which ALPR data may be collected or used. The updated January 2019 SIR adds a November 2018 memo from SPD Deputy Chief Marc Garth Green (page 42), which states that SPD anticipates having an updated policy by January 31, 2019. The memo states:~~

> ~~"**New policies:** SPD recognizes that its current ALPR policy needs updating and anticipates that an updated ALPR policy will be in place by January 31, 2019. In addition, SPD has recently updated its policy related to Foreign Nationals, emphasizing that SPD has no role in immigration enforcement and will not inquire about any person's immigration status. In addition, SPD welcomes the OIG to audit its use of ALPR technologies and data."~~

~~Although the updated SIR (with the November 2018 memo addition) was conveyed to CSWG in March 2019, the SIR does not indicate whether or not the new policies mentioned in the November 2018 memo have already been adopted by SPD, nor include those policies.~~

~~Additional concerns regarding this technology are listed below. To address these concerns, we recommend that the Council ensure not only that the minimum rules listed above in the Executive Summary apply to ALPR-Patrol Systems by ordinance, but that the issues noted below with SPD's current policies are addressed as set forth in the corresponding recommendations, all of which should be incorporated into the Council's approval of the technology.~~

~~SPD's policy:~~

- ~~Does not impose meaningful restrictions on the purposes for which ALPR data may be collected or used.~~
  - ~~*Recommendation: SPD's policy must clearly define and meaningfully restrict the purposes for which ALPR data may be collected, accessed, and used. These purposes should be limited to checking vehicles against specified hotlists connected to specific criminal investigations. SPD must have reasonable suspicion that a crime has occurred (in the context of a specifically defined criminal investigation) before examining collected license plate reader data; they must not examine license plate reader data in order to generate reasonable suspicion. While SPD's ALPR policy says there must be a specific criminal investigation in order for ALPR data to be accessed, it does not describe how such an investigation is defined or documented.*~~
- ~~Does not justify SPD's 90-day retention period. SPD retains ALPR data for 90 days, but examples given in the SIR of crimes solved using ALPRs largely appear to involve immediate matches against a hotlist. We acknowledge that state law and technical considerations may impact this retention period.~~
  - ~~*Recommendation: SPD's policy must require a shorter retention period of 48 hours at most, during which time it must use the data for the specified purpose, then immediately delete the data. SPD should retain no information at all when a passing*~~

~~*vehicle does not match a hot list (particularly given that such data is subject to public disclosure, including to federal agencies).*~~

- ~~Does not limit data sharing by policy or statute. The sharing of ALPR data with other agencies is of great concern, and SPD states a variety of situations in which such data may be shared (see SIR Section 6.1). However, the policies cited do not make clear the criteria for such sharing, nor any inter-agency agreement that governs such sharing, nor why the data must be shared in the first place. The November 2018 memo only adds the statement, "SPD limits data-sharing with other law enforcement agencies for official law enforcement purposes," which does not address the concerns above.~~
    - ~~*Recommendation: SPD's policy must limit sharing of ALPR data to third parties that have a written agreement holding those third parties to the same use, retention, and access rules as SPD; make clear to whom and under what circumstances the data are disclosed; and make publicly available a list of what disclosures have been made to which third parties.*~~
- ~~Does not make clear whether and how audits of inquires to the system can be conducted (see SIR Sections 4.10 and 8.2, for example). The November 2018 memo does not add any new information.~~
    - ~~*Recommendation: SPD's policy must include a regular audit system to protect against abuse.*~~
- ~~Does not make clear how and to what degree Patrol and Parking Enforcement ALPR systems are separated, and whether SPD's policies on ALPR apply to the Parking Enforcement Systems (whose data may be equally prone to misuse).~~
    - ~~*Recommendation: SPD's policy must include strong protections against abuse that are applied to all ALPR systems.*~~
- ~~Does not include measures to minimize false matches.~~
    - ~~*Recommendation: SPD's policy must specific that whenever a hit occurs, an officer, before taking any action, must confirm visually that a plate matches the number and state identified in the alert, confirm that the alert is still active by calling dispatch and, if the alert pertains to the registrant of the car and not the car itself, for example in a warrant situation, develop a reasonable belief that the vehicle's occupant(s) match any individual(s) identified in the alert.*~~
- ~~Does not include systematic tracking to assess how many crimes each year are actually solved using ALPR data.~~
    - ~~*Recommendation: SPD's policy must require detailed records of ALPR scans, hits, and crimes solved specifically attributable to those hits, as well as an accounting of how ALPR use varies by neighborhood and demographic.*~~
- ~~Does not create clear restrictions on who can access the data.~~
    - ~~*Recommendation: SPD's policy must require access controls on the ALPR databases, with only agents who have been trained in the policies governing such databases permitted access, and with every instance of access logged.*~~

2. Parking Enforcement Systems (Including ALPR) (SPD)

As with the updated ALPR-Patrol SIR, the January 2019 Parking Enforcement Systems SIR includes a November 2018 memo from SPD Deputy Chief Marc Garth Green (page 39) stating that SPD anticipates having an updated policy by January 31, 2019. Again, although the updated SIR was conveyed to CSWG in March 2019, it does not indicate whether or not these new policies have already been adopted by SPD, nor address issues previously highlighted in public comment.

Particularly given the partly merged nature of the Parking Enforcement and Patrol ALPRs, including use of the Parking Enforcement ALPRs to check vehicle plates against hot lists, the concerns and recommendations stated above with respect to SPD Patrol ALPRs (e.g., data access, clear standards for data sharing with third party entities, clear purpose of sharing, auditing requirements) apply equally to Parking Enforcement Systems. The Council should therefore ensure that the same minimum rules (listed in the Executive Summary) apply to Parking Enforcement Systems via ordinance, and that the issues noted below with SPD's current policies are addressed as set forth in the corresponding recommendations, all of which should be incorporated into the Council's approval of the technology.

SPD's policy:

- Does not make clear how the Parking Enforcement ALPR systems integrate with the Patrol ALPR systems—it appears that some integration occurs at least in the case of the Scofflaw enforcement vans that store collected data in the BOSS system.
    - *Recommendation: SPD's policy must require that the data collected by Parking Enforcement ALPR systems is not shared with Patrol ALPR systems.*
- Does not make clear whether software and hardware providers (as mentioned in Section 2.3 of the SIR) all contract directly with SPD itself, with each other, or with a third-party entity to provide ALPR and related services.
    - *Recommendation: SPD's policy must require all data-sharing relationships to be disclosed to the public in clear terms, and, as stated above in the ALPR-Patrol Section, SPD's policy must limit sharing of ALPR data to third parties that have a written agreement holding those third parties to the same use, retention, and access rules as SPD, and requiring disclosure of to whom and under what circumstances the data are disclosed.*
- Does not include systematic tracking to assess the numbers of scans, hits, and revenue generated from the Parking Enforcement ALPR systems.
    - *Recommendation: SPD's policy must require detailed records of ALPR scans, hits, and revenue generated specifically attributable to those hits, as well as an accounting of how ALPR use varies by neighborhood and demographic*.
- Does not make clear whether pictures of the vehicle are being taken in addition to the license plate, and if so, if and for how long these pictures are stored (Section 4.1)
    - *Recommendation: SPD's policy must make explicit what photos are taken by the ALPR on Parking Enforcement vehicles, and require the same 48-hour maximum retention period for all photos.*

~~3. License Plate Readers (LPR) (SDOT)~~

~~In contrast to the SPD SIRs, the License Plate Readers (SDOT) SIR clearly defines and states meaningful restrictions on the purposes for which LPRs data may be collected, accessed, and used; it states that no license plate data is retained by SDOT or WSDOT; and it states that the license plate information SDOT accesses will never be used as a part of any criminal investigation.~~

~~However, it remains unclear whether SDOT's stated no-retention practice is reflected in written policy. Furthermore, SDOT's use of LPRs poses the concern of data sharing with a state entity (WSDOT). It is unclear whether an explicit agreement exists between SDOT and WSDOT ensuring that WSDOT uses the data only for the purpose of calculating travel times, and deletes the data immediately after such use.~~

~~In addition to the minimum standards stated in the Executive Summary, the Council should in its approval of this technology ensure that:~~

1. ~~The LPR data collected by SDOT is used only for the purpose of calculating travel times, and explicitly never for criminal or law enforcement purposes.~~
2. ~~No LPR data is retained.~~
3. ~~No third party other than SDOT and WSDOT can access the LPR data at any time.~~
4. ~~A written agreement holds WSDOT to the above restrictions.~~

CTO RESPONSE

Memo

Date: 11/17/2020

To: Seattle City Council, Transportation and Utilities Committee

From: Saad Bashir

Subject: CTO Response to the Surveillance Working Group ALPR (Parking Enforcement) SIR Review

---

To the Council Transportation and Utilities Committee Members,

I look forward to continuing to work together with Council and City departments to ensure continued transparency about the use of surveillance technologies and finding a mutually agreeable means to use technology to improve City services while protecting the privacy and civil rights of the residents we serve.

As provided in the Surveillance Ordinance, SMC 14.18.080, this memo outlines the Chief Technology Officer's (CTO's) response to the Surveillance Working Group assessment on the Surveillance Impact Report for Seattle Police Department's Automated License Plate Readers.

In their review, the Working Group has raised concerns about these cameras being used in a privacy impacting way, including video recording, data retention, data sharing, integration with other technologies and secondary uses of recorded video. We believe that policy, training and technology limitations enacted by SPD provide adequate mitigation for the potential privacy and civil liberties concerns raised by the Working Group about the use of this important operational technology.

Background

The Information Technology Department (ITD) is dedicated to the Privacy Principles and Surveillance Ordinance objectives to provide oversight and transparency about the use and acquisition of specialized technologies with potential privacy and civil liberties impacts. All City departments have a shared mission to protect lives and property while balancing technology use and data collection with negative impacts to individuals. This requires ensuring the appropriate use of privacy invasive technologies through technology limitations, policy, training and departmental oversight.

The CTO's role in the SIR process has been to ensure that all City departments are compliant with the Surveillance Ordinance requirements. As part of the review work for surveillance technologies, ITD's Privacy Office has facilitated the creation of the Surveillance Impact Report documentation, including collecting comments and suggestions from the Working Group and members of the public about these technologies. IT and City departments have also worked collaboratively with the Working Group to answer additional questions that came up during their review process.

Technology Purpose

Seattle Police Department (SPD) facilitates the flow of traffic, assists with the collection of revenue related to parking violations in the City of Seattle, and recovers stolen vehicles through a number of means. Among these is Parking Enforcement Systems technology, which is used by SPD as a necessary tool in the following ways:

1. Scofflaw – SPD employs three vehicles (two vans, and one truck) with ALPR systems to identify parked vehicles in violation of the City Scofflaw Ordinance. Vehicles in violation are subject to booting, pending payment of past due balances.

2. Time-Restricted Parking Areas – 47 sedans, 54 scooters, 2 vans, and 1 truck are utilized to monitor time-restricted parking within the City. Five of the sedans are equipped with ALPR systems and operated by civilian employees to digitally “chalk” vehicles parked in time-restricted zones. Utilizing GPS location and stem-valve comparison technology, the system alerts on those vehicles that are in violation of the time zone restriction upon a second pass. The remaining vehicles are used in traditional pay to park enforcement, and for manually chalking vehicle tires in time-restricted locations.

3. Restricted Parking Zones ("RPZ") means a portion of the street commonly used for vehicular parking where vehicles properly displaying a permit or other authorization are exempt from the posted RPZ. Seattle Department of Transportation provides SPD with a list of vehicles permitted to park in an RPZ. Parking Enforcement Officers may use ALPR to determine that a vehicle does not have the appropriate permit or authorization to park in an RPZ.

4. Parking Enforcement Officers may use ALPR using a list of vehicles reported stolen or sought in connection with criminal investigation to identify those vehicles and report their location to Dispatch.

5. Parking in the City is also monitored by Parking Enforcement officers on bicycles, foot, and scooters. ALPR is not used in this capacity.

Working Group Concerns

In their review, the Working Group has raised concerns about these cameras being used in a privacy impacting way, including video recording, data retention, data sharing, integration with other technologies and secondary uses of recorded video. Specifically:

1. The use of these systems and the data collected by them for purposes other than those intended.
2. Over-collection and over-retention of data.
3. Sharing of that data with third parties (such as federal law enforcement agencies).

UPDATE: Through the course of the completion of the Surveillance Impact Report, SPD recognized the need to update the existing ALPR Policy and on February 1, 2019 the new SPD ALPR policy went into effect. This new policy expanded on the previous version by adding definitions of the terms used in the operation of the technology, expanding on the required training for employees prior to access and use of ALPR, detailing authorized and prohibited uses of ALPR, defining response to alerts, detailing how ALPR equipment is to be handled, detailing ALPR administrator roles, defining ALPR data storage and retention, and detailing policy around the release or sharing of ALPR data.

We believe that the updated policy, training and technology limitations enacted by SPD provide adequate mitigation for the potential privacy and civil liberties concerns raised by the Working Group about the use of this important operational technology.

Response to Specific Concerns: SPD PE ALPR

Concern: The use of these systems and the data collected by them for purposes other than those intended.

CTO Assessment: There are four stated uses of the Parking Enforcement ALPR technology, as outlined in the technology purpose section above. These include Scofflaw enforcement, Time-Restricted Parking Areas, Restricted Parking Zones ("RPZ"), identification and recovery of vehicles reported stolen or sought in connection with criminal investigation. SPD provides links to six policies referencing acceptable use and limitations to access to the data collected for investigative purposes, including the data collected by the ALPR system. This system has been subject to oversight and audit to ensure that the data is only accessed and used for these purposes. We have assessed that there are appropriate policies and technology in place to restrict data use and access. Details about these policies and access controls are provided in the SIR responses, provided below.

SIR Response:
Section 4.7: How will data that is collected be accessed and by whom?

- All data collected for Parking Enforcement systems are hosted on City SPD servers and are not accessible by vendors without knowledge and/or permission of City personnel. Unlike some ALPR systems, SPD's systems do not "pool" SPD's ALPR data with that collected by other agencies.
- Only authorized users can access the data collected by ALPR for Parking Enforcement. Also, all activity by users in the AutoVu ALPR system is logged and auditable.
- Data removed from the system/technology and entered into investigative files is securely input and used on SPD's password-protected network with access limited to authorized SPD personnel.
- All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.

Section 4.8: If operated or used by another entity on behalf of the city, provide details about access, and applicable protocols

Access to the Parking Enforcement ALPR system is limited to ALPR-trained parking enforcement officers, the Parking Enforcement Supervisor, authorized SPD administrators, and authorized Seattle IT administrators.

Section 4.9: What are acceptable reasons for access to the equipment and/or data collected?

Users can only access the equipment for purposes earlier outlined– recovery of stolen vehicles to assist with active investigations, Scofflaw Law enforcement, and parking enforcement. Per SPD Policy 16.170, "ALPR may be used during routine patrol or any criminal investigation," and ALPR data may be accessed "only when the data relates to a specific criminal investigation."

Section 4.10: What safeguards are in place, for protecting data from unauthorized access?

- Individuals can only access the Parking Enforcement AutoVu ALPR system via unique login credentials. Hardware systems can only be accessed in-vehicle (which are assigned by superiors for each shift), and Parking Enforcement software systems can only be accessed in-vehicle or on-site of SPD. As previously noted, all activity in the systems is logged and can be audited.
- Further, City IT manages SQL on the system's backend that purges ALPR data at the required intervals (90 days). A record of the purge is generated and accessible at any time for verification of purges.

Concern: Over-collection and over-retention of data.

CTO Assessment: Individual city departments do not have the ability to set their own data retention schedules but must follow requirements set by the State of Washington. Regarding criminal justice data, there are additional requirements to ensure that the quality and availability of data follows legally required retention periods, ensuring that data is preserved after the investigation in case of any dispute. The data is protected and only accessible by those who are related to the investigation. Data collected by AutoVu (parking enforcement system) is not retained after the end of the officer's shift.

SIR Response:
Section 5.1: How will data be securely stored?

- All data collected from SPD's ALPR systems is stored, maintained, and managed on premises. Retention is automated, so that all ALPR data from the three ALPR-equipped Parking Enforcement boot vans is retained in the same BOSS database as ALPR data collected by ALPR-equipped patrol vehicles and is retained until automatically deleted after 90 days per department retention policy unless a record is identified as being related to a parking violation or criminal investigation and exported in support of that citation or investigation (see ALPR: Patrol SIR for further detail). All data collected from the five ALPR-equipped Parking Enforcement sedans is deleted from the vehicle on-board system when the Parking Enforcement Officer logs off the at the end of the shift.
- Unless a record is identified as being related to a parking violation or criminal investigation and exported in support of that matter, all data collected from the five ALPR-equipped Parking Enforcement sedans is deleted from the vehicle on-board system when the Parking Enforcement Officer logs off the at the end of the shift. No data from those sedans is retained by SPD except for records identified as being related to a parking violation or criminal investigation and exported during the shift it was captured.
- Parking Enforcement systems that are contracted by SPD include only PCS Mobile's Patroller and Gtechna. Data collected by Patroller and Gtechna are hosted on City SPD servers.

Section 5.4: Which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

Seattle City IT, in conjunction with SPD's Enforcement Supervisor, are responsible for ensuring compliance with data retention requirements. Additionally, external audits by OIG can review and ensure compliance, at any time.

Section 4.2: What measures are in place to minimize inadvertent or improper collection of data?

- When the ALPR system registers a hit, the user must verify accuracy before taking any action. In Parking Enforcement, users verify first that a vehicle hit for Scofflaw violation is still actively in

violation by checking for updated information in Bootview before booting a vehicle. Parking Enforcement Officers then visually verify that a vehicle suspected of time-zone restriction or metered parking violation is, in fact, in violation prior to issuing a ticket. Images captured serve as "evidence" that the system and the user are not in error.

- Unless a hit has been exported for investigation and exported from the database for this purpose, all data captured by the five ALPR-equipped parking enforcement sedans is retained in the same database as ALPR data collected by ALPR-equipped patrol vehicles and is retained until automatically deleted after 90 days, per department retention policy (see ALPR Surveillance Impact Report).
- Unless a hit has been exported for booting or investigation and exported for this purpose, all data captured by boot van ALPR is deleted when the Parking Enforcement Officer logs off the system at the end of shift.

Section 8.2: What auditing measures are in place to safeguard the information?
Parking Enforcement Systems, including ALPR, do not self-audit. Instead, third party audits exist, as follows: 1) The Parking Enforcement Supervisor has the responsibility of managing the user list and ensuring proper access to the system; 2) The Office of the Inspector General (OIG) can also conduct an audit at any time. Violations of policy may result in referral to Office of Professional Accountability (OPA).

Section 6.5: Explain how the project/technology checks the accuracy of the information collected. If accuracy is not checked, please explain why.

- Parking Enforcement systems technologies do not check themselves for errors. This is because the systems are unaware that they are gathering incorrect data. Instead, users are trained to visually verify accuracy (i.e., comparing a license plate hit from the system to the physical plate that the system read before taking any action). If they note a misread, they can enter a note into the system recognizing the read, as such. If they cannot verify visually, no action is taken.
- Individuals can challenge citations, alleged scofflaw violations, or criminal charges and provide correct information.

Concern: Sharing of that data with third parties (such as federal law enforcement agencies).

CTO Assessment: While civil liberties groups have expressed great concern with this practice in other jurisdictions, SPD does not "pool" data with other agencies that create a large database of license plates. SPD's revised policy 16.170 address data sharing and states, "ALPR data will only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law." Specific examples of these agencies are outlined in the SIR documentation.

SIR Response:
Section 5.1: How will data be securely stored?

- All data collected from SPD's ALPR systems is stored, maintained, and managed on premises. Retention is automated, so that all ALPR data from the three ALPR-equipped Parking Enforcement boot vans is retained in the same BOSS database as ALPR data collected by ALPR-equipped patrol vehicles and is retained until automatically deleted after 90 days per department retention policy unless a record is identified as being related to a parking violation or criminal investigation and exported in support of that citation or investigation (see ALPR:

Patrol SIR for further detail). All data collected from the five ALPR-equipped Parking Enforcement sedans is deleted from the vehicle on-board system when the Parking Enforcement Officer logs off the at the end of the shift.

- Unless a record is identified as being related to a parking violation or criminal investigation and exported in support of that matter, all data collected from the five ALPR-equipped Parking Enforcement sedans is deleted from the vehicle on-board system when the Parking Enforcement Officer logs off the at the end of the shift. No data from those sedans is retained by SPD except for records identified as being related to a parking violation or criminal investigation and exported during the shift it was captured.
- Parking Enforcement systems that are contracted by SPD include only PCS Mobile's Patroller and Gtechna. Data collected by Patroller and Gtechna are hosted on City SPD servers.

Section 5.4: Which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

Seattle City IT, in conjunction with SPD's Enforcement Supervisor, are responsible for ensuring compliance with data retention requirements. Additionally, external audits by the Office of the Inspector General (OIG) can review and ensure compliance, at any time.

Section 6.1: Which entity or entities inside and external to the city will be data sharing partners?

- Data obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law. Seattle's Scofflaw Ordinance and Traffic Code require that SPD share information with Seattle Municipal Court.
- Data may be shared with outside entities in connection with criminal prosecutions:
  - Seattle City Attorney's Office
  - King County Prosecuting Attorney's Office
  - King County Department of Public Defense
  - Private Defense Attorneys
  - Seattle Municipal Court
  - King County Superior Court
  - Similar entities where prosecution is in Federal or other State jurisdictions
- Data may be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.
- Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."
- Discrete pieces of data collected by the parking enforcement systems may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by SPD Policy 12.050 and 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayor's Directive, dated February 6, 2018.

- SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the parking enforcement systems.

Section 7.2: Describe what privacy training is provided to users either generally or specifically relevant to the project/technology.

Users are trained in how to use the parking enforcement and ALPR systems and how to properly access data by other trained Parking Enforcement Officers. The Parking Enforcement Supervisor confirms the training before providing access to new users.

SPD Policy 12.050 mandates that all employees, including Parking Enforcement Officers, who use terminals that have access to information in WACIC/NCIC files, must be certified by completing complete Security Awareness Training (Level 2) with recertification testing required every two years, and all employees also complete City Privacy Training. Failure to comply with ACCESS/NCIC/WACIC user requirements can result in termination of the right to continue using ACCESS services.

Section 6.2: Why is data sharing necessary?

Data sharing is necessary for SPD to fulfill its mission as a law enforcement agency and to comply with legal requirements.

Section 6.3.1: Are there any restrictions on non-city data use?

- Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.
- Once disclosed in response to PRA request, there are no restrictions on non-City data use; however, applicable exemptions will be applied prior to disclosure to any requestor who is not authorized to receive exempt content.

APPENDIX A: GLOSSARY

Accountable: (Taken from the Racial Equity Toolkit.) Responsive to the needs and concerns of those most impacted by the issues you are working on, particularly to communities of color and those historically underrepresented in the civic process.

ALPR: "Automated License Plate Readers"

Community Outcomes: (Taken from the Racial Equity Toolkit.) The specific result you are seeking to achieve that advances racial equity.

Contracting Equity: (Taken from the Racial Equity Toolkit.) Efforts to achieve equitable racial outcomes in the way the City spends resources, including goods and services, consultants and contracting.

DON: "Department of Neighborhoods."

Genetec's Patroller software: a non-surveillance technology that is required for APLR to be used for Parking Enforcement purposes, the interface and backend server through which retention periods are set (and auditable), user permissions are managed, user activity is tracked and logged, and camera "read" and "hit" data is accessible.

Gtechna software: a non-surveillance technology that is required for APLR to be used for Parking Enforcement purposes, prints citations for vehicles found in violation of scofflaw, overtime zone parking, and metered parking.

Immigrant and Refugee Access to Services: (Taken from the Racial Equity Toolkit.) Government services and resources are easily available and understandable to all Seattle residents, including non-native English speakers. Full and active participation of immigrant and refugee communities exists in Seattle's civic, economic and cultural life.

Inclusive Outreach and Public Engagement: (Taken from the Racial Equity Toolkit.) Processes inclusive of people of diverse races, cultures, gender identities, sexual orientations and socio-economic status. Access to information, resources and civic processes so community members can effectively engage in the design and delivery of public services.

Individual Racism: (Taken from the Racial Equity Toolkit.) Pre-judgment, bias, stereotypes about an individual or group based on race. The impacts of racism on individuals including white people internalizing privilege, and people of color internalizing oppression.

Institutional Racism: (Taken from the Racial Equity Toolkit.) Organizational programs, policies or procedures that work to the benefit of white people and to the detriment of people of color, usually unintentionally or inadvertently.

Neology Back Office System Software (BOSS): System through which ALPR camera reads are interpreted and administrative control is managed. This includes the ability to set and verify retention periods, track and log user activity, view camera "read" and "hit" data, and manage user permissions.

Neology PIPS: Mobile license plate recognitions system installed in eleven Patrol vehicles.

OCR: "Office of Arts and Culture."

Opportunity Areas: (Taken from the Racial Equity Toolkit.) One of seven issue areas the City of Seattle is working on in partnership with the community to eliminate racial disparities and create racial equity. They include: Education, Health, Community Development, Criminal Justice, Jobs, Housing, and the Environment.

Paylock's Bootview software: a non-surveillance, Municipal Court technology that is required for APLR to be used for Parking Enforcement purposes, which tracks the status of vehicles in violation of Scofflaw through its Bootview software program.

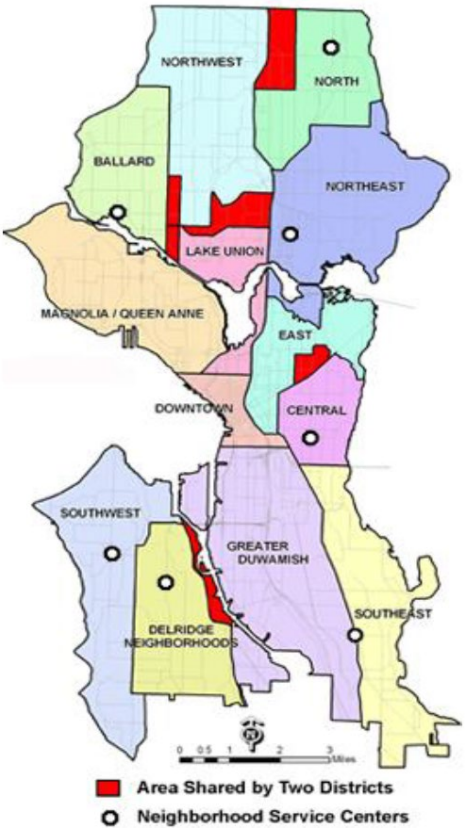
Racial Equity: (Taken from the Racial Equity Toolkit.) When social, economic and political opportunities are not predicted based upon a person's race.

Racial Inequity: (Taken from the Racial Equity Toolkit.) When a person's race can predict their social, economic, and political opportunities and outcomes.

RET: "Racial Equity Toolkit"

Samsung devices: a non-surveillance technology that is required for APLR to be used for Parking Enforcement purposes, which allows Officers to access the software required to write tickets and enter ticket information.

Seattle Neighborhoods: (Taken from the Racial Equity Toolkit Neighborhood.) Boundaries defined for the purpose of understanding geographic areas in Seattle.



Stakeholders: (Taken from the Racial Equity Toolkit.) Those impacted by proposed policy, program, or budget issue who have potential concerns or issue expertise. Examples might include: specific racial/ethnic groups, other institutions like Seattle Housing Authority, schools, community-based organizations, Change Teams, City employees, unions, etc.

Structural Racism: (Taken from the Racial Equity Toolkit.) The interplay of policies, practices and programs of multiple institutions which leads to adverse outcomes and conditions for communities of color compared to white communities that occurs within the context of racialized historical and cultural conditions.

Surveillance Ordinance: Seattle City Council passed Ordinance 125376, also referred to as the "Surveillance Ordinance."

SIR: "Surveillance Impact Report", a document which captures the fulfillment of the Council-defined Surveillance technology review process, as required by Ordinance 125376.

Workforce Equity: (Taken from the Racial Equity Toolkit.) Ensure the City's workforce diversity reflects the diversity of Seattle.

APPENDIX B: PUBLIC COMMENT DEMOGRAPHICS AND ANALYSIS

OVERVIEW OF PUBLIC COMMENT ANALYSIS

Analysis of public comments was completed using a combination of thematic analysis and qualitative coding. Comments were gathered from many sources, from public engagement meetings, an online survey form, letters, emails, and focus group discussions. All comments may be reviewed in Appendix E.

After assigning a theme and code for the content, City staff conducted an analysis using R. A high-level summary of the results of this analysis are shown below. A detailed description of the methodology is available in Appendix H.

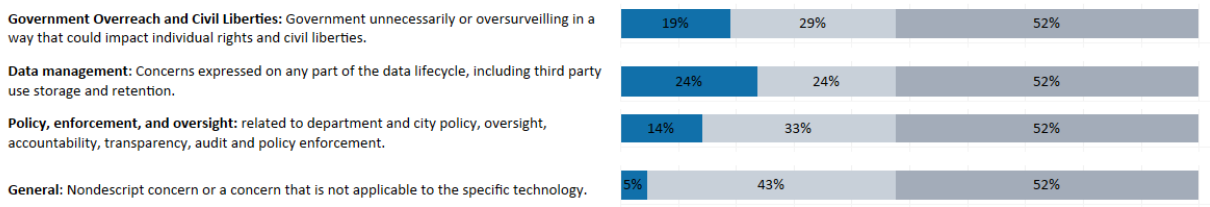
COMMENTS SPECIFICALLY ADDRESSING PARKING ENFORCEMENT

Question 1

Do you have concerns about this specific technology or how it is used?

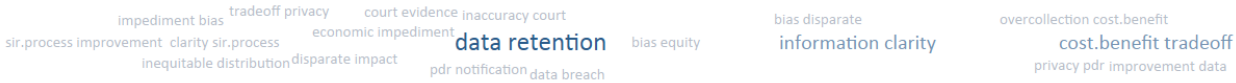
10

Reponses to this question



"There is a lot of data collection, but a small number of 'hits'"

Common Themes

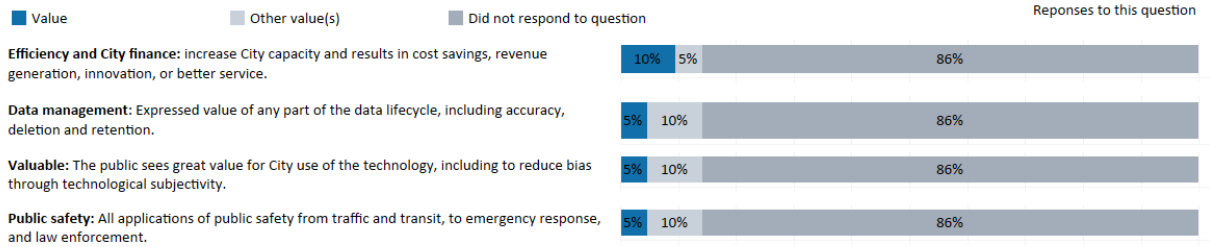


Question 2

What value do you think this technology brings to our city?

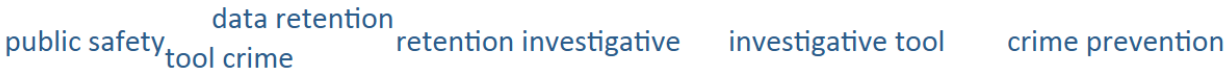
3

Reponses to this question



"Relieving writer's cramp ad tedium" *"Brings order to the City"*

Common Themes



Question 3

What worries you about how this is used?

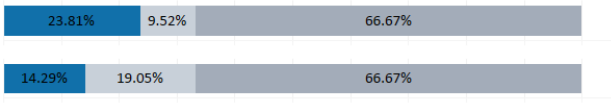
No responses.

Question 4

What recommendations would you give policy makers at the City about this technology?

7

Reponses to this question



Increase policy, enforcement, and oversight: recommendations related to department and city policy, oversight, accountability, transparency, audit and policy enforcement.

Improve data management: Recommendation to improve approach to data lifecycle management, including third party use storage and retention.

"Ensure the data retention for all non-investigation parking enforcement ALPR data is only til end of shift/day."

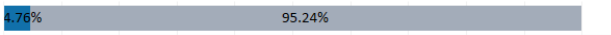
Common Themes

metric development policy development transparency equitable
equitable distribution policy alignment pdr policy policy enforcement development reporting data deletion
deletion policy transit funding audit metric reporting statistics

Question 5

Can you imagine another way to solve the problem this technology solves?

1



Public safety: All applications of public safety from traffic and transit, to emergency response, and law enforcement

"Could be done manually but lots of time"

Common Themes

community education increase police

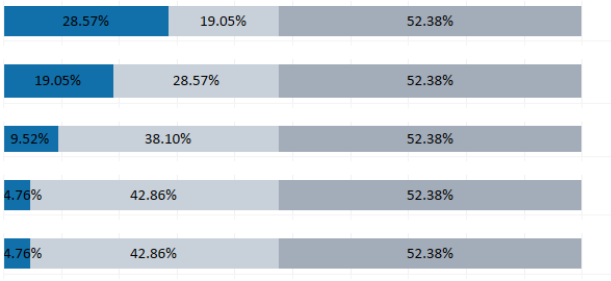
Question 6

Do you have any other comments?

10

Reponses to this question

Comment Other comment Did not respond to question



Public safety: All applications of public safety from traffic and transit, to emergency response, and law enforcement.

Unconcerned: Expressed a lack of concern around technology use or interest in expansion of use.

Policy, enforcement, and oversight: related to department and city policy, oversight, accountability, transparency, audit and policy enforcement.

Alternative technology: Recommends either another technology, such drones or RFID, etc.

Improve SIR Process: Change the surveillance impact report process, suggestions include adding a cost benefit analysis, increaseing information clarity, etc.

Common Themes

law enforcement safety inaccuracy overcollection cost.benefit cost.benefit tradeoff sir.process improvement
public safety

GENERAL SURVEILLANCE COMMENT THEMES

Many comments were submitted as part of the public comment period that were not specific to a technology, but to either the concept of surveillance in general, or to technologies which are not on the Master List.

Themes

Top themes

public safety	Safety of the public, including first response, and in some cases traffic safety.
crime prevention	Tool or process to aid in the prevention of crime by police.
transit safety	Safety on or around public transit, roadways, or relating to traffic overall, including bicycle and pedestrian.
law enforcement	Enforce the laws, whether related to City policy, traffic law, or public safety law enforcement.
increase police	Policy recommendation or alternative solution that requires more police officers.
parking enforcement	Enforcement of laws specifically related to parking infractions.
facilitate traffic.flow	Improve the ability for cars, buses and bicycle to navigate through the City.
redlight cameras	Subject of comment was a camera technology exempt from SIR process by Ordinance and not under review.
add cameras	Desire for additional cameras, to include police, traffic, red-light or other.
investigative tool	Value or other comment of police to use technology as a tool for solving open or active crimes.
public oversight	Desire for public oversight of technology, may include voting, audits, or other transparency methods.
increase deployment	Increase the use and deployment of surveillance technology.

DEMOGRAPHICS FOR GROUP ONE COMMENTS

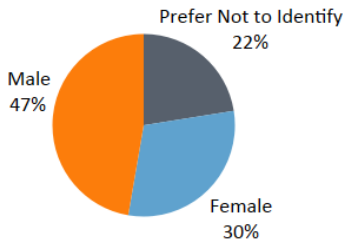
The number of reported demographics does not correspond to the number of comments received for the following reasons.

1. The demographic information includes all responses, regardless of which technology was commented on to protect the privacy of those who provided a response.
2. Some individuals offered more than one comment.
3. Some individuals did not provide any demographic information.

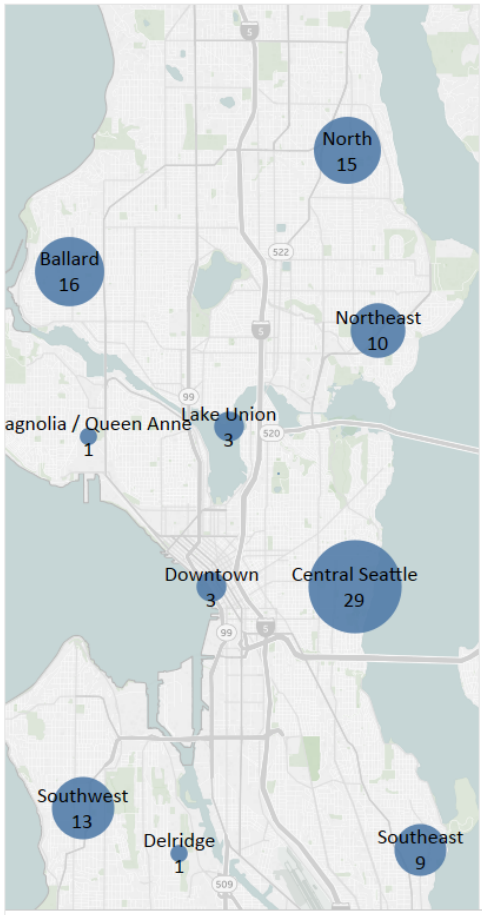
Method Submitted By

Focus Group 1	9
Focus Group 2	5
Meeting 1	15
Meeting 2	7
Meeting 3	10
Meeting 4	14
Meeting 5	5
Survey Monkey	64
Grand Total	129

Gender

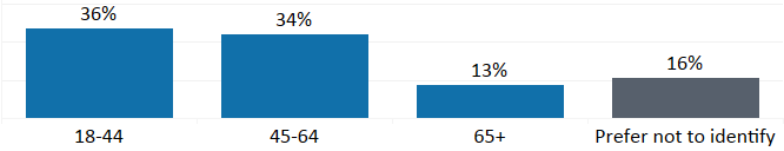


Neighborhoods

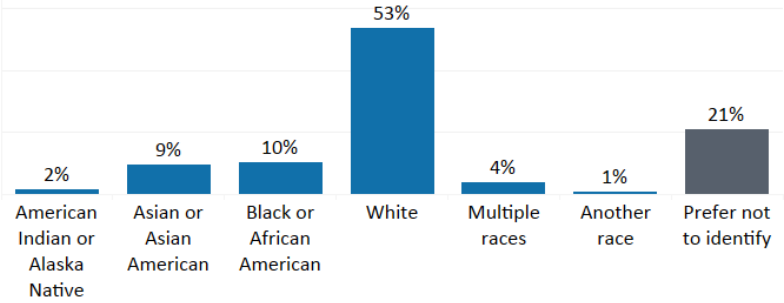


King County (outside Seattle)	8
Outside of King County	1
Prefer not to identify	10

Age



Enthnicity



APPENDIX C: PUBLIC MEETING NOTICE(S)

Notice of Public Meetings
Surveillance Technology Public Comment

This is the first round of public comment on previously acquired surveillance technologies. For more information on these technologies or Surveillance Ordinance visit **seattle.gov/privacy**.

	Meeting 1	Meeting 2	Meeting 3	Meeting 4	Meeting 5
Depts. Presenting	Police Dept.	Transportation, Fire Dept.	Police Dept.	Police Dept.	Transportation, Fire Dept.
Date & Time	October 22, 2018 5-6:30 p.m.	October 25, 2018 5-6:30 p.m.	October 29, 2018 5-6:30 p.m.	October 30, 2018 5-6:30 p.m.	November 5, 2018 4:30-5:30 p.m.
Location	**Columbia City Branch Library** 4721 Rainier Ave S, Seattle, WA 98118	**American Legion Hall: West Seattle** 3618 SW Alaska St. Seattle, WA 98126	**Bertha Knight Landes Room** 1st Floor City Hall - 600 4th Ave, Seattle, WA 98104 (5th Ave door)	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115

Technologies discussed at the meetings include:

Transportation (Meetings 2 & 5)	**Fire Dept.** (Meetings 2 & 5)	**Police Dept.** (Meetings 1, 3, & 4)
Traffic Cameras & License Plate Readers	Emergency Scene Cameras & Hazmat Cameras	Parking Enforcement Systems & Automated License Plate Readers

Here's how you can provide comments:

The open comment period for these technologies is **October 8 - November 5, 2018.** There are three ways to comment:

1. Attend the meeting. See the table above for locations and times.

2. Submit comment online at **seattle.gov/privacy**.

3. Send mail to Attn: Surveillance & Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.

Comments submitted will be included in the final Surveillance Impact Report submitted to City Council and available to the public. To comment after this period has closed, contact City Council staff at **seattle.gov/Council**.

Please note, this meeting will:

Be video recorded. **Ask for a sign-in record of attendees.** **Collect public comments.**

For meeting accommodations: Please let us know **two weeks in advance of the meeting date** if language translation, or other services are needed by emailing **Surveillance@seattle.gov**.

City of Seattle

Aviso de audiencias públicas

Comentarios del público sobre tecnologías de vigilancia

Esta es la primera ronda de audiencias públicas sobre tecnologías de vigilancia adquiridas previamente. Para obtener más información sobre estas tecnologías o sobre la Surveillance Ordinance (Ordenanza sobre Vigilancia), visite **seattle.gov/privacy**.

	Audiencia 1	Audiencia 2	Audiencia 3	Audiencia 4	Audiencia 5
Departamentos a cargo	Depto. de Policía	Depto. de Transporte y de Bomberos	Depto. de Policía	Depto. de Policía	Depto. de Transporte y de Bomberos
Fecha y hora	22 de octubre de 2018 5:00 a 6:30 p. m.	25 de octubre de 2018 5:00 a 6:30 p. m.	29 de octubre de 2018 5:00 a 6:30 p. m.	30 de octubre de 2018 5:00 a 6:30 p. m.	5 de noviembre de 2018 4:30 a 5:30 p. m.
Lugar	**Columbia City Branch Library** 4721 Rainier Ave S, Seattle, WA 98118	**American Legion Hall: West Seattle** 3618 SW Alaska St. Seattle, WA 98126	**Bertha Knight Landes Room** 1st Floor City Hall - 600 4th Ave, Seattle, WA 98104 (5th Ave door)	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115

En las audiencias se hablará de las siguientes tecnologías:

Transporte (audiencias 2 y 5)	**Depto. de Bomberos** (audiencias 2 y 5)	**Depto. de Policía** (audiencias 1, 3 y 4)
Cámaras de tránsito y lectores de placas de automóviles	Cámaras para escenas de emergencia y cámaras para Hazmat (hazardous materials, materiales peligrosos)	Sistemas de control de áreas de estacionamiento y lectores automáticos de placas de automóviles

Cómo puede enviar sus comentarios:

El período abierto para recibir comentarios sobre estas tecnologías es desde el **8 de octubre hasta el 5 de noviembre de 2018.** Existen tres formas de aportar comentarios:

1. Asista a la audiencia. Consulte la tabla anterior para conocer los horarios y los lugares.

2. Deje sus comentarios en línea en **seattle.gov/privacy**.

3. Envíe comentarios por correo postal a la siguiente dirección: Surveillance & Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.

Los comentarios enviados se incluirán en la versión final del Surveillance Impact Report (Informe del efecto de la vigilancia) que se presentará ante el Consejo de la Ciudad y estará disponible al público en general. Para aportar comentarios luego de este período, comuníquese con el personal del Consejo de la Ciudad desde la página web **seattle.gov/Council**.

Tenga en cuenta que esta audiencia tendrá las siguientes características:

Se grabará en video. **Se llevará un registro de asistencia.** **Se recolectarán comentarios del público.**

Adaptaciones para las audiencias: Si necesita servicios de traducción u otros servicios, envíenos un correo electrónico a **Surveillance@seattle.gov dos semanas antes de la audiencia.**

City of Seattle

Ogaysiiska Kulanada Dadwaynaha

Fikradaha Dadwayanaha ee ku aadan Qalabka Muraaqabaynta Casriga ah

Kani waa wareegi koowaad ee lagu aruurinaayo fikradaha dadwaynuhu kaqabaan qalabka muraaqabaynta casriga ah noociisii hore. Wixii macluumaad dheeraad ah oo kusaabsan qalabkaan ama Surveillance Ordinance (Qaabka Muraaqabaynta) booqo **seattle.gov/privacy**.

	Kulanka 1	Kulanka 2	Kulanka 3	Kulanka 4	Kulanka 5
Waaxaha. Soojeedinta	Waaxda Booliiska.	Gaadiidka, Waaxda Dab Damiska.	Waaxda Booliiska.	Waaxda Booliiska.	Gaadiidka, Waaxda Dab Damiska.
Tariikhda iyo waqtiga	Oktoobar 22, 2018 5-6:30 p.m.	Oktoobar 25, 2018 5-6:30 p.m.	Oktoobar 29, 2018 5-6:30 p.m.	Oktoobar 30, 2018 5-6:30 p.m.	Nofeembar 5, 2018 4:30-5:30 p.m.
Goobta	**Laanta Maktabada ee Magaalada Columbia** 4721 Rainier Ave S, Seattle, WA 98118	**American Legion Hall: West Seattle** 3618 SW Alaska St. Seattle, WA 98126	**Bertha Knight Landes Room** 1st Floor City Hall - 600 4th Ave, Seattle, WA 98104 (5th Ave door)	**Laanta Maktabada Green Lake** 7364 East Green Lake Dr. N, Seattle, WA 98115	**Laanta Maktabada Green Lake** 7364 East Green Lake Dr. N, Seattle, WA 98115

Tignoolojiyadaha looga dooday kulanada waxaa kamid ah:

Gaadiidka (kulanada 2 iyo 5)	**Waaxda Dab damiska.** (Kulanada 2 iyo 5)	**Waaxda Booliiska.** (Kulanada 1, 3, iyo 4)
Kaamirooyinka taraafikada iyo Qalabka Akhriya Aqoonsiga Shatiyada	Kaamirooyinka Dhacdooyinka Degdega ah iyo kaamiroyinka Hamzat	Nidaamyada Xakamaynta Baakinka iyo Qalabka Akhriya Aqoonsiga Shatiyada

Halkaan kabaro sida aad fikrado kudhiiban karto:

Mudada ay furantahay fikrad kadhiibashada qalabkaan casriga ah waa Oktoobar 8 - Nofeembar 5, 2018. Waxaa jira saddex qaab oo fikir lagu dhiiban karo:

1. Inaad kulanka kaqaybgasho. Fiiri shaxda kore oo ay kuqoran yihiin goobaha iyo xiliyada laqabanaayo kulanada.
2. Fikirkaaga kudir si oonleen ah **seattle.gov/privacy**.
3. Boosto udir: Surveillance & Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.

Fikrado kasta oo lasoo gudbiyo waxaa lagu darayaa War bixinta ugu danbaysa Surveillance Impact Report (Saamaraynta Qalabka Muraaqabada) ee loogudbiyo Dawlada hoose dadwaynuhuna ay akhri sankaraan. Si aad fikirkaaga udhiibato kadib marka mudadaan dhammaato, laxiriir Shaqaalaha Dawlada Hoose oo ciwaankoodu yahay **seattle.gov/Council**.

Fadlan ogsoonow, kulankaan waa:

Laduubayaa si muqaal ahaan ah. **Dalbo Diiwanka Galitaanka dadka Kaqaybgalaaya ay saxiixayaan.** **Aruuri Fikradaha Dadwaynaha.**

Wixi laxiriira adeegyada kulanada intay socdaan labixinaayo: Fadlan noosoosheeg **labo asbuuc kahor taariikhda kulanku dhacayo** haddii adeegyada turjumida luuqada, ama adeegyo kale loobaahdo adoo email noogusoo diraaya **Surveillance@seattle.gov**.

City of Seattle

公開會議通知
監視技術公開意見徵集會

這是第一輪會議，徵集公眾對之前取得的監控技術的建議。要獲取有關這些技術或 Surveillance Ordinance（監控條例）的更多資訊，請瀏覽 seattle.gov/privacy。

	會議 1	會議 2	會議 3	會議 4	會議 5
出席部門	警察署	交通、消防署	警察署	警察署	交通、消防署
日期及時間	2018 年 10 月 22 日 下午 5-6:30	2018 年 10 月 25 日 下午 5-6:30	2018 年 10 月 29 日 下午 5-6:30	2018 年 10 月 30 日 下午 5-6:30	2018 年 11 月 5 日 下午 4:30-5:30
地點	**Columbia City Branch Library** 4721 Rainier Ave S, Seattle, WA 98118	**American Legion Hall: West Seattle** 3618 SW Alaska St. Seattle, WA 98126	**Bertha Knight Landes Room** 1st Floor City Hall - 600 4th Ave, Seattle, WA 98104 (5th Ave door)	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115

會上討論的技術包括：

交通署（會議 2 和會議 5）	**消防署**（會議 2 和會議 5）	**警察署**（會議 1、3 和 4）
交通攝像頭和車輛牌照識別器	緊急現場攝像頭與危險品攝像頭	停車執行系統與車輛牌照自動識別器

您提交意見的方式：

針對這些技術的公眾意見徵集時間是 **2018 年 10 月 8 日至 11 月 5 日**。有三種方式可提交意見：

出席會議。
和時間見上表。

2. 透過 seattle.gov/privacy 網上提交意見。

3. 寄郵件至：Surveillance & Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124。

提交的所有意見都將收錄於最終的 Surveillance Impact Report（監控影響報告），遞交至市議會並向大眾開放。如果要在此期間結束後提交意見，請瀏覽 seattle.gov/Council，聯繫市議會的工作人員。

請注意，此會議將：

進行錄影。 **要求參會者簽到。** **收集公眾意見。**

會議輔助服務：如果需要語言翻譯或其他服務，請**參照會議日期提前兩週**發送電子郵件至 Surveillance@seattle.gov 告知我們。

City of Seattle

公开会议通知

监控技术公众意见征集会

这是第一轮会议，征集公众对之前取得的监控技术的意见。要获得有关这些技术或 Surveillance Ordinance（监控条例）的更多信息，请访问 **seattle.gov/privacy**。

	第 1 次会议	第 2 次会议	第 3 次会议	第 4 次会议	第 5 次会议
出席部门	警察局	交通、消防局	警察局	警察局	交通、消防局
日期与时间	2018 年 10 月 22 日 下午 5-6:30	2018 年 10 月 25 日 下午 5-6:30	2018 年 10 月 29 日 下午 5-6:30	2018 年 10 月 30 日 下午 5-6:30	2018 年 11 月 5 日 下午 4:30-5:30
地点	**Columbia City Branch Library** 4721 Rainier Ave S, Seattle, WA 98118	**American Legion Hall: West Seattle** 3618 SW Alaska St. Seattle, WA 98126	**Bertha Knight Landes Room** 1st Floor City Hall - 600 4th Ave, Seattle, WA 98104 (5th Ave door)	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115

会上讨论的技术包括：

交通局（第 2 和第 5 次会议）	**消防局**（第 2 和第 5 次会议）	**警察局**（第 1、3、4 次会议）
交通摄像头和车辆牌照识别器	紧急现场摄像头与危险品摄像头	停车执行系统与车辆牌照自动识别器

您提交意见的方式：

针对这些技术的公众意见征集时间是 **2018 年 10 月 8 日至 11 月 5 日**。提交意见的三种途径：

1. 出席会议。
地点和时间见上表。

2. 通过网站 **seattle.gov/privacy** 在线提交意见。

3. 寄送邮件至：Surveillance & Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124。

提交的所有意见都将收录于最终的 Surveillance Impact Report（监控影响报告），递交至市议会并向大众开放。如果要在此期间结束后提交意见，请浏览 **seattle.gov/Council**，联系市议会的工作人员。

请注意，此会议将：

进行录像。 **要求参会者签到。** **收集公众意见。**

会议辅助服务：如果需要语言翻译或其他服务，请参照会议**日期提前两周**发送电子邮件至 **Surveillance@seattle.gov**

City of Seattle

Thông Báo Về Các Cuộc Họp Công Chúng
Ý Kiến Của Công Chúng Về Công Nghệ Giám Sát

Đây là vòng thu thập ý kiến của công chúng đầu tiên về các công nghệ giám sát đã được ứng dụng trước đây. Để có thêm thông tin về các công nghệ này hoặc Surveillance Ordinance (Sắc Lệnh Giám Sát), hãy truy cập **seattle.gov/privacy**.

	Cuộc họp 1	Cuộc họp 2	Cuộc họp 3	Cuộc họp 4	Cuộc họp 5
Các Sở Tổ Chức Cuộc Họp	Sở Cảnh Sát	Sở Giao Thông Vận Tải, Sở Cứu Hỏa	Sở Cảnh Sát	Sở Cảnh Sát	Sở Giao Thông Vận Tải, Sở Cứu Hỏa
Ngày & Giờ	Ngày 22 tháng 10 năm 2018 5 giờ - 6 giờ 30 phút chiều	Ngày 25 tháng 10 năm 2018 5 giờ - 6 giờ 30 phút chiều	Ngày 29 tháng 10 năm 2018 5 giờ - 6 giờ 30 phút chiều	Ngày 30 tháng 10 năm 2018 5 giờ - 6 giờ 30 phút chiều	Ngày 5 tháng 11 năm 2018 4 giờ 30 - 5 giờ 30 phút chiều
Địa điểm	**Columbia City Branch Library** 4721 Rainier Ave S, Seattle, WA 98118	**American Legion Hall: West Seattle** 3618 SW Alaska St. Seattle, WA 98126	**Bertha Knight Landes Room** 1st Floor City Hall - 600 4th Ave, Seattle, WA 98104 (5th Ave door)	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115

Các công nghệ được thảo luận tại các cuộc họp bao gồm:

Giao thông vận tải (Cuộc họp 2 & 5)	**Sở Cứu Hỏa** (Cuộc họp 2 & 5)	**Sở Cảnh Sát** (Cuộc họp 1, 3 & 4)
Các Máy Quay Giao Thông & Các Thiết Bị Đọc Biển Số Xe	Máy Quay Trường Hợp Khẩn Cấp & Máy Quay Hazmat	Hệ Thống Thực Thi Việc Đậu Xe & Các Thiết Bị Đọc Biển Số Xe Tự Động

Đây là cách quý vị có thể đưa ra ý kiến của mình:

Thời gian lấy ý kiến cho các công nghệ trên là **Ngày 8 tháng 10 – Ngày 5 tháng 11 năm 2018.** Có ba cách đưa ra ý kiến:

1. Tham dự cuộc họp. Xem bảng bên trên để biết thời gian và địa điểm.

2. Nộp ý kiến trực tuyến tại **seattle.gov/privacy**.

3. Gửi thư đến Attn: Surveillance & Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.

Các ý kiến được nộp sẽ được đưa vào bản Surveillance Impact Report (Báo Cáo Tác Động Giám Sát) cuối cùng nộp cho Hội Đồng Thành Phố và có sẵn dành cho công chúng. Để đưa ra ý kiến sau khi giai đoạn thu thập ý kiến đã kết thúc, hãy liên hệ với nhân viên của Hội Đồng Thành Phố tại **seattle.gov/Council**.

Vui lòng lưu ý, cuộc họp này sẽ:

Được ghi hình. **Yêu cầu lưu tên trong danh sách đăng ký tham dự.** **Thu thập các ý kiến của công chúng.**

Để đáp ứng các yêu cầu điều chỉnh: Vui lòng thông báo cho chúng tôi biết **hai tuần trước ngày diễn ra cuộc họp** nếu quý vị cần dịch vụ thông dịch ngôn ngữ hoặc các dịch vụ khác, bằng cách gửi email đến **Surveillance@seattle.gov**.

City of Seattle

Paunawa sa Mga Pampublikong Pagpupulong

Komento ng Publiko sa Teknolohiya sa Pagmamanman

Ito ang unang round para sa pagkomento ng publiko tungkol sa mga dating nakuhang teknolohiya sa pagmamanman. Para sa higit pang impormasyon tungkol sa mga teknolohiyang ito o sa Surveillance Ordinance (Ordinansa sa Pagmamanman), bumisita sa **seattle.gov/privacy**.

	Pagpupulong 1	Pagpupulong 2	Pagpupulong 3	Pagpupulong 4	Pagpupulong 5
Mga departamento na Naglalahad	Departamento ng Pulisya	Departamento ng Transportasyon, Bumbero	Departamento ng Pulisya	Departamento ng Pulisya	Departamento ng Transportasyon, Bumbero
Petsa at Oras	Oktubre 22, 2018 5-6:30 p.m.	Oktubre 25, 2018 5-6:30 p.m.	Oktubre 29, 2018 5-6:30 p.m.	Oktubre 30, 2018 5-6:30 p.m.	Nobyembre 5, 2018 4:30-5:30 p.m.
Lokasyon	**Columbia City Branch Library** 4721 Rainier Ave S, Seattle, WA 98118	**American Legion Hall: West Seattle** 3618 SW Alaska St. Seattle, WA 98126	**Bertha Knight Landes Room** 1st Floor City Hall - 600 4th Ave, Seattle, WA 98104 (5th Ave door)	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115

Kabilang sa mga teknolohiyang tatalakayin sa mga pagpupulong ang:

Transportasyon (Pagpupulong 2 at 5)	**Departamento ng Bumbero** (Pagpupulong 2 at 5)	**Departamento ng Pulisya** (Pagpupulong 1, 3, at 4)
Mga Camera sa Trapiko at License Plate Readers (Mga Tagabasa ng Lisensyadong Plaka)	Mga Camera sa Pinangyarihan ng Emergency at Mga Camera ng Hazmat	Mga Sistema sa Pagpapatupad ng Tamang Pagpaparada at Mga Automated License Plate Reader (Mga Awtomatikong Tagabasa ng Lisensyadong Plaka)

Narito ang mga paraan kung paano ka makapagbibigay ng mga komento:

Ang panahon ng bukas na pagkokomento para sa mga teknolohiyang ito ay mula **Oktubre 8 - Nobyembre 5, 2018.** May tatlong paraan upang makapagkomento:

1. Dumalo sa pulong. Tingnan ang talahanayan sa itaas para sa mga lokasyon at oras.
2. Magsumite ng komento online sa **seattle.gov/privacy**.
3. Magpadala ng liham sa Attn: Surveillance & Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.

Isasama ang anumang isinumiteng komento sa huling Surveillance Impact Report (Ulat sa Epekto ng Pagmamanman) na isusumite sa Konseho ng Lungsod at isasapubliko. Upang makapagbigay ng komento pagkalipas ng panahong ito, makipag-ugnayan sa mga kawani ng Konseho ng Lungsod sa **seattle.gov/Council**.

Mangyaring tandaan, ang pulong na ito ay:

Ire-record sa video.

Hihingi ng tala ng pag-sign in ng mga dadalo.

Mangongolekta ng mga komento ng publiko:

Para sa mga pangangailangan sa pagpupulong: Mangyaring ipaalam sa amin kung kailangan mo ng mga serbisyo sa pagsasalin ng wika o iba pang serbisyo **dalawang linggo bago ang petsa ng pagpupulong** sa pamamagitan ng pagpapadala ng email sa **Surveillance@seattle.gov**.

City of Seattle

공개 회의 통지
감시 기술 여론 수렴

본 회의는 과거 획득된 감시 기술에 대한 제1차 여론 수렴 회의입니다. 본 기술 또는 Surveillance Ordinance(감시 조례 관련) 자세한 정보는 **seattle.gov/privacy**를 참조해 주시기 바랍니다.

	회의1	회의2	회의3	회의4	회의5
발표 부처	경찰국	교통국, 소방국	경찰국	경찰국	교통국, 소방국
날짜 및 시간	2018년 10월 22일 5-6:30 p.m.	2018년 10월 25일 5-6:30 p.m.	2018년 10월 29일 5-6:30 p.m.	2018년 10월 30일 5-6:30 p.m.	2018년 11월 5일 4:30-5:30 p.m.
장소	**Columbia City Branch Library** 4721 Rainier Ave S, Seattle, WA 98118	**American Legion Hall: West Seattle** 3618 SW Alaska St. Seattle, WA 98126	**Bertha Knight Landes Room** 1st Floor City Hall - 600 4th Ave, Seattle, WA 98104 (5th Ave door)	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115

회의에서 논의되는 기술 항목:

교통국(회의 2 & 5)	**소방국** (회의 2 & 5)	**경찰국** (회의 1, 3, & 4)
교통 카메라 및 번호판 판독기	응급 현장 카메라 및 Hazmat 카메라	주차 단속 시스템 및 자동 번호판 판독기

의견 전달 방법:

상기 기술에 대한 공개 의견 기간은 **2018년 10월 8일~11월 5일**입니다. 의견 전달 방법은 다음 세 가지입니다.

1. 회의에 참석합니다. 장소 및 시간은 상기 표를 참조해 주십시오.

2. 의견은 온라인 **seattle.gov/privacy**로 제출해 주십시오.

3. 우편 발송지: Surveillance & Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.

제출된 의견은 시의회에 전달되는 최종Surveillance Impact Report(감시 영향 보고서)에 수록되며 일반에게도 공개됩니다. 본 의견 수렴 기간 종료 후 의견을 제출하시려면, 시의회 담당 직원에게 **seattle.gov/Council**로 문의해 주시기 바랍니다.

회의 시 참고 사항은 다음과 같습니다.

비디오가 녹화됩니다. **참가 기록을 요청합니다.** **대중 의견을 수집합니다.**

회의 편의 제공: 언어 번역 또는 기타 서비스가 필요한 경우 **회의 개최일 2주 전**에 **Surveillance@seattle.gov**로 이메일을 보내 당국에 알려 주시기 바랍니다.

City of Seattle

APPENDIX D: MEETING SIGN-IN SHEET(S)

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☑ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☑ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☑ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☒ Female
☐ Central	☒ North	☐ Black or African American	☒ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☑ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☑ Northeast	☐ American Indian or Alaska Native	☑ 45-64	☐ Transgender
☐ East District	☐ Southeast	☑ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☑ Ballard	☐ Lake Union	☑ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☑ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☒ North	☐ Black or African American	☒ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☒ Female
☒ Central	☐ North	☐ Black or African American	☒ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☒ Female
☒ Central INTERNATIONAL DIST/CHINATOWN	☐ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☒ Asian	☒ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

10-22-18 - LIBRARY

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☑ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☑ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest Rainier Beach	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☒ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☒ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☒ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☒ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☑ White	☐ Under 18	☑ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☑ 45-64	☐ Transgender
☐ East District	☑ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☑ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☑ 45-64	☐ Transgender
☐ East District	☑ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☑ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☒ North	☐ Black or African American	☒ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☑ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☑ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☑ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☒ North	☐ Black or African American	☒ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☒ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☐ Central	☒ North	☒ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☒ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☒ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

QA

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☒ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☒ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☒ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☒ Female
☒ Central	☐ North	☒ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☒ Central	☐ North	☐ Black or African American	☒ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☒ Female
☐ Central	☐ North	☐ Black or African American	☒ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify outside of King Co		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☒ Female
☒ Central	☐ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☒ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☒ Female
☑ Central	☐ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☒ Asian	☒ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☐ Central	☑ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☑ Asian	☑ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☑ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☑ White	☐ Under 18	☐ Female
☑ Central	☐ North	☐ Black or African American	☑ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☑ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☒ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☒ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☑ Ballard	☐ Lake Union	☑ White	☐ Under 18	☑ Female
☐ Central	☐ North	☐ Black or African American	☑ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☒ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☒ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☒ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☒ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☐ Central	☑ North	☐ Black or African American	☐ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☑ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☑ White	☐ Under 18	☐ Female
☑ Central	☐ North	☐ Black or African American	☑ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☑ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☑ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☑ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☑ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☑ North	☐ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☑ Female
☑ Central	☐ North	☑ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☑ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☑ Female
☑ Central	☐ North	☑ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☑ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☒ Central	☐ North	☒ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☒ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☒ Central	☐ North	☒ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☐ Central	☐ North	☒ Black or African American	☐ 18-44	☒ Male
☒ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☒ Central	☐ North	☒ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☒ Central	☐ North	☒ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☒ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☒ Female
☒ Central	☐ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☒ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☑ White	☐ Under 18	☒ Female
☑ Central	☐ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☑ 18-44	☑ Male
☐ Delridge	☐ Northeast	☑ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

International District

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☑ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☑ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

CID

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☒ South Seattle CID				
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☐ Central	☑ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☑ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☑ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☑ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☑ Female
☐ Central	☐ North	☐ Black or African American	☑ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☑ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☑ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

APPENDIX E: ALL INDIVIDUAL COMMENTS RECEIVED

ALL COMMENTS RECEIVED ON PARKING ENFORCEMENT

ID: 87

Submitted Through: Focus Group 2

Date: 11/20/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Saves money on chalk

ID: 86

Submitted Through: Focus Group 2

Date: 11/20/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Good idea

ID: 85

Submitted Through: Focus Group 2

Date: 11/20/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Belltown – has signs letting drivers know how many spots are available

---

ID: 84

Submitted Through: Focus Group 2

Date: 11/20/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Hopes it doesn't replace police or PEO

ID: 83

Submitted Through: Focus Group 2

Date: 11/20/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Good means for enforcing parking scoff laws

ID: 82

Submitted Through: Focus Group 2

Date: 11/20/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Understanding parking rules is hard – Don't want to give up revenue from tickets by removing parking for visitors/tourists

---

ID: 81

Submitted Through: Focus Group 2

Date: 11/20/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Happy about mitigation for people living in vehicles

ID: 80

Submitted Through: Focus Group 2

Date: 11/20/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Long term parkers were hogging parking and cause problems

ID: 79

Submitted Through: Focus Group 2

Date: 11/20/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Business owners like enforcement of parking law – turn over rates. Effective enforcement is a positive.

ID: 58

Submitted Through: Focus Group 1

Date: 11/8/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement Systems

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Police should get with the community and let them know whats going on

Do you have any other comments?

ID: 56

Submitted Through: Focus Group 1

Date: 11/8/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement Systems

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Don't commit the violation

Do you have any other comments?

Car in my neighborhood that has been parked over a year, call it in twie before, and no boot

---

ID: 3

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

Privacy concerns in general. Potential privacy impact, will those in program be notified?

What value do you think this technology brings to our city?

What worries you about how this is used?

Large collection in a database of innocent persons is troubling

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Large amount of data collected for a small percentage of hits

---

ID: 4

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

There is a lot of data collection, but a small number of 'hits'. Therefore, is the technology worth it?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Like to see alignment between data collection policies and the intelligence ordinance.

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Is the risk/benefit of the technology really worth being surveilled, given the number of 'hits' vs. how much data is collected

---

ID: 5

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

Scalability--this isn't a really scalable technology.

What value do you think this technology brings to our city?

Brings order to the City

What worries you about how this is used?

The system may make mistakes. Also there should be correlation between databases (i.e. between the hit and the verification).

What recommendations would you give policy makers at the City about this technology?

Have better integration between systems. Also, use a technology, or allow this technology, to scale up or that is scalable

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 7

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

Selective use of technology (i.e. RV parking)

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Personal experience of criminals swapping plates and I got pulled over without realizing plates were swapped on my car.

ID: 16

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

Targeting certain areas and populations

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Where they are deployed/distributed and how needs to be more transparent and equitable

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 17

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

Greater distress and economic and community impact from higher enforcement of low-income residents

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Provide better research and method and evaluation for distribution. For example, random assignment test equity impact assessment.

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 18

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

Inconsistent enforcement

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Use the money for transit instead

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 19

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

What is gained (revenue, enforcement) may not offset privacy needs

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Encourage development of policy on how PDR's get released

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 20

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

Potential risk of wireless hacking to get at the information

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 21

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

Red level of alert (for patrol vehicles) doesn't clarify differences

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 22

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

Need public information of procedures for responding to the data

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 37

Submitted Through: Meeting 3

Date: 10/29/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

Autovu datais deletede in a day, but PIPs data is retained for 90 days

What value do you think this technology brings to our city?

The value of keeping the data is that you can find a missing person or an abducted person.

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 47

Submitted Through: Meeting 4

Date: 10/30/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

Great for parking enforcement

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Once parking ticket is paid record / data deleted

Can you imagine another way to solve the problem this technology solves?

Could be done manually but lots of time

Do you have any other comments?

ID: 38

Submitted Through: Meeting 4

Date: 10/30/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement including ALPR

Do you have concerns about this specific technology or how it is used?

If records are kept after a fine is paid.

What value do you think this technology brings to our city?

Relieving writer's cramp ad tedium

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Severe consequences for official mischief

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 10333776204

Submitted Through: Survey Monkey

Date: 11/7/2018 5:57:15 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Parking Enforcement Systems

Do you have concerns about this specific technology or how it is used?

Lack of clarity regarding the data retention from the ALPR cameras used by parking enforcement. Different parts of the draft SIR referred to different lengths of time (90 days - same as patrol ALPR data vs data deleted at end of shift/day unless it was explicitly saved in correlation to an active investigation). If all the parking enforcement ALPR data not involved with an investigation is indeed deleted at the end shift/day, then I'm not concerned. If some (again non-active-investigation) data is retained for 90 days, then I have the same concerns/worries/recommendations/etc as the feedback previously given regarding ALPR usage by Patrol.

What value do you think this technology brings to our city?

What worries you about how this is used?

See #2 above.

What recommendations would you give policy makers at the City about this technology?

Ensure the data retention for all non-investigation parking enforcement ALPR data is only til end of shift/day. If not, see recommends given for ALPR used by Patrol.

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

While I appreciate the time extension that was given for public comments, I do feel like the overall public review period was too short and the community meetings should be more spaced out to give people with competing schedules a chance to block off time so they can attend in person.

ALL COMMENTS RECEIVED ON GENERAL SURVEILLANCE

ID: 66

Submitted Through: Focus Group 1

Date: 11/8/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

no. Glad some surveillance is being used.

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 65

Submitted Through: Focus Group 1

Date: 11/8/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Technologies discussed are less dangerous then some other technologies in our personal lives

---

ID: 63

Submitted Through: Focus Group 1

Date: 11/8/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

not a lot of privacy anymore: google earth, maps, streetview

What value do you think this technology brings to our city?

What worries you about how this is used?

Google home is always listening. There is always someone listening to your conversations.

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Some of the images you can find online appear to be voyerism

ID: 61

Submitted Through: Focus Group 1

Date: 11/8/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Street sweepers coming in the middle of the night are ineffective, cars are parked and blocking areas

---

ID: 60

Submitted Through: Focus Group 1

Date: 11/8/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

Sometimes too much surveillance

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Curious about how much construction has to pay when blocking off half a block for parking.

ID: 56

Submitted Through: Mail

Date: 10/23/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Surveillance. I don't want it. Any of it. Just stop.

ID: 28

Submitted Through: Meeting 2

Date: 10/25/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Can you please do a better job telling the public about these meetings? Targeted Ads? KUOW - helped, Blogs, Newspaper - Poor turnout

---

ID: 27

Submitted Through: Meeting 2

Date: 10/25/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Most too technical and need to communicate better with public

---

ID: 26

Submitted Through: Meeting 2

Date: 10/25/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

Concerned about aggregation of technology and data collected

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

More transparent; less defnesive is how you gain trust

ID: 25

Submitted Through: Meeting 2

Date: 10/25/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

KC Parcel viewer information is too much. State listings of addresses of voters is a problem. Too much info has impact on DV victims - keeping them from voting

---

ID: 24

Submitted Through: Meeting 2

Date: 10/25/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Work and Human Rights Activist- Process too complicated. Can be benign but SPD doesn't make dark usage more clear. Info is too complex/data need better education for public on technologies.

ID: 23

Submitted Through: Meeting 2

Date: 10/25/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

No concerns as a professor. Traffic is getting worse - how do we make imporvements. How do we use data in other ways to improve our lives?

What value do you think this technology brings to our city?

Impressed by how City handles data - Check it and Chuck it

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Spent time on dark web and stunned by what they can do

ID: 53

Submitted Through: Meeting 4

Date: 10/30/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

People lose track of "public service" being performed. Misuse of data

---

ID: 52

Submitted Through: Meeting 4

Date: 10/30/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Hate to go "China route" tied to credit

ID: 51

Submitted Through: Meeting 4

Date: 10/30/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Restricted use: will it generate income? Mission creep. Report back to community

---

ID: 10334071978

Submitted Through: Survey Monkey

Date: 11/7/2018 9:41:13 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

Yes

What value do you think this technology brings to our city?

Minimal

What worries you about how this is used?

Very concerned about how red light enforcement cameras are racially unjust and frequently cause tickets to be issued to people of color.

What recommendations would you give policy makers at the City about this technology?

Remove red light cameras, if a particular intersection requires policing then assign officers to be posted there to create a presence that can be seen.

Can you imagine another way to solve the problem this technology solves?

Use officers in cars.

Do you have any other comments?

Red light cameras create an unjust, racially imbalanced burden on blacks, latinos and other marginalized groups. They should be eliminated from the city.

ID: 10328244312

Submitted Through: Survey Monkey

Date: 11/5/2018 8:41:00 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

We, the Critical Platform Studies Group, are a collective of researchers at the University of Washington Information School conducting a third-party ethnographic research study of the Seattle Surveillance Ordinance. In our ongoing research, we are conducting interviews with stakeholders on the processes leading to the revised Seattle Surveillance Ordinance. We have also compared the law to similar U.S. initiatives, and analyzed the functionality of each technology covered by Seattle's ordinance. Despite the salience of algorithmic processes in surveillance technologies, we are finding that the ordinance does not describe or address machine learning, artificial intelligence (AI), or algorithmic bias. We conclude that there is a pressing need for attention to algorithmic bias within disclosed surveillance technologies, for which we suggest additional elements be added to Seattle Surveillance Impact Reports, or by expanded stakeholder engagement in the RFP stage of the procurement process. Our preliminary findings that lead to these recommendations are as follows: *Expanded use of technologies triggers new surveillance review*: The Seattle ordinance models a strong process for submitting a given to

technology to further review in the event its functionality or uses are expanded. *Law motivated by concern for marginalized groups*: The motivation for the Seattle Surveillance Ordinance was to protect groups that have historically been targeted by surveillance programs. Given that the implicit biases that have been demonstrated to exist in algorithmic systems invariably affect marginalized groups, it is critical to consider the algorithmic aspects and potential algorithmic biases in disclosed surveillance technologies. *Gap between perception and reality of current machine learning use*: Three municipal employees familiar with the Surveillance program stated that machine learning technologies are not used in technologies on the Master List. Contrary to these statements we found that at least two technologies on the Master List rely on machine algorithms---Automated License Plate Recognition (ALPR) and Booking Photo Comparison Software (BPCS). We found that at least two other technologies on the Master List rely on AI technology that could also be used long term in a way that implicates protected groups---i2 iBase and Maltego. The reliance on machine learning technologies likely introduces algorithmic bias, such as through "false positive" identifications. *Absence of algorithmic considerations in other surveillance ordinances*: None of the six municipal surveillance ordinances we surveyed included language for wrestling with algorithmic bias. *Opportunity to strengthen existing processes*: The Seattle Surveillance Impact Reports could include questions or prompts that would target and stimulate investigation into machine learning / AI facets or into algorithmic bias in disclosed surveillance technologies.

ID: 10326819811

Submitted Through: Survey Monkey

Date: 11/5/2018 9:14:43 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

Adaptive signal technology does not seem ready for a multimodal city where bikes/pedestrians need priority.

What value do you think this technology brings to our city?

It can potentially improve mobility and that has certainly been demonstrated for cars at least.

What worries you about how this is used?

It doesn't account for bikes or pedestrians or requires some sort of additional effort (like installing an app) to work for those groups.

What recommendations would you give policy makers at the City about this technology?

Are these technologies helping or hurting the vision zero goals?

Can you imagine another way to solve the problem this technology solves?

I would question whether cars being in gridlock is a problem that can be solved or simply a consequence of the culture that we are encouraging in a dense city.

Do you have any other comments?

ID: 10326707921

Submitted Through: Survey Monkey

Date: 11/5/2018 8:38:49 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

No

What value do you think this technology brings to our city?

As our population grows this is the only way to enforce laws as we don't have enough police to do it

What worries you about how this is used?

None. If you're abiding by the law you have nothing to fear

What recommendations would you give policy makers at the City about this technology?

Allow police to use it to their advantage to do their job to keep us all safe, but don't use it against them!

Can you imagine another way to solve the problem this technology solves?

Create an environment that would make police want to stay in Seattle and do the job they were hired to do.

Do you have any other comments?

See above

ID: 10324587536

Submitted Through: Survey Monkey

Date: 11/4/2018 3:55:12 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

License plate cameras in general, I'm supportive of, if they can be used at greater frequency to crack down on illegal parking and driving.

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Full steam ahead! Bus lane camera on every bus, so that operators can push a button to send video of an illegal bus lane violator or other moving/parking violations when they see one, to get folks to drive better.

Can you imagine another way to solve the problem this technology solves?

Literally no.

Do you have any other comments?

I have no worries about these technologies. Get bus cameras online ASAP.

ID: 10322210731

Submitted Through: Survey Monkey

Date: 11/2/2018 9:47:34 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

This is government overreach and Big Brother at it's finest. Surveillance technologies do not belong in a free society and are solely implemented to farm money from taxpayers for minor infractions, at "best".

What value do you think this technology brings to our city?

None; outside of the ticket-issuing racket.

What worries you about how this is used?

Law Enforcement will abuse this technology. As a prior victim of stalking at the hands of a Law Enforcement Officer, we don't need to give Police more surveillance tools which make it easier to harass citizens.

What recommendations would you give policy makers at the City about this technology?

Do not turn Seattle into Singapore, China, or the United Kingdom. America is The Land of the Free. We don't want to be under the Watchful Eye of Big Brother.

Can you imagine another way to solve the problem this technology solves?

Use your eyes and have officers enforce the law as needed.

Do you have any other comments?

Robots are not Sworn Officers of the Law. SPD should be writing tickets, not computers. This technology will likely be abused, it will violate privacy laws, and I don't trust the Government to keep secure such a Mass Surveillance system. The costs of securing and maintaining such a system will require massive amounts of artificial "ticketing". At best, this is a Perpetual Revenue Generator for City Hall; at worst, it's a Gross Violation of Our Civil Rights.

ID: 10315099454

Submitted Through: Survey Monkey

Date: 10/30/2018 7:57:58 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

No

What value do you think this technology brings to our city?

Hi it brings proof. It impacts crime before it occurs.

What worries you about how this is used?

Mone

What recommendations would you give policy makers at the City about this technology?

Where you see lots of camera you see less crime.

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 10314183202

Submitted Through: Survey Monkey

Date: 10/30/2018 12:34:32 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

The location of the cameras/where the police vans circulate can be racially discriminatory. The city should make sure that these are distributed equitably.

What recommendations would you give policy makers at the City about this technology?

If the city is already going to be placing these cameras, they should also use these cameras to enforce speeding violations. Cars are always driving dangerously fast in this city, and these cameras should also make people follow the law.

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 10312185174

Submitted Through: Survey Monkey

Date: 10/29/2018 7:45:04 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

Yes

What value do you think this technology brings to our city?

What worries you about how this is used?

Over-policing. Waste of tax money. City government probably isn't sufficiently organized or skilled to process and analyze the data collected. It will ultimately lead to more overly bureaucratic, under-skilled, departments hopelessly trying to learn how to use the equipment and manage a massive records collection. The City should think twice before tying their shoes together on this one. It won't turn out well. I suggest you save yourselves the headache and bad PR by abandoning any surveillance plans now.

What recommendations would you give policy makers at the City about this technology?

Fire whoever is responsible for trying to waste tax money on invasive surveillance equipment. Also, whoever wrote question #6 should take a course on writing unbiased survey questions because the question assumes that the proposed surveillance equipment in fact solves a problem but that is not an established truth.

Can you imagine another way to solve the problem this technology solves?

This is a loaded question. It does not solve a problem. It creates an IT nightmare, costs way too much to store the data, invasive surveillance, and bad PR. Eventually, someone involved will likely lose a future election as a result.

Do you have any other comments?

ID: 10312163737

Submitted Through: Survey Monkey

Date: 10/29/2018 7:35:08 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

Yes, I don't agree on public surveillance. This is America not China!

What value do you think this technology brings to our city?

I think it strips me from my right as a citizen and make me feel like the whole country is big huge jail

What worries you about how this is used?

How it's interpret and what people of color will have to go through to not been punished for small and trivial crimes.

What recommendations would you give policy makers at the City about this technology?

We're not ready, this is not London. Don't do it!

Can you imagine another way to solve the problem this technology solves?

I don't think it's solving a problem as much as it's creating one.

Do you have any other comments?

Don't do it!

ID: 10310577035

Submitted Through: Survey Monkey

Date: 10/29/2018 8:13:55 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

Yes, the police are not honest about how and when they use this technology which means they are violating the 4th amendment rights which is a federal offense. Are they held accountable? No, almost never.

What value do you think this technology brings to our city?

The percentage of crimes solved with these technologies is a very small amount. And violating 4th amendment rights is a normal act by police in many of those instances.

What worries you about how this is used?

I support the pursuit of justice to make our city safer but but lawful citizens and criminals all have rights which the police disregard because there is no price to pay. If you could cheat and got caught doing so but there was no consequences, why wouldn't you? Its examples like this in our leaders, public officials and public servants that have eroded society and the trust people in each other.

What recommendations would you give policy makers at the City about this technology?

Until we have good honest leaders at the top who oversee the ones who use these technologies and who have no bias about who is held accountable for violations of ANY kind, they should be sidelined.

Can you imagine another way to solve the problem this technology solves?

Good morals and the respect for your fellow humans. It starts with the people on top to set good examples. We as a society have gotten more numb to violence, dishonesty and corruption at the highest levels ,it has now sown itself into our way of life. If we see this kind of behavior from the people that are "roll models" or "leaders" then we adopt them as our own values.

Do you have any other comments?

Unfortunately, corruption is widespread in government agencies and public enterprises. Our political system promotes nepotism and wasting money. This has undermined our legal system and confidence in the functioning of the state. Communism is the corruption of a dream of justice.

ID: 10307049643

Submitted Through: Survey Monkey

Date: 10/26/2018 7:08:32 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

I need the red light cameras NOT to have flash equipment on them. These lights are too bright, and they flash without warning, blinding people on the sidewalks at intersections.

What value do you think this technology brings to our city?

Damn all. It may be that drivers get citations--but this does not compensate for the blinding of pedestrians, bicyclists, etc.

What worries you about how this is used?

I have several times been so bedazzled and startled that I might easily have stumbled into traffic, if I'd chanced to be closer to the curb.

What recommendations would you give policy makers at the City about this technology?

Get cameras that don't need so much light, if you INSIST on having such cameras.

Can you imagine another way to solve the problem this technology solves?

Since I don't think it solves anything, no.

Do you have any other comments?

Other cameras are intrusive and invasive--but they're not so immediately dangerous, generally.

ID: 10307028243

Submitted Through: Survey Monkey

Date: 10/26/2018 6:42:15 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

None of these technologies are novel, particularly compared to other parts of the world (Europe, Asia). However, the use of the automated parking enforcement technology specifically for the purpose of booting cars is of highly questionable value.

What value do you think this technology brings to our city?

Hopefully some efficiencies in reducing human effort required to perform basic data-gathering and enforcement. If the parking enforcement buggies can cover many more blocks in a day, or a police officer yanks someone out of a car that's actually stolen, great!

What worries you about how this is used?

Abuse of data access, lax enforcement of retention and removal-of-access policies, above SECURITY BREACH OF DATA that may be useful in some level of identification (car with plate X was seen at location Y at time Z). Be wary of social justice impacts, particularly of the auto-boot technology. Those who are the most vulnerable may be in more frequently trouble with the law (and absolutely unable to rectify fines) and would thus unable to reach services. It would be absolutely unacceptable if a vulnerable member of the population who may be living in a vehicle is booted and unable to access basic human services, or worse.

What recommendations would you give policy makers at the City about this technology?

Data security is of paramount importance -- if data cannot be handled safely by the right people at the right time with prompt removal processes for data and access, then none of this matters and the public trust is gone. If there are any questions about this whatsoever, do not proceed with adoption. After that is transparency. Be specific about what is gathered, down to individual data elements: publicly post the data schemas (but obviously not the data). E.g., when your license plate is recorded, it also gathers: date, time, location, and so on. Finally, policies about use must be clearly understood by the public and the civil servants the tech is entrusted too. "SPD may use tech [when] for [reason] in order to perform duty [elaborate]." "SDOT uses these cameras to perform analysis of [condition]". People care

about access and retention policies in this day and age -- post them and perform routine audits no less than quarterly but ideally more often than that (again, posting results publicly).

Can you imagine another way to solve the problem this technology solves?

Drone-mounted cameras can be used to gather movement data for travel time analysis; this doesn't require the use or exposure of any identifying marks whatsoever. They may also be helpful for SFD response scenes to perform rapid large area surveys.

Do you have any other comments?

Addressing these topics with serious care and thoughtfulness raises chances of success. Be intentional about uses of these technologies and do not allow for hidden uses.

ID: 10307002973

Submitted Through: Survey Monkey

Date: 10/26/2018 6:13:10 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

Not particularly

What value do you think this technology brings to our city?

CCTV makes this city safer, particularly since we are so short of police officers.

What worries you about how this is used?

Nothing

What recommendations would you give policy makers at the City about this technology?

Beat policemen are better.

Can you imagine another way to solve the problem this technology solves?

Policemen/women who walk or ride bikes in the same neighborhood on a daily basis. We've all read English novels. Doesn't the bobby on his beat seem like the best way to protect a neighborhood, and make a neighborhood feel safe?

Do you have any other comments?

I've lived in Ballard for 35 years. In the last five years I've put grates on my windows, bought a wrought-iron screen door, locked the gate to the backyard. This is after the theft of my bicycle from my shed, shoes from my porch, etc. Opioids. The government is cracking down on doctors who overprescribe. How about cracking down on street drug dealers as well? If a bath tub is overflowing from two spigots going full blast, turning off only one of those spigots doesn't work. Gotta turn off both.

ID: 10306958976

Submitted Through: Survey Monkey

Date: 10/26/2018 5:25:35 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

I do have concerns. However, if there is public oversight of the surveillance technology used, both by elected officials and through releases of content recorded to the general public, then these concerns will be sufficiently addressed.

What value do you think this technology brings to our city?

I think this has the ability to automate many of the services currently done by the city. Further, it can provide hard evidence of events that occurred which human testimony cannot do.

What worries you about how this is used?

I am worried that these systems could be used by its operators to spy on people they know or to blackmail individuals both known and unknown to the operators. The accountability to elected officials and through releases to the public would prevent these things from happening.

What recommendations would you give policy makers at the City about this technology?

Make sure there is actual transparency and accountability to the general public and the press, and make sure this technology is about automation and providing evidence, not to keep tabs on people.

Can you imagine another way to solve the problem this technology solves?

no

Do you have any other comments?

ID: 10303980026

Submitted Through: Survey Monkey

Date: 10/25/2018 12:46:20 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

I have concerns about the validity of Seattle's privacy program after listening to Seattle's Chief Privacy Officer on KUOW today. Per Ordinance 125376, greykey (the ability for the Seattle Govt to unlock iphones without having the password) should have been reviewed by the Privacy Officer Armbruster, but it wasn't and she provided no explanation why. She offered no apology. This lacks transparency and accountability.

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 10300614662

Submitted Through: Survey Monkey

Date: 10/24/2018 9:04:59 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

yes

What value do you think this technology brings to our city?

On a world level, at the federal government level, and at the city level we move closer towards fascism and other forms of authoritarianism, expanded surveillance will give expanded power to authoritarian regimes such as ours.

What worries you about how this is used?

The list of technologies for surveillance should include all other 'law' inforcement agencies at work in our city such as ICE.

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

As I sat down on the Seattle Trolley on Jackson Street a drone flew up and held stationary and then titled slightly up. The blue lens of a camera flashed and the drone banked off. I'd like to know what other technologies are at use in our city, by ICE for instance as well as other 'law' agencies.

ID: 10299219171

Submitted Through: Survey Monkey

Date: 10/23/2018 7:14:36 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

in general I'm concerned about the collection, retention, aggregation, sharing, and mining of information collected thru surveillance technologies, particularly with regard to the risk for abuse by agencies like ICE or other yet-to-be created Federal agencies that do not represent the views of the Seattle area population.

What value do you think this technology brings to our city?

Emergency Scene cameras give medical professional an opportunity to prepare for treating emergencies and protect first responders from frivolous lawsuits. Hazmat cams gather information while allowing humans to remain at a safe distance. The rest of them essentially allow the city to more effectively collect revenue, except for ALPR, which scans licenses in search of stolen cars or vehicles sought for other reasons.

What worries you about how this is used?

ALPR is essentially a surveillance dragnet. Data is retained for 90 days even on vehicles that have nothing to do with anything.

What recommendations would you give policy makers at the City about this technology?

Do not retain any ALPR data except that which pertains to tagged vehicles. In general, always err on the side of not collecting data, not storing it, and not sharing it. Please. I work for Google.

Can you imagine another way to solve the problem this technology solves?

Fund transportation infrastructure so we don't have so many cars on the road running traffic lights and hitting pedestrians and cyclists and being driven by drunks.

Do you have any other comments?

Thank you for the opportunity to comment.

ID: 10298281561

Submitted Through: Survey Monkey

Date: 10/23/2018 11:18:38 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

It seems like all of these technologies are primarily focused on the movement of vehicles through Seattle instead of pedestrians and their own needs

What value do you think this technology brings to our city?

Giving the illusion of gathering useful, but inactionable, data.

What worries you about how this is used?

general privacy concerns about collecting so much data. There's no such thing as perfect security, to say the least.

What recommendations would you give policy makers at the City about this technology?

Use it to benefit the most vulnerable road users: pedestrians, including cyclists and other small transport methods/vehicles.

Can you imagine another way to solve the problem this technology solves?

Does it solve things? It's a bit early to say that.

Do you have any other comments?

Stop focusing on car throughput, and instead focus on people.

ID: 10298170617

Submitted Through: Survey Monkey

Date: 10/23/2018 10:37:29 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

Can you quantify the # of crime investigations, stolen cars recovered and $ amount of traffic violations recovered by using the ALPR/LPR technology.

What value do you think this technology brings to our city?

I am concerned that we are trading our privacy for a "sense" of security. How have surveillance technologies incrementally affected our security in Seattle.

What worries you about how this is used?

slippery slope -- see "The Last Enemy" film

What recommendations would you give policy makers at the City about this technology?

I'd like to see more police body cams; less surveillance;

Can you imagine another way to solve the problem this technology solves?

I have not been convinced except in the case of the Fire Department technology that we are actually better off -- I need to see numbers.

Do you have any other comments?

I would like to see year over year numbers comparing "before technology - after technology"

ID: 10296707285

Submitted Through: Survey Monkey

Date: 10/22/2018 9:13:04 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

The public ought to be made aware of all surveillance technologies being used. In the case of permanent fixed surveillance devices such as cameras, the public should be readily able to find information about where all such devices are installed.

What value do you think this technology brings to our city?

The provided examples of traffic monitoring seem useful. However, a full-blown security system similar to the widespread CCTV coverage in London seems overly pervasive.

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Minimize the number of surveillance devices implemented, and make their locations available for online viewing by the public at any time. No surveillance devices should be installed without informing the public.

Can you imagine another way to solve the problem this technology solves?

Security cameras should be limited to guarding private property or specific locations of concern, and not used to generally monitor all public areas at all times.

Do you have any other comments?

ID: 10296428154

Submitted Through: Survey Monkey

Date: 10/22/2018 5:35:21 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 10295649414

Submitted Through: Survey Monkey

Date: 10/22/2018 11:24:46 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

I don't want any surveillance. Any of it. Let us live privately and in peace. Just stop.

What value do you think this technology brings to our city?

I don't want any surveillance. Any of it. Let us live privately and in peace. Just stop.

What worries you about how this is used?

I don't want any surveillance. Any of it. Let us live privately and in peace. Just stop.

What recommendations would you give policy makers at the City about this technology?

I don't want any surveillance. Any of it. Let us live privately and in peace. Just stop.

Can you imagine another way to solve the problem this technology solves?

I don't want any surveillance. Any of it. Let us live privately and in peace. Just stop.

Do you have any other comments?

I don't want any surveillance. Any of it. Let us live privately and in peace. Just stop.

ID: 10295424650

Submitted Through: Survey Monkey

Date: 10/22/2018 10:02:24 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

SPD has proved over decades that it should BE constantly monitored, rather than be further enabled to abuse - the inseparable seduction of its under-controlled power.

What value do you think this technology brings to our city?

Surveillance tech further dehumanizes and commoditizes residents. A better SPD investment would be in outside beat walking and mingling with citizens.

What worries you about how this is used?

SPD is under Federal oversight due to its documented abuses. Its modus operandi are Trumpist (i.e. thrive only in the dark). We have witness where that tends.

What recommendations would you give policy makers at the City about this technology?

No Councilperson can adequately oversee or hold accountable her portfolio, let alone the Mishmash and Safe Communities octopus. Until proven effective governance by elected officials obtains, no greater powers should be distributed to SPD.

Can you imagine another way to solve the problem this technology solves?

The morality police in Iran and Saudi Arabia and the like in China demonstrate that everyday citizens are readily induced to spy and report on their neighbors. Although beyond the pale, a progressive version of neighborly support and assistance should be the direction Seattle pioneers to deal with the pressing problems of Mass Humanity.

Do you have any other comments?

One cannot "tech" to a humanitarian city, least of all through an insidiously equipped praetorian armed force. SPD elevates the interests of its minuscule membership above those of a citizenry whose dwarf it in all regards. City Council year-in/year-out approves the contracts cementing this folly. Seattle needs a formal goal of reducing its separate-but-armed constituency into the service element it should be, not the formidable power-center it is.

ID: 10295330166

Submitted Through: Survey Monkey

Date: 10/22/2018 9:29:06 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

Yes. We have crimes and shootings that occur in public areas where there is no reasonable expectation of privacy but we lack the info to respond effectively.

What value do you think this technology brings to our city?

By placing cameras in certain areas with frequent criminal activity we could both deter and aid in the arrest and prosecution of those responsible. The city is undergoing an epidemic of property crime and dumping of garbage in many areas. Cameras could help deter, aid in the arrest/fines and prosecution of those responsible.

What worries you about how this is used?

Very little. If used in public spaces there is no reasonable expectation of privacy. If there is concern about privacy or tracking, the data could be encrypted by default and then made available to police after an incident with a court order or approval of some oversight body.

What recommendations would you give policy makers at the City about this technology?

Hurry up and put cameras in place where it makes sense. If there are privacy concerns, implement some kind of a check on access but get moving.

Can you imagine another way to solve the problem this technology solves?

Not cost effectively.

Do you have any other comments?

ID: 10295152382

Submitted Through: Survey Monkey

Date: 10/22/2018 8:30:01 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

A person could be set up, I suppose. I just read that the journalist who was murdered in the embassy....well his ambushers had a double for him. Now whether this is true or not it could happen. Of course facial recognition might put a stop to imposters posing as someone else.

What value do you think this technology brings to our city?

Safety in public spaces is increased...although, it is sadly 'after the fact' that it is usually the most effective. I think that just the knowledge that you might be watched could deter criminal behavior or, for that matter, abuse by law enforcement. It works both ways. Also, if you had more speed detectors you could generate a lot of revenue with speeding tickets. I can't tell you the number of times I've had cars speed by me in neighborhoods where speed limits are 25 mph. I know police can't be everywhere...but cameras can be. People are much less respectful nowadays. I drive to neighborhoods all over Seattle 5 days a week as a caregiver and have people honking at me because I'm driving too slow for them. I wish I could take the Mayor along with me on some of my trips so she could see first hand how rude people can be.

What worries you about how this is used?

It will alleviate my worries about road rage....maybe make people feel safer walking about outside...especially those most vulnerable who stay cooped up in their homes too afraid to go outside.

What recommendations would you give policy makers at the City about this technology?

Please...more sir. I would love to see children outside playing...who aren't afraid of being outside playing...in quiet neighborhoods or parks. We need these cameras etc. if only to act as a babysitter in some respects.

Can you imagine another way to solve the problem this technology solves?

Change human nature....which is nearly impossible.

Do you have any other comments?

I'm sure there would be people who could try to use surveillance to watch women etc.....when I was younger I've had police pull me over I'm sure just to check me out...stupid weirdos....BUT there is a lot of good to be had with watching over the public for the public good

---

ID: 10291758143

Submitted Through: Survey Monkey

Date: 10/19/2018 2:19:06 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

No, I support surveillance cameras, even as I understand this is a tradeoff to privacy. But, CC TVs are widely accepted and extraordinarily helpful for law enforcement in other countries such as the UK.

What value do you think this technology brings to our city?

The ability to safeguard spaces and revisit victimizations.

What worries you about how this is used?

How long the data is kept. We should have a period of time that the data is kept after which it is destroyed.

What recommendations would you give policy makers at the City about this technology?

Adopt this widely.

Can you imagine another way to solve the problem this technology solves?

NO.

Do you have any other comments?

As a UW professor who studies law, I fully support better surveillance of our population--this includes police, citizens, and so on.

ID: 10287347565

Submitted Through: Survey Monkey

Date: 10/17/2018 9:55:10 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

No. Technology is ubiquitous; surveillance is everywhere. Technology plays a pivotal role in keeping our communities safe. The paranoia of some should be easily address by strong policies and auditing of use.

What value do you think this technology brings to our city?

Technology is critical to solving crime, deterring crime, and bringing criminals to justice, and providing closure to victims.

What worries you about how this is used?

I worry that it is not used enough. I live in the South End, yes, in a black community (I am black) and we have been pleading with the city (you, Councilmember Harrell) for cameras for years. The ACLU, and supposed "community activists", do not speak for the average among us who go to work, take our kids to school, and just want to live in a safe community.

What recommendations would you give policy makers at the City about this technology?

Lead. Do what you're paid to do. Protect the communities you serve, and allow - perhaps even enable - the police to keep our communities safe.

Can you imagine another way to solve the problem this technology solves?

A ridiculous question. If the city's not going to invest in a technological solution, why would the city invest in a lesser solution?

Do you have any other comments?

Please, do not hamstring our first responders anymore. Property crime is rampant. Auto theft is rampant. Our kids are being robbed on the street. And you want to TAKE AWAY tools to solve crime?? We want cameras - like we were promised, Councilmember Harrell. We want crimes solved, and deterred. Do not let absurdity rule the day.

ID: 10281389699

Submitted Through: Survey Monkey

Date: 10/15/2018 4:13:31 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

No

What value do you think this technology brings to our city?

Possible reduction in open street crimes

What worries you about how this is used?

May be comsidered not useful to detect crimes in low income communities.

What recommendations would you give policy makers at the City about this technology?

Use the technologies to cut down the kidnappers/rapist-- violent sex predators working and living in southend housing.

Can you imagine another way to solve the problem this technology solves?

Police patrols more often and seizure--not just showing up and leaving the scene.

Do you have any other comments?

The city seems to be over-run by kidnappers raping, I am getting sick to my stomach. Violent Sex Predators seem to be running the city via what I know.

ID: 10281279313

Submitted Through: Survey Monkey

Date: 10/15/2018 3:10:22 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 10273624842

Submitted Through: Survey Monkey

Date: 10/11/2018 1:35:22 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 10271359916

Submitted Through: Survey Monkey

Date: 10/10/2018 6:19:02 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

I think we need more. Especially at every bus stop.

What value do you think this technology brings to our city?

Hopefully catching criminals

What worries you about how this is used?

Nothing

What recommendations would you give policy makers at the City about this technology?

More cameras.

Can you imagine another way to solve the problem this technology solves?

No

Do you have any other comments?

ID: 10270768915

Submitted Through: Survey Monkey

Date: 10/10/2018 1:10:42 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

No

What value do you think this technology brings to our city?

I think it has great value in areas of high use, especially in areas where crime is historically reported. Both deterrent to crime and tool that helps law enforcement in the event crime has occurred.

What worries you about how this is used?

totally ok with it, as long as it's targeted in areas of heavy use, congested areas, high volume of people, areas with historically issues with crime, etc.

What recommendations would you give policy makers at the City about this technology?

Make sure law enforcement has real time access. Limit access to law enforcement type groups, don't get sidetracked as to possible other uses of the data.

Can you imagine another way to solve the problem this technology solves?

more police officers

Do you have any other comments?

Believe this is a cost effective way to help keep people safe.

ID: 10270556248

Submitted Through: Survey Monkey

Date: 10/10/2018 11:50:08 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

I do not want increased surveillance. License Plate Readers,

What value do you think this technology brings to our city?

None.

What worries you about how this is used?

Privacy and tracking concerns are rampant in an age where social media [LinkedIn] is almost required for a profession, a cell phone is required for jobs, and cars are required for jobs. StingRay [cell phone interceptor] has already been shown to be used unlawfully. I can only imagine a database version would be subject to equal lack of scrutiny.

What recommendations would you give policy makers at the City about this technology?

Vote no.

Can you imagine another way to solve the problem this technology solves?

Mountains out of molehills. Patrol HOV lanes.

Do you have any other comments?

Enforce HOV restrictions.

ID: 10270098107

Submitted Through: Survey Monkey

Date: 10/10/2018 9:10:36 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

ALPR/LPR: how is this technology used; if the data is being passively collected - how can the general public audit the back-end systems for sake of privacy (in the age of data breaches, this is a risk of *when* there is a breach and not *if*)

What value do you think this technology brings to our city?

Studies have shown that increased surveillance does not actually lead to reduced crime. More studies have also shown that community watch organisations do more to reduce crime than passive/active remote surveillance.

What worries you about how this is used?

Unclear duration of data usage, sharing and retention, and public request process to remove targeted data.

What recommendations would you give policy makers at the City about this technology?

Carefully evaluate vendors and their products to make sure the systems are hardened against breaches; evaluate whether the systems allow for public access to the data so that people can limit invasive surveillance.

Can you imagine another way to solve the problem this technology solves?

Better community education and watch programs. Try to find root causes of crimes and solve those causes. Surveillance is a short term gain with long term consequences and it doesn't address the problem of why crimes happen. Getting to the root cause may prove to be more productive (and in some cases, cost less public money)

Do you have any other comments?

ID: 10269149042

Submitted Through: Survey Monkey

Date: 10/10/2018 1:58:48 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

With all of these technologies, my main concern is unnecessary storage and retention. For example, what if you're storing some kind of information on people's cars, which then is acquired by ICE to prosecute undocumented individuals in spite of our city's sanctuary status?

What value do you think this technology brings to our city?

I believe there is value in the diagnostic capabilities, for example finding out what kind of traffic levels there are on a street or sidewalk, finding out how many bus lane cheaters there are, or maybe finding a pattern of frequent dangerous behavior on a street. In the same vein, I'm extremely supportive of having cameras on buses that bus operators can use to report bus lane violations because I think the level of bus lane violations we have is a serious impediment to our transportation system. I also appreciate that tech like this removes any prejudices that a police officer may have. Either you broke the law, or you didn't. I love that this tech will be used in parking enforcement. We need to enforce our traffic laws or nobody will care.

What worries you about how this is used?

Though it removes prejudice on the part of officers, I do also think this may be sub-optimal in some circumstances. Perhaps someone as speeding by only 1 mile per hour, which reasonably, we should let slide, but with cameras, we probably won't.

What recommendations would you give policy makers at the City about this technology?

Bus and bike lane camera enforcement, yes! You have no idea how many times some bus lane violators slow down a 60-person bus, or someone blocks the bike lane forcing me to make an unsafe movement. I'd also love to see box blocking or crosswalk blocking detection technology to prevent those things from happening because it seriously reduces the livability and safety of pedestrians and transit users. Don't have any facial recognition software though.

Can you imagine another way to solve the problem this technology solves?

I don't know how actionable this is, but maybe we could work with the judicial system to give the law a little bit of discretion on the prosecution of crimes, so for example if you're speeding by 1 mph, you don't get the same fine as someone speeding by 10 mph or 30 mph.

Do you have any other comments?

Please implement bus/bike lane enforcement cameras yesterday. I get there are challenges WRT privacy and whatnot, but if we're sensitive to these issues, we can make our city safer.

APPENDIX F: LETTERS FROM ORGANIZATIONS

Shankar Narayan
TECHNOLOGY AND LIBERTY PROJECT DIRECTOR

ACLU
AMERICAN CIVIL LIBERTIES UNION of WASHINGTON

October 24th, 2018

RE: ACLU-WA Comments Regarding Group 1 Surveillance Technologies

Dear Seattle IT:

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON
901 5TH AVENUE, STE 630
SEATTLE, WA 98164
T/206.624.2184
WWW.ACLU-WA.ORG

JEAN ROBINSON
BOARD PRESIDENT

KATHLEEN TAYLOR
EXECUTIVE DIRECTOR

On behalf of the ACLU of Washington, I write to offer the ACLU-WA's comments on the surveillance technologies included in Group 1 of the Seattle Surveillance Ordinance process. We are submitting these comments by mail because they do not conform to the specific format of the online comment form provided on the CTO's website, and because the technologies form groups in which some comments apply to multiple technologies.

These comments should be considered preliminary, given that the Surveillance Impact Reports for each technology leave a number of significant questions unanswered. Specific unanswered questions for each technology are noted in the comments relating to that technology, and it is our hope that those questions will be answered in the updated SIR provided to the City Council prior to its review of that technology.

The technologies in Group 1 are covered in the following order:

I. Automated License Plate Recognition (ALPR) Group

1. Automated License Plate Recognition (ALPR)(Patrol)(SPD)
2. Parking Enforcement Systems (Including ALPR)(SPD)
3. License Plate Readers (SDOT)

II. Camera Group

1. Emergency Scene Cameras (SFD)
2. Hazardous Materials (Hazmat) Camera (SFD)
3. Closed Circuit Television "Traffic Cameras" (SDOT)

I. ALPR Group

Automated License Plate Reader Systems (ALPRs) are powerful surveillance technologies that have the potential to significantly chill constitutionally protected activities by allowing the government to create a detailed picture of the movements—and therefore the lives—of a massive number of community members doing nothing more than going about their daily business. Indeed, at the first public meeting seeking comment on the SPD Patrol ALPRs, it was revealed that the ALPR system collected

1

37,000 license plates in a 24 hour period—which equates to over *13.5 million* scans over a full year. The overwhelming majority of these drivers are not suspected of any crime.

With this massive database of information, agencies can comprehensively track and plot the movements of individual cars over time, even when the driver has not broken any law. This enables agencies, including law enforcement, to undertake widespread, systematic surveillance on a level that was never possible before. Aggregate data stored for long periods of time becomes more invasive and revealing. Existing law in Seattle places no specific limits on the use of ALPR technology or data, meaning an agency can choose whether and how they want to retain data and track vehicle movements.

ALPR technology can be used to target drivers who visit sensitive places such as centers of religious worship, protests, union halls, immigration clinics, or health centers. Whole communities can be targeted based on their religious, ethnic, or associational makeup, and indeed, exactly that has happened elsewhere. In New York City, police officers drove unmarked vehicles equipped with license plate readers around local mosques in order to record each attendee as part of a massive program of suspicionless surveillance of the Muslim community. In the U.K., law enforcement agents installed over 200 cameras and license plate readers to target a predominantly Muslim community suburbs of Birmingham. ALPR data obtained from the Oakland Police Department showed that police there disproportionately deployed ALPR-mounted vehicles in low-income communities and communities of color. And the federal Immigration and Customs Enforcement agency has sought access to ALPR data in order to target immigrants for deportation. All of these concerns are magnified in light of a long history of the use of invasive surveillance technologies to target vulnerable communities (see, for example, Simone Browne's excellent, multidisciplinary book on the subject, *Dark Matters: On the Surveillance of Blackness*).

The foregoing concerns suggest the Council should ensure strong protections against the misuse of this technology, regardless of which agency is deploying it and for what purpose. Specific comments follow.

1. Automated License Plate Recognition (ALPR)(Patrol)(SPD)

The SIR relating to Patrol ALPRs raises a number of specific concerns around current policy and practice, and leaves open a number of significant questions. I attempt to capture these in sections below on concerns, questions, and recommendations.

a. Major Concerns

- *Inadequate Policies.* Policies cited in the SIR are vague, contradictory, and appear to impose no meaningful restrictions on the purposes for which ALPR data may be collected or used. Policy 16.170—the only apparent policy specific to ALPRs—for example, is very short, contains undefined terms, and focuses on training rather than use. Subsection 3 of the policy says that "ALPR Operation Shall be for Official Department Purposes" and that ALPR may be used "during routine patrol or any criminal investigation." This does not meaningfully restrict

the purposes for which ALPR may be used. And another part of the policy states that ALPR data may be accessed only when it relates to a specific criminal investigation—yet it is unclear how this relates to the enforcement of civil violations mentioned in both SPD SIRs. More generally, much of the practice described in the SIR does not appear to be reflected in any written policy at all (for example, the practice of manually verifying a hit visually is not reflected in policy).

- *Dragnet Use with No Justification.* While the SIR contains contradictory information on this point, it appears that ALPR cameras are always running, offering a vast dragnet of data collection. No legal standard is stated to justify this general, dragnet use. The Seattle Intelligence Ordinance is cited, but SPD seems to assume that dragnet surveillance is consistent with this Ordinance, without any specific policy (for example, are ALPR-equipped vehicles kept away from protests?).

- *Lengthy Retention Window with No Justification.* SPD retains ALPR data for 90 days, but examples given in the SIR of crimes solved using ALPRs largely appear to involve immediate matches against a hotlist. It is unclear what justifies this long retention window.

- *Data Sharing is Not Explicitly Limited by Policy or Statute.* The sharing of ALPR data with other agencies is of great concern, and SPD states a variety of situations in which such data may be shared (see SIR Section 6.1). But the policies cited do not make clear the criteria for such sharing, nor any inter-agency agreement that governs such sharing, nor why the data must be shared in the first place (see perfunctory answer to SIR Section 6.2). This issue of data sharing was raised in the enactment of the Surveillance Ordinance itself, and has only become more urgent under the current federal administration.

- *Inadequate Auditing.* The SIR appears to contradict itself on the subject of whether and how audits of inquiries to the system can be conducted (see SIR Sections 4.10 and 8.2, for example). As with any invasive surveillance system, a clear and regular audit trail to protect against abuse is important.

b. *Outstanding Questions*

I'm listing questions here that I hope will be answered in an updated SIR:

- To what degree are patrol and parking enforcement ALPR systems are separated, and do SPD policies on ALPR apply fully to the Parking Enforcement Systems? It appears the systems are merged at least to some extent, and in that case, the same strong protections against abuse should be applied to all systems.

- ALPR policy says there has to be a specific criminal investigation in order for ALPR data to be accessed. Does reasonable suspicion of a crime equate to a

specific criminal investigation? How is a specific criminal investigation documented?

- Under what agreements is data shared with outside agencies, and where "required by law," what specific laws require this sharing? To which systems outside SPD is data uploaded?

- How many plate images collected by the system every day? What is the hit rate on those images? Is there systematic data reflecting how many crimes each year are actually solved using ALPR data?

- How often do misreads occur? Are they systematically tracked?

c. *Recommendations*

These recommendations should be considered preliminary, pending answers to the questions above. But we urge the Council to ensure binding enforceable protections in ordinance that ensure the following minimum protections:

- Dragnet use and long retention of ALPR data should be outlawed. SPD must have reasonable suspicion that a crime has occurred before examining collected license plate reader data; they must not examine license plate reader data in order to generate reasonable suspicion. SPD should retain no information at all when a passing vehicle does not match a hot list (particularly given that such data is subject to public disclosure, including to federal agencies).

- People should be able to find out if plate data of vehicles registered to them are contained in SPD's ALPR database. They should also be able to access the data.

- There must be access controls on the ALPR databases, with only agents who have been trained in the policies governing such databases permitted access, and with every instance of access logged.

- SPD should not share any ALPR data with third parties without a written agreement ensuring that those third parties conform to the above retention and access rules, and should disclose to whom and under what circumstances the data are disclosed.

- Whenever a hit occurs, an officer, before taking any action, must confirm visually that a plate matches the number and state identified in the alert, confirm that the alert is still active by calling dispatch and, if the alert pertains to the registrant of the car and not the car itself, for example in a warrant situation, develop a reasonable belief that the vehicle's occupant(s) match any individual(s) identified in the alert.

- ALPRs should not be used for non-criminal enforcement purposes, other than parking enforcement.

- SPD should produce detailed records of ALPR scans, hits, and crimes solved specifically attributable to those hits, as well as an accounting of how ALPR use varies by neighborhood and demographic.

2. Parking Enforcement Systems (Including ALPR)(SPD)

Particularly given the partly merged nature of the parking enforcement and patrol ALPRs, including use of the parking enforcement ALPRs to check vehicle plates against hot lists, the concerns stated above with respect to SPD Patrol ALPRs apply equally to parking enforcement systems, and Council should ensure that the same minimum rules apply to them via ordinance—the intended primary use for parking enforcement does not in itself mitigate the concerns raised. In addition, the following outstanding questions should be answered in an updated SIR:

- It is unclear from the SIR how the Parking Enforcement ALPR systems integrate with the Patrol ALPR systems—it appears that some integration occurs at least in the case of the Scofflaw enforcement vans, that store collected data in the BOSS system. An updated ALPR should clarify specifically what rules apply to that data, and how they differ from rules applied to data collected by Patrol ALPR.

- A number of software and hardware providers are mentioned in Section 2.3 of the SIR—an updated SIR should clarify whether all contract directly with SPD itself, or with each other or a third party entity, to provide ALPR and related services.

- As with Patrol ALPR, statistics on numbers of scans, hits, and revenue from the systems would be helpful.

- Section 4.1 suggests pictures of the vehicle are being taken in addition to the plate—are these pictures stored, and if so, for how long?

- Concerns set forth in the section above relating to patrol ALPR regarding data access, clear standards for data sharing with third party entities and the purpose of such sharing, as well as auditing, all apply to these systems as well—and an updated SIR should clarify those standards.

3. License Plate Readers (SDOT)

The concerns stated above with respect to patrol ALPR largely apply to this set of ALPRs as well, with the additional concern of explicit sharing with a state entity. It is heartening that the SIR suggests that no license plate data is retained, but it is not clear whether that no-retention practice is reflected in policy. It is also unclear whether an explicit agreement exists with WSDOT ensuring deletion of the data and use only for the

purpose of calculating travel times. With that in mind, the following outstanding questions should be answered in an updated SIR:

- What explicit, written policies govern what SDOT and WSDOT can do with this ALPR data? Is there a written agreement with WSDOT requiring no personal data collection and deletion of all data?

- Under what circumstances might this data be used for law enforcement purposes? Is it possible for third parties to subpoena any data retained?

- What additional third parties get access to the data?

The Council should ensure by ordinance that the data collected is used only for the purpose of calculating travel times, that no data is retained, that no third party other than SDOT and WSDOT access the data at any time, and that a written agreement holds WSDOT to these restrictions.

II. Camera Group

Overall, concerns around this group of technologies largely focus on the use of these systems and the data collected by them for purposes other than those intended, over-collection and over-retention of data, and sharing of that data with third parties (such as federal law enforcement agencies). While the stated purposes of the cameras may be relatively innocuous, it is important to remember that images taken by such cameras, for example at emergency scenes, can compromise the privacy of individuals at vulnerable moments, and can be misused for the same kinds of targeting and profiling of particular communities detailed in Section I above. In addition, with the widespread and cheap availability of facial recognition technology, which can be applied after the fact to any image showing a face, it is all the more important that protections limiting the use of these tools to their intended purpose be enacted.

For all of these systems, the Council should adopt, via ordinance, clear and enforceable rules that ensure, at a minimum, the following:

- The purpose of camera use should be clearly defined, and its operation and data collected should be explicitly restricted to that purpose only.

- Data retention should be limited to the time needed to effectuate the purpose defined.

- Data sharing with third parties should be limited to those held to the same restrictions.

- Clear policies should govern operation, and all operators of the cameras should be trained in those policies.

Specific comments follow:

1. **Emergency Scene Cameras (ESCs)(SFD)**

The SIR for this technology states that no explicit internal policy exists at SFD that governs the use of ESCs, so a good start would be to create such a policy and include it in an updated SIR. This process should begin with an explicit list of specific uses for the ESCs, which are currently only set forth in general terms, and with apparent contradictions between sections of the SIR (for example, Section 1.0 describes three uses for the cameras, but Section 2.1 adds several more). In addition, the updated SIR should set forth any other internal internal policies and Washington laws governing use, retention, and disclosure of the data; where the data is stored; and which third parties, if any, have access to it, and for what purpose. (The SIR indicates data sharing with SPD, but the purpose is not clear.)

In turn, the Council should ensure via ordinance that no use is made of the images beyond the specific emergency, investigative, or training uses set forth, and that the data is deleted immediately upon completion of those purposes. Data sharing with third parties should be prohibited unless for those specific uses, and those third parties should be held to the same use and retention standards.

2. **Hazardous Materials (Hazmat) Cameras (SFD)**

As with ESCs, the SIR for Hazmat cameras indicates that no policy governing the use of this technology currently exists, with one limited exception for mechanism-of-injury recordings (see SIR Section 3.3). So similarly to ESCs, with this technology, an explicit policy that lists specific uses for the cameras should be created and included in an updated SIR. In addition, answers to questions such as who stores the data and which third parties have access to it should be made explicit. In particular, the SIR describes data sharing with law enforcement, but purposes of that disclosure are not made explicit (see SIR Section 4.7). In instances where a legal standard such as reasonable suspicion is applied, it should be clear what the standard is, who applies it, and how that application is documented. Overall, use of this technology should be limited to emergency response purposes, and any law enforcement use of the data should be restricted by ordinance.

3. **Closed Circuit Television "Traffic Cameras" (SDOT)**

As with the other two camera technologies, the crux of concern around these traffic cameras relates to limiting their use to specific purposes, enshrining in statute protections against invasion of privacy and general data collection, and limiting data sharing. It would be helpful to see the SDOT camera control guidelines referenced in the SIR, as well as to make clear in a policy applicable specifically to these cameras, what data will be deleted when (Section 5 appears to contain several different retention policies). Additional questions that an updated SIR should answer are as follows:

- The current SIR does not reference specific camera vendors and models—these would be helpful to have.

- Are there currently explicit guidelines on when recording occurs, and what's maintained? (See SIR Section 3.3 referencing recording for "compelling traffic operational needs"—the term is undefined.)

- Law enforcement use appears to be explicitly contemplated by the SIR, but the specific allowable uses are not defined—these should be made clear.

As with the other camera technologies, the Council should ensure clear purposes are defined in statute for these traffic cameras, that no use is made of the images for other purposes, that data is immediately deleted when the purpose is achieved, and that data sharing with third parties should be prohibited unless for those specific uses.

Thank you for your consideration, and we look forward to working with you on the process of ordinance implementation. Please feel free to contact me with questions or concerns.

Sincerely,

Shankar Narayan

cc: Seattle City Council and Executive

CASA LATINA
With Dignity and Opportunity

317 17TH AVENUE SOUTH, SEATTLE, WA 98144
TEL. 206.956.0779 FAX. 206.956.0780

October 29, 2018

My name is Marcos Martinez and I am the Executive Director at Casa Latina, a nonprofit organization based in Seattle that serves low income Latinx immigrant community through employment, education and community organizing.

The community that we serve at Casa Latina is particularly vulnerable to abuses by government agencies. Since the elections of 2016, our communities have been on edge due to the increased enforcement activities of agencies like ICE and Customs and Border Protection (CBP).

In addition, while government officials have pledged that the private information of individuals would be protected within agencies such as the State Department of Licensing, we have seen that those promises are not always borne out in reality. Breaches of community trust are very difficult to repair.

It is for these reasons that technologies such as the Automated License Plate Reader System cause concerns for our communities. The ACLU, in its comments on these technologies, has pointed out some major concerns regarding the policies that govern the use of the ALPR, including the lack of meaningful restrictions on the purposes for which ALPR data may be collected or used.

Limitations on data sharing are of particular concern, since this could affect immigrant community members who are subject to detention by immigration authorities but who are not the subject of any active criminal investigation by SPD. It's not clear that strong policies are in place to prohibit the sharing of data with ICE or CBP which would serve to aid those agencies in their efforts to detain immigrant community members.

Thank you for your consideration and I look forward to working with you to develop policies that protect the privacy of our most vulnerable communities.

Sincerely,

Marcos Martinez

www.casa-latina.org

DENSHŌ
The Japanese American Legacy Project

November 5, 2018

Dear Seattle IT:

I am writing to offer Densho's comments on the recently released Group 1 Surveillance Impact Reports (SIRs) under the Seattle Surveillance Ordinance review process. Densho is a community-based 501(c)(3) organization. For more than twenty years, we have been documenting the World War II incarceration of Japanese Americans to promote equity and social justice both in Seattle and across the country. The experiences of Japanese Americans are a somber lesson about the fragility of civil society in the face of intolerance and fear.

We have reason to cast a critical eye on infrastructure and systems created to monitor our citizenry. Some two decades before the beginning of WWII, the Japanese American community was targeted for mass surveillance in a coordinated effort involving the Federal Bureau of Investigation (FBI), the Office of Naval Intelligence (ONI), and the War Department's Military Intelligence Division, assisted by local law enforcement agencies. In the immediate aftermath of Pearl Harbor, US Census data was improperly used to develop exclusion area maps and lists of Japanese American citizens for registration. In the current political environment, we remember this history and are concerned about how a new breed of technologies may affect the rights of our friends and neighbors who belong to ethnic, religious and other vulnerable minority communities

These comments will cover the SIRs for the six Group 1 technologies in two primary sections. The first will address the Automated License Plate Reader (ALPR) sub-group, including SPD Patrol, Parking Enforcement, and SDOT. The second offers comments on the camera technology SIRs for SFD Emergency Scene Cameras, SFD Hazmat Cameras, SDOT Closed Circuit "Traffic Cameras"

Section 1: Automated License Plate Reader technologies

A. *General Concerns*

ALPR is a powerful technology that creates almost unprecedented abilities to surveil and track the movement of individuals across our city and region. It is already being utilized in ways that impact religious, ethnic and other minority communities. In the wake of the September 11 attacks, ALPR was used to monitor Muslim communities in New York, and more recently, US Immigration and Customs Enforcement has employed ALPR data through large aggregators such as Vigilant Solutions to target Latinx populations.

While ALPR is valuable to SPD (and SDOT) in their work, and – as discussed in the SIRs – there are generally benign and beneficial uses, the creation of a large pool of highly sensitive data presents a risk for misuse.

B. *SPD Patrol*

1416 South Jackson St. Seattle, WA 98144 Phone: 206 320.0095 Fax: 206 320.0098 www.densho.org

DENSHŌ
The Japanese American Legacy Project

1. Retention policy inconsistent with stated goals
   In the SIR, the primary goal of the ALPR program is stated as, "Property Recovery" – locating stolen vehicles, while the report cites, use, "[o]n occasion," of the stored data to assist criminal investigations, in particular, the location of Amber and Silver Alert subjects. If this is the case, this casts significant doubt on the need for a lengthy data retention period. The agency does not provide the analysis that led to the decision for the 90-day period anywhere in the SIR or, in response to questions during the public engagement meeting on October 30, 2018. This policy should be driven by careful consideration of the needs of the program, rather than

2. Third-party data sharing
   As stated in the SIR, data is shared with third-parties, including law enforcement and researchers, under a number of policies and inter-agency agreements. However, the criteria for permissible sharing is vague; these policies should be articulated in a clear, consistent and explicit fashion.
3. Lack of transparency and reporting
   Statistical data regarding the collection and use of the ALPR data should be made publicly available. The implementation of SPD's new RMS should include functionality for tracking and recording when ALPR data has been used in investigations and enforcement.
4. Governing policies
   Currently, the management and use of ALPR systems is guided principally by SPD Policy 16.170. SPD officials themselves admit that Policy 16.170 is inadequate and incomplete. ALPR is a novel, powerful technology that requires

C. *Parking Enforcement (SPD)*
   1. Co-mingling of Parking Enforcement and Patrol data
      The SIR describes the flow of data from the Scofflaw "boot vans" to the centralized Neology BOSS system, shared with Patrol. It is not clear whether this data is aggregated directly with the Patrol dataset. If so, this should be more explicitly stated, and the same policies and rules should apply.

D. *SDOT*
   1. Sharing of data with WSDOT and other third parties
      The SIR does not outline whether the data-sharing agreement with WSDOT includes provisions governing the sharing and use of SDOT-collected data.

Section 2: Camera technologies

The use of image and video technologies has obvious benefits in the efficiency and delivery of emergency services in crisis situations, as was articulated in the each of the SIRs covering this group. Densho's primary concern is the possibility that the infrastructure and the data collected may be subject to uses beyond the scope of the stated purposes. While it is highly unlikely that

1416 South Jackson St. Seattle, WA 98144 Phone: 206 320.0095 Fax: 206 320.0098 www.densho.org

DENSHŌ
The Japanese American Legacy Project

SFD and SDOT would utilize the systems in ways that directly impact privacy, unless the collection, retention and sharing of data is carefully regulated, there is potential for real harm to civil liberties in the hands of third parties. Coupled with facial recognition technology, camera data can be used in ways that SFD and SDOT may not have anticipated.

We appreciate the opportunity to share these concerns with you, and hope that this process may help to make our city a welcoming, safe and truly civil society.

Sincerely,

Geoff Froh
Deputy Director

1416 South Jackson St. Seattle, WA 98144 Phone: 206 320.0095 Fax: 206 320.0098 www.densho.org

APPENDIX G: EMAILS & LETTERS FROM THE PUBLIC

Letter submitted by individual constituent:

Surveillance.
I don't want it.
Any of it.
Just stop.

APPENDIX G: EMAILS & LETTERS FROM THE PUBLIC

Letter submitted by individual constituent:

Kevin Orme
502 N 80th
Seattle, WA 98103
206-789-3891

November 4, 2018

Public Input Commentary – Seattle Surveillance Technology open Public Comment period – 10/22 through 11/5, 2018.

Opening Remarks:

1. Surveillance technology usage in the United States of America, regardless of use, purpose and policy, is completely and wholly within the basic tenets of the Bill of Rights, otherwise known as Amendments 1-10 to the US Constitution. There are no more fundamental laws in the United States than the Constitution and the amendments thereto.

As regards privacy, public surveillance/data capture technology and police oversight – these governing principles have to be considered in any and all policies and local procedures/laws created for our democratic society. Doing anything less is simply illegal and against our whole theory of government – it's that simple.

Specifically:

The First Amendment, including rights to freedom of speech, public assembly and the press.

The Fourth Amendment, including rights preventing unreasonable search, seizure and requiring warrants for same.

The Fifth Amendment, including rights against self-incrimination and deprivation of life, liberty and property without due process.

The Sixth Amendment, including the right to confront the accuser by the accused; defense counsel when accused of a crime and proper/complete informing of the accused concerning the nature and extent of criminal accusation if occurs.

And beyond the Bill of Rights, **the 14th Amendment, Section 1**, regarding rights of due process and federal laws also applying equally to the states (which means *cities* in those same states, of course)

2) The WA State Constitution:

In addition to the Bill of Rights and the US Constitution, the WA State Constitution is also instructive:

Article 1, Section 1 – all political power is inherent in the people, and governments …..are established to protect and maintain individual rights;

Article 1, Section 2 – the US Constitution is the supreme law of the land;

Article 1, Section 7 - Invasion of Private Affairs or Home Prohibited

Article 1, Section 32- "A frequent recurrence to fundamental principles is essential to the security of individual right and the perpetuity of free government."

3) Context for Seattle: The above means essentially:

You cannot simply 'surveil everything' in the hopes of finding a criminal (or even worse, someone you simply "don't agree with"). That is called 'guilty until proven innocent' and has been overturned time and time again in our system of laws by courts and legislators at every level. The Bill of Rights has protected the 4th Amendment concept of 'Innocent until Proven Guilty' and 24-7 surveillance of **any** sort flies in the face and openly defies this most basic law.

You cannot 'surveil' public assemblies, protests, or similar gatherings, most especially with facial recognition, phone network/bluetooth data capture or public video recordings and/or microphones without again, violating the above basic constitutional principles – otherwise known as "laws" (US and WA).

You cannot store data simply according to 'policy', or come up with what you believe adequate controls may or may not be, and then implement them without complete transparency and public input, including that of the City Attorney's office, elected officials and arguably most important, THE PUBLIC. I believe this effort you have begun to solicit feedback is a good start, but there's a long way to go and this is only the very beginning, rest assured.

Finally, you cannot pay lip service to these previous paragraphs by not actively doing them yourself, and then simply turn around and receive/use/retain the data anyway through other means – that is, you cannot obtain the data from the NSA's Fusion Center already located in downtown Seattle, or the FBI, or TSA, DHS, or increasingly rogue agencies like ICE – all of these still break the law, plain and simple.

Specific technologies being discussed in this public outreach:

1) SDOT LPR's.

Positive – the data is stated as being deleted immediately after a transit time calculation;
Positive – the data is stated as only being available to SDOT personnel after relay from WSDOT, with individual identifying license plates not part of that incoming data;
Positive – stated purpose – facilitate effective and efficient traffic management within the Seattle city limits.

SDOT LPR's - COMMENT for Submission/consideration:

a) It is unclear how long WSDOT is retaining this data for handoff to SDOT and Seattle generally – even if SDOT deletes it nearly immediately after a calculation/use, can they go back and re-retrieve

it later? The answer should be NO, and simply that WSDOT is doing the same thing at minimum – deleting the data almost immediately after said calculation too (I recognize this latter is beyond SDOT's control, however, certainly as the biggest city in the state, Seattle would have major influence on these policies and procedures were you to weigh in and state clear policy positions).

b) It is also unclear what the statement 'travel time calculation' precisely means for these purposes. Is it just me driving through downtown and getting spotted if I go by any of these cameras/devices? Assuming the answer is yes, when is the 'timeout' – 1 minute if not seen by another camera? 5 minutes? When and how quickly does the 'calculation' occur (so that I know purportedly the data is then "immediately deleted" as you say?

c) It is also unclear if anyone else working for the City of Seattle has access to this WSDOT data (and if so, for how long, in what capacity, at what level of detail, etc.) – say, the SPD, City Attorney's office, or? So maybe SDOT isn't "surveilling" anyone within the normal meaning of the term given the safeguards noted in the policy PDF, but certainly the SPD have far different reasons for using this data, and most (if not all) of them are far removed from simple data calculations, and include direct data review to carry out those tasks?

Traffic Cameras (SDOT)

Positive – similar purposes to those above – namely efficient and effective traffic mgmt in real time, using systems and human operators (either in a data center or on the scene, e.g. tow truck, etc.) to make it happen.

SDOT Traffic Cams - COMMENT for Submission/consideration:

a) What are the 'SDOT Camera Control Protocol Guidelines' and are they public? If not, can they be and where can we review them? Have they ever been amended due to public input, potential past problems or abuses? When were they written and by whom with what expertise?
b) What are the 'specific cases' where footage is archived and for how long?
c) Has this data ever been subpoena'd by City personnel, or outside entities (e.g. ICE, NSA or similar)?
d) The 'protections' paragraph says archived footage isn't shared with any other City dept – but what about data that is 'in transit' between realtime capture and potential archiving later (whether only for 10 days or not)? How/when and in what circumstances might footage be temporarily retained or shared outside normal policy, and potentially 'evade' the otherwise typical 10-day delete policy as a result?

SPD – ALPR's

Positive – as stated by SPD with any such whiz-bang tech – 'preventing crime' ***SPD ALPR's: COMMENT***

for Submission/consideration:

a) Why 90 days? Why not something much more reasonable, like 15? Certainlyif the tech is sophisticated enough to create a 'hot list' as described here, **15 days – two working weeks in other words – is surely more than enough time for the data's intended purpose.**

b) Can we see examples of these 'auditable records' supposedly created by SPD when logging into ALPR/contacting dispatch? If you are making them 'auditable' for the purposes of ensuring restricted and limited use of the technology generally, then surely you don't mind if we see how that works at minimum so WE can know this (and believe you) too?

c) When does something become an 'active investigation' – and how long is the data retained, where stored and accessible by who then? What if the investigation is called off or invalidated by a court or city officer/city attorney – is the data immediately deleted, and an 'auditable record' of that activity created to prove it?

d) You say nothing about sharing the data with other entities (e.g. ICE, DHS, etc.) - do you? Are you planning to? Have you done so in the past? If so on any of these, under what circumstances and did they provide any sort of a warrant of any kind?

e) You stated there are eight SPD cars equipped with ALPR systems now, and that statement implies that this is the 'only' such ALPR system deployed 1) for these purposes, 2) with this specific technology citywide. Is this true? Are there stationary systems mounted elsewhere in the city that are networked (now or can be in the future) and if so, how many are there? Are there plans (either already in motion or for say, the next few years) to implement either more cars, add in stationary systems, or both? Certainly at minimum, just like with red light cameras, we deserve and demand publicly posted notice of any such stationary systems if they exist or are being deployed.

f) I have read the online 16.170-POL governing ALPR use http://www.seattle.gov/police-manual/title-16---patrol-operations/16170--automatic-license-plate-readers – and it's pretty sparse with only 4 short bullet points.
– more questions:

f1) what is ACCESS certification and how can we know more that it does what it's intended to do? Where is the training, who does it, is it a private entity creating coursework, etc.?

f2) how often are these standards updated (e.g. the policy is already 6 years old, dating from 2012 – certainly the technology is not falling behind in the same way);

f3) Who is in charge of TESU and what are their qualifications? Are they elected officials or behind the scenes?

f4) does the terminology 'part of an active investigation' = 'we got a hit on a license plate of X' – and X is a known criminal, there's a warrant out, or? Need way more information here, this is far too vague and un-specific when regards data management and control. I could be the most qualified TESU guy in the department and yet it doesn't mean I should be entitled to look at *any* data – especially without a legal warrant to do so? Where are the other controlling provisions?

Emergency Scene Cameras

Positive – improve and continue to enhance emergency preparedness and response effectiveness.

Emergency Cams: COMMENT for Submission/consideration:

a) where are the 'internal policies' and 'WA laws' governing storage of said photos and materials? The PDF is pretty vague.
b) Is live footage/drone image, sound and data capture being considered or already being used? As to data captured (audio, video, photo), storage management, retention and access policies – the Details, Please.
c) what about the same (live footage/audio/video) from vehicles or bodycams/etc.? Again, Details please.

Hazmat Cameras

Positive – largely identical to that of Emergency Incident Response, save the potential for nefarious/negligent actors to be involved

Hazmat Cams: COMMENT for Submission/consideration:

a) similar to with Emergency Cameras – essentially how long is the data stored, especially if no criminal activity is determined or the investigation concludes

b) anything beyond tablets used or planned to be used? This mentions tablets as the primary tech, but that doesn't foreclose plans for more (or by aggressive tech vendors already talking to you)?

c) what sort of data management training is provided to either HazMat or Emergency Responders, for that matter?

Parking Enforcement (SPD)

Positive – enforce parking and related laws, determine 'booting' situations ***SPD Parking Enforcement: COMMENT for Submission/consideration:***

a) there is nothing seen here about general data storage or retention parameters – Details, Please.
b) there is nothing here about whether this ALPR data is 'pooled' with ALPR datacollected from the eight so-equipped SPD cars mentioned earlier – and if so, whether governed by those parameters and restrictions too/not? Details, Please.

c) are these technologies governed by TESU as the others are? Barring possibly those controlled directly by the Seattle Municipal Court itself, separate from the SPD? Details, Please.

d) there is also no mention of the (likely older) Red Light Traffic Cam technology that has been in use in city locations for some years now, possibly over a decade. These aren't for SDOT use, these are for people running red lights, of course. All the relevant details (Data capture, retention, storage, access, certification, etc.) - all these apply here too – Details, Please.

Submitted 11/4/2018 by

Kevin Orme
502 N 80th
Seattle, WA 98103
206-789-3891

APPENDIX H: PUBLIC COMMENT ANALYSIS METHODOLOGY

OVERVIEW

The approach to comment analysis includes combination of qualitative and quantitative methods. A basic qualitative text analysis of the comments received, and a subsequent comparative analysis of results, were validated against quantitative results. Each comment was analyzed in the following ways, to observe trends and confirm conclusions:

1. Analyzed collectively, as a whole, with all other comments received
2. Analyzed by technology
3. Analyzed by technology and question

A summary of findings are included in Appendix B: Public Comment Demographics and Analysis. All comments received are included in Appendix E: All Individual Comments Received.

BACKGROUND ON METHODOLOGICAL FRAMEWORK

A modified Framework Methodology was used for qualitative analysis of the comments received, which "*…approaches [that] identify commonalities and differences in qualitative data, before focusing on relationships between different parts of the data, thereby seeking to draw descriptive and/or explanatory conclusions clustered around themes" (Gale, N.K., et.al, 2013).* Framework Methodology is a coding process which includes both inductive and deductive approaches to qualitative analysis.

The goal is to classify the subject data so that it can be meaningfully compared with other elements of the data and help inform decision-making. Framework Methodology is "not designed to be representative of a wider population, but purposive to capture diversity around a phenomenon" (*Gale, N.K., et.al, 2013).*

METHODOLOGY

STEP ONE: PREPARE DATA

1. Compile data received.
    a. Daily collection and maintenance of 2 primary datasets.
        i. Master dataset: a record of all raw comments received, questions generated at public meetings, and demographic information collected from all methods of submission.
        ii. Comment analysis dataset: the dataset used for comment analysis that contains coded data and the qualitative codebook. The codebook contains the qualitative codes used for analysis and their definitions.
2. Clean the compiled data.
    a. Ensure data is as consistent and complete as possible. Remove special characters for machine readability and analysis.
    b. Comments submitted through SurveyMonkey for "General Surveillance" remained in the "General Surveillance" category for the analysis, regardless of content of the

comment. Comments on surveillance generally, generated at public meetings, were categorized as such.

c. Filter data by technology for inclusion in individual SIRs.

STEP TWO: CONDUCT QUALITATIVE ANALYSIS USING FRAMEWORK METHODOLOGY

1. Become familiar with the structure and content of the data. This occurred daily compilation and cleaning of the data in step one.
2. Individually and collaboratively code the comments received, and identify emergent themes.
    I. Begin with deductive coding by developing pre-defined codes derived from the prescribed survey and small group facilitator questions and responses.
    II. Use clean data, as outlined in Data Cleaning section above, to inductively code comments.
        A. Each coder individually reviews the comments and independently codes them.
        B. Coders compare and discuss codes, subcodes, and broad themes that emerge.
        C. Qualitative codes are added as a new field (or series of fields) into the Comments dataset to derive greater insight into themes, and provide increased opportunity for visualizing findings.
    III. Develop the analytical framework.
        A. Coders discuss codes, sub-codes, and broad themes that emerge, until codes are agreed upon by all parties.
        B. Codes are grouped into larger categories or themes.
        C. The codes are be documented and defined in the codebook.
    IV. Apply the framework to code the remainder of the comments received.
    V. Interpret the data by identifying differences and map relationships between codes and themes, using R and Tableau.

STEP THREE: CONDUCT QUANTITATIVE ANALYSIS

1. Identify frequency of qualitative codes for each technology overall, by questions, or by themes:
    I. Analyze results for single word codes.
    II. Analyze results for word pair codes (for context).
2. Identify the most commonly used words and word pairs (most common and least common) for all comments received.
    I. Compare results with qualitative code frequencies and use to validate codes.
    II. Create network graph to identify relationships and frequencies between words used in comments submitted. Use this graph to validate analysis and themes.
3. Extract CSVs of single word codes, word pair codes, and word pairs in text of the comments, as well as the corresponding frequencies for generating visualizations in Tableau.

STEP FOUR: SUMMARIZATION

1. Visualize themes and codes in Tableau. Use call out quotes to provide context and tone.
2. Included summary information and analysis in the appendices of each SIR.

APPENDIX I: POLICIES AND PROCEDURES GOVERNING ALPR

City of Seattle
Mayor Jenny A. Durkan

MAYORAL DIRECTIVE

Date: February 6, 2018

To: City of Seattle Department Directors

From: Mayor Jenny A. Durkan

Subject: City of Seattle Protocol on Federal Immigration Enforcement

---

Background on Seattle as a Welcoming City

We have pledged to be a Welcoming City that protects all residents. This is not only the morally right thing to do, it is essential to a fundamental City duty. The City has a duty to protect the public safety of all of its residents. Confidence and trust in law enforcement is critical to this duty. Such confidence and trust supports essential functions of law enforcement including reporting of crimes to officers, participation of witnesses in investigations, and enhancing respect for law enforcement in our communities. This support for the essential work of law enforcement makes everyone in a community safer.

Many people do not distinguish the various types and roles of law enforcement. Positive and negative interactions with any law enforcement can adhere to all law enforcement. Recent actions and pronouncements by federal authorities, particularly by Federal Immigration and Customs Enforcement (ICE), undermine the trust and confidence essential to law enforcement. Many residents, regardless of their immigration status, may be unwilling to report crimes or participate in investigations because of concerns about potential impacts on others in their families or communities. This erodes and undermines the community trust that is essential for the City to provide public safety.

To bolster and maintain the trust needed for public safety, all residents must know we will take the steps necessary to protect them. Recent reports regarding lapses by government, including by the Washington State Department of Licensing, show we must have robust protocols for all City departments.

As discussed below, we will be assessing all Departments to determine what information is collected and distributed, whether that information is necessary to collect, and the need for individual departmental protocols. Until such assessment is completed the following will be effective immediately:

To further Seattle as a Welcoming City for all residents, including immigrant and refugee residents and workers, City department directors are hereby directed to refer all requests from ICE authorities to the Mayor's Office Legal Counsel, including:

Office of the Mayor | 600 Fourth Avenue, P.O. Box 94749, Seattle, WA 98124 | 206-684-4000 | seattle.gov/mayor

- Access to non-public areas in City buildings and venues (i.e., areas not open to the public such as staff work areas that require card key access and other areas designated as "private" or "employee only");
- Actions seeking data or information (written or oral) about City employees, residents or workers.

In all cases, City employees are directed to ask ICE agents to wait to enter any non-public areas until the Mayor's Office Legal Counsel is contacted at (206) 471-0664. Counsel will review credentials, submission of written authority to conduct action, and determine whether to grant approval of access.

These protocols will work in conjunction with existing City ordinance and policy:

- **City employees are prohibited from asking about immigration status**. Often referred to as the City's "don't ask" law, Seattle Ordinance 121063, passed in 2003, instructs all City employees to refrain from inquiring about the immigration status of any person except police officers where officers have a reasonable suspicion that a person 1) has previously been deported from the United States; (2) is again present in the United States; and (3) is committing or has committed a felony criminal-law violation.

- **City employees will serve all residents and city services will be accessible to all residents, regardless of immigration status.** Seattle Resolution 31730, passed in 2017, reaffirms Ordinance 121063 and states that city agencies and law enforcement cannot withhold services based on ancestry, race, ethnicity, national origin, color, age, sex, sexual orientation, gender identity, marital status, physical or mental disability, religion, or immigration status. See, also, Seattle Resolution 30672, passed in 2004.

Assessment of City Systems

All City department directors will participate in an assessment of City policies and practices – including but not limited to employment, law enforcement, public safety, IT, and social service delivery. The purpose of the assessment is to assess City compliance with Seattle Municipal Code 4.18.15, and to gain a better understanding what information is collected by the City, whether collecting that information is necessary, and how the City's work interacts with federal immigration enforcement.

All department directors shall identify a department lead to assist in this assessment by February 13, 2018.

City Contractors

City departments will issue a letter to all contractors receiving General Fund dollars to clarify and inform about the protocols described above. A communication will be issued by City departments to their contractors by March 6, 2018.

County Policy

As a reminder, jails are in King County's jurisdiction and enforcing civil federal immigration violations are in the purview of the U.S. Department of Homeland Security, City department directors are reminded to comply with the City's policy to defer to King County on ICE detainer requests.

- **City employees will refer detainer requests from the U.S. Department of Homeland Security's Immigration and Customs Enforcement (ICE) to King County.** King County Ordinance 17886 passed in 2014 clarifies that the County will not honor ICE requests for notification or detention, unless accompanied by a judicial warrant.

Directive for Implementation

To achieve full Department participation in ensuring that responses to ICE requests are consistent with Seattle Ordinance 121063 and to assess departmental compliance with Seattle Ordinance 121063, I request all Departments identify a lead to the Mayor's Office by February 13, 2018.

Contact for Further Information

Thank you for your cooperation. If you have any questions, please contact Mayor's Office Legal Counsel, Ian Warner (206) 471.0664.

(3) Inserted in any envelope and/or publication the contents of which may be construed to be inappropriate for association with the Missing Children Penalty Mail Program.

(e) Each component shall provide the General Services Staff, Justice Management Division, with the name(s), telephone number(s) and mailing address(es) of each designated Missing Children Program Coordinator within 30 days of the effective date of this regulation.

(f) Each component shall submit a quarterly report to the General Services Staff, Justice Management Division, within 5 days after the close of each Fiscal Year quarter providing the specific information identified in §19.5 concerning implementation and participation in the program.

PART 20—CRIMINAL JUSTICE INFORMATION SYSTEMS

Subpart A—General Provisions

Sec.
20.1 Purpose.
20.2 Authority.
20.3 Definitions.

Subpart B—State and Local Criminal History Record Information Systems

20.20 Applicability.
20.21 Preparation and submission of a Criminal History Record Information Plan.
20.22 Certification of compliance.
20.23 Documentation: Approval by OJARS.
20.24 State laws on privacy and security.
20.25 Penalties.

Subpart C—Federal Systems and Exchange of Criminal History Record Information

20.30 Applicability.
20.31 Responsibilities.
20.32 Includable offenses.
20.33 Dissemination of criminal history record information.
20.34 Individual's right to access criminal history record information.
20.35 Criminal Justice Information Services Advisory Policy Board.
20.36 Participation in the Interstate Identification Index System.
20.37 Responsibility for accuracy, completeness, currency, and integrity.
20.38 Sanction for noncompliance.
APPENDIX TO PART 20—COMMENTARY ON SELECTED SECTIONS OF THE REGULATIONS ON CRIMINAL HISTORY RECORD INFORMATION SYSTEMS

AUTHORITY: 28 U.S.C. 534; Pub. L. 92–544, 86 Stat. 1115; 42 U.S.C. 3711, *et seq.*, Pub. L. 99–169, 99 Stat. 1002, 1008–1011, as amended by Pub. L. 99–569, 100 Stat. 3190, 3196; Pub. L. 101–515, as amended by Pub. L. 104–99, set out in the notes to 28 U.S.C. 534.

SOURCE: Order No. 601–75, 40 FR 22114, May 20, 1975, unless otherwise noted.

Subpart A—General Provisions

SOURCE: 41 FR 11714, Mar. 19, 1976, unless otherwise noted.

§ 20.1 Purpose.

It is the purpose of these regulations to assure that criminal history record information wherever it appears is collected, stored, and disseminated in a manner to ensure the accuracy, completeness, currency, integrity, and security of such information and to protect individual privacy.

[Order No. 2258–99, 64 FR 52226, Sept. 28, 1999]

§ 20.2 Authority.

These regulations are issued pursuant to sections 501 and 524(b) of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Crime Control Act of 1973, Public Law 93–83, 87 Stat. 197, 42 U.S.C. 3701, *et seq.* (Act), 28 U.S.C. 534, and Public Law 92–544, 86 Stat. 1115.

§ 20.3 Definitions.

As used in these regulations:

(a) *Act* means the Omnibus Crime Control and Safe Streets Act, 42 U.S.C. 3701, *et seq.*, as amended.

(b) *Administration of criminal justice* means performance of any of the following activities: Detection, apprehension, detention, pretrial release, posttrial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal history record information.

(c) *Control Terminal Agency* means a duly authorized state, foreign, or international criminal justice agency with

direct access to the National Crime Information Center telecommunications network providing statewide (or equivalent) service to its criminal justice users with respect to the various systems managed by the FBI CJIS Division.

(d) *Criminal history record information* means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system.

(e) *Criminal history record information system* means a system including the equipment, facilities, procedures, agreements, and organizations thereof, for the collection, processing, preservation, or dissemination of criminal history record information.

(f) *Criminal history record repository* means the state agency designated by the governor or other appropriate executive official or the legislature to perform centralized recordkeeping functions for criminal history records and services in the state.

(g) *Criminal justice agency* means:

(1) Courts; and

(2) A governmental agency or any subunit thereof that performs the administration of criminal justice pursuant to a statute or executive order, and that allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspector General Offices are included.

(h) *Direct access* means having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of or intervention by any other party or agency.

(i) *Disposition* means information disclosing that criminal proceedings have been concluded and the nature of the termination, including information disclosing that the police have elected not to refer a matter to a prosecutor or that a prosecutor has elected not to commence criminal proceedings; or disclosing that proceedings have been indefinitely postponed and the reason for such postponement. Dispositions shall include, but shall not be limited to, acquittal, acquittal by reason of insanity, acquittal by reason of mental incompetence, case continued without finding, charge dismissed, charge dismissed due to insanity, charge dismissed due to mental incompetency, charge still pending due to insanity, charge still pending due to mental incompetence, guilty plea, nolle prosequi, no paper, nolo contendere plea, convicted, youthful offender determination, deceased, deferred disposition, dismissed-civil action, found insane, found mentally incompetent, pardoned, probation before conviction, sentence commuted, adjudication withheld, mistrial-defendant discharged, executive clemency, placed on probation, paroled, or released from correctional supervision.

(j) *Executive order* means an order of the President of the United States or the Chief Executive of a state that has the force of law and that is published in a manner permitting regular public access.

(k) *Federal Service Coordinator* means a non-Control Terminal Agency that has a direct telecommunications line to the National Crime Information Center network.

(l) *Fingerprint Identification Records System* or "FIRS" means the following FBI records: Criminal fingerprints and/or related criminal justice information submitted by authorized agencies having criminal justice responsibilities; civil fingerprints submitted by federal agencies and civil fingerprints submitted by persons desiring to have their fingerprints placed on record for personal identification purposes; identification records, sometimes referred to as "rap sheets," which are compilations of criminal history record information pertaining to individuals who have criminal fingerprints maintained in the FIRS; and a name index pertaining to all individuals whose fingerprints are maintained in the FIRS. See the FIRS Privacy Act System Notice periodically published in the FEDERAL REGISTER for further details.

(m) *Interstate Identification Index System* or "III System" means the cooperative federal-state system for the exchange of criminal history records, and includes the National Identification Index, the National Fingerprint File, and, to the extent of their participation in such system, the criminal history record repositories of the states and the FBI.

(n) *National Crime Information Center* or "NCIC" means the computerized information system, which includes telecommunications lines and any message switching facilities that are authorized by law, regulation, or policy approved by the Attorney General of the United States to link local, state, tribal, federal, foreign, and international criminal justice agencies for the purpose of exchanging NCIC related information. The NCIC includes, but is not limited to, information in the III System. See the NCIC Privacy Act System Notice periodically published in the FEDERAL REGISTER for further details.

(o) *National Fingerprint File* or "NFF" means a database of fingerprints, or other uniquely personal identifying information, relating to an arrested or charged individual maintained by the FBI to provide positive identification of record subjects indexed in the III System.

(p) *National Identification Index* or "NII" means an index maintained by the FBI consisting of names, identifying numbers, and other descriptive information relating to record subjects about whom there are criminal history records in the III System.

(q) *Nonconviction data* means arrest information without disposition if an interval of one year has elapsed from the date of arrest and no active prosecution of the charge is pending; information disclosing that the police have elected not to refer a matter to a prosecutor, that a prosecutor has elected not to commence criminal proceedings, or that proceedings have been indefinitely postponed; and information that there has been an acquittal or a dismissal.

(r) *State* means any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

(s) *Statute* means an Act of Congress or of a state legislature or a provision of the Constitution of the United States or of a state.

[Order No. 2258–99, 64 FR 52226, Sept. 28, 1999]

Subpart B—State and Local Criminal History Record Information Systems

SOURCE: 41 FR 11715, Mar. 19, 1976, unless otherwise noted.

§ 20.20 Applicability.

(a) The regulations in this subpart apply to all State and local agencies and individuals collecting, storing, or disseminating criminal history record information processed by manual or automated operations where such collection, storage, or dissemination has been funded in whole or in part with funds made available by the Law Enforcement Assistance Administration subsequent to July 1, 1973, pursuant to title I of the Act. Use of information obtained from the FBI Identification Division or the FBI/NCIC system shall also be subject to limitations contained in subpart C.

(b) The regulations in this subpart shall not apply to criminal history record information contained in:

(1) Posters, announcements, or lists for identifying or apprehending fugitives or wanted persons;

(2) Original records of entry such as police blotters maintained by criminal justice agencies, compiled chronologically and required by law or long standing custom to be made public, if such records are organized on a chronological basis;

(3) Court records of public judicial proceedings;

(4) Published court or administrative opinions or public judicial, administrative or legislative proceedings;

(5) Records of traffic offenses maintained by State departments of transportation, motor vehicles or the equivalent thereof for the purpose of regulating the issuance, suspension, revocation, or renewal of driver's, pilot's or other operators' licenses;

(6) Announcements of executive clemency.

(c) Nothing in these regulations prevents a criminal justice agency from disclosing to the public criminal history record information related to the offense for which an individual is currently within the criminal justice system. Nor is a criminal justice agency prohibited from confirming prior criminal history record information to members of the news media or any other person, upon specific inquiry as to whether a named individual was arrested, detained, indicted, or whether an information or other formal charge was filed, on a specified date, if the arrest record information or criminal record information disclosed is based on data excluded by paragraph (b) of this section. The regulations do not prohibit the dissemination of criminal history record information for purposes of international travel, such as issuing visas and granting of citizenship.

§ 20.21 Preparation and submission of a Criminal History Record Information Plan.

A plan shall be submitted to OJARS by each State on March 16, 1976, to set forth all operational procedures, except those portions relating to dissemination and security. A supplemental plan covering these portions shall be submitted no later than 90 days after promulgation of these amended regulations. The plan shall set forth operational procedures to—

(a) *Completeness and accuracy.* Insure that criminal history record information is complete and accurate.

(1) Complete records should be maintained at a central State repository. To be complete, a record maintained at a central State repository which contains information that an individual has been arrested, and which is available for dissemination, must contain information of any dispositions occurring within the State within 90 days after the disposition has occurred. The above shall apply to all arrests occurring subsequent to the effective date of these regulations. Procedures shall be established for criminal justice agencies to query the central repository prior to dissemination of any criminal history record information unless it can be assured that the most up-to-date disposition data is being used. Inquiries of a central State repository shall be made prior to any dissemination except in those cases where time is of the essence and the repository is technically incapable of responding within the necessary time period.

(2) To be accurate means that no record containing criminal history record information shall contain erroneous information. To accomplish this end, criminal justice agencies shall institute a process of data collection, entry, storage, and systematic audit that will minimize the possibility of recording and storing inaccurate information and upon finding inaccurate information of a material nature, shall notify all criminal justice agencies known to have received such information.

(b) *Limitations on dissemination.* Insure that dissemination of nonconviction data has been limited, whether directly or through any intermediary only to:

(1) Criminal justice agencies, for purposes of the administration of criminal justice and criminal justice agency employment;

(2) Individuals and agencies for any purpose authorized by statute, ordinance, executive order, or court rule, decision, or order, as construed by appropriate State or local officials or agencies;

(3) Individuals and agencies pursuant to a specific agreement with a criminal justice agency to provide services required for the administration of criminal justice pursuant to that agreement. The agreement shall specifically authorize access to data, limit the use of data to purposes for which given, insure the security and confidentiality of the data consistent with these regulations, and provide sanctions for violation thereof;

(4) Individuals and agencies for the express purpose of research, evaluative, or statistical activities pursuant to an agreement with a criminal justice agency. The agreement shall specifically authorize access to data, limit the use of data to research, evaluative, or statistical purposes, insure the confidentiality and security of the data consistent with these regulations and with section 524(a) of the Act and any regulations implementing section

524(a), and provide sanctions for the violation thereof. These dissemination limitations do not apply to conviction data.

(c) *General policies on use and dissemination.* (1) Use of criminal history record information disseminated to noncriminal justice agencies shall be limited to the purpose for which it was given.

(2) No agency or individual shall confirm the existence or nonexistence of criminal history record information to any person or agency that would not be eligible to receive the information itself.

(3) Subsection (b) does not mandate dissemination of criminal history record information to any agency or individual. States and local governments will determine the purposes for which dissemination of criminal history record information is authorized by State law, executive order, local ordinance, court rule, decision or order.

(d) *Juvenile records.* Insure that dissemination of records concerning proceedings relating to the adjudication of a juvenile as delinquent or in need or supervision (or the equivalent) to noncriminal justice agencies is prohibited, unless a statute, court order, rule or court decision specifically authorizes dissemination of juvenile records, except to the same extent as criminal history records may be disseminated as provided in paragraph (b) (3) and (4) of this section.

(e) *Audit.* Insure that annual audits of a representative sample of State and local criminal justice agencies chosen on a random basis shall be conducted by the State to verify adherence to these regulations and that appropriate records shall be retained to facilitate such audits. Such records shall include, but are not limited to, the names of all persons or agencies to whom information is disseminated and the date upon which such information is disseminated. The reporting of a criminal justice transaction to a State, local or Federal repository is not a dissemination of information.

(f) *Security.* Wherever criminal history record information is collected, stored, or disseminated, each State shall insure that the following requirements are satisfied by security standards established by State legislation, or in the absence of such legislation, by regulations approved or issued by the Governor of the State.

(1) Where computerized data processing is employed, effective and technologically advanced software and hardware designs are instituted to prevent unauthorized access to such information.

(2) Access to criminal history record information system facilities, systems operating environments, data file contents whether while in use or when stored in a media library, and system documentation is restricted to authorized organizations and personnel.

(3)(i) Computer operations, whether dedicated or shared, which support criminal justice information systems, operate in accordance with procedures developed or approved by the participating criminal justice agencies that assure that:

(*a*) Criminal history record information is stored by the computer in such manner that it cannot be modified, destroyed, accessed, changed, purged, or overlaid in any fashion by non-criminal justice terminals.

(*b*) Operation programs are used that will prohibit inquiry, record updates, or destruction of records, from any terminal other than criminal justice system terminals which are so designated.

(*c*) The destruction of records is limited to designated terminals under the direct control of the criminal justice agency responsible for creating or storing the criminal history record information.

(*d*) Operational programs are used to detect and store for the output of designated criminal justice agency employees all unauthorized attempts to penetrate any criminal history record information system, program or file.

(*e*) The programs specified in paragraphs (f)(3)(i) (*b*) and (*d*) of this section are known only to criminal justice agency employees responsible for criminal history record information system control or individuals and agencies pursuant to a specific agreement with the criminal justice agency to provide such programs and the program(s) are kept continuously under maximum security conditions.

(*f*) Procedures are instituted to assure that an individual or agency authorized direct access is responsible for (*1*) the physical security of criminal history record information under its control or in its custody and (*2*) the protection of such information from unauthorized access, disclosure or dissemination.

(*g*) Procedures are instituted to protect any central repository of criminal history record information from unauthorized access, theft, sabotage, fire, flood, wind, or other natural or manmade disasters.

(ii) A criminal justice agency shall have the right to audit, monitor and inspect procedures established above.

(4) The criminal justice agency will:

(i) Screen and have the right to reject for employment, based on good cause, all personnel to be authorized to have direct access to criminal history record information.

(ii) Have the right to initiate or cause to be initiated administrative action leading to the transfer or removal of personnel authorized to have direct access to such information where such personnel violate the provisions of these regulations or other security requirements established for the collection, storage, or dissemination of criminal history record information.

(iii) Institute procedures, where computer processing is not utilized, to assure that an individual or agency authorized direct access is responsible for

(*a*) The physical security of criminal history record information under its control or in its custody and

(*b*) The protection of such information from unauthorized access, disclosure, or dissemination.

(iv) Institute procedures, where computer processing is not utilized, to protect any central repository of criminal history record information from unauthorized access, theft, sabotage, fire, flood, wind, or other natural or manmade disasters.

(v) Provide that direct access to criminal history record information shall be available only to authorized officers or employees of a criminal justice agency and, as necessary, other authorized personnel essential to the proper operation of the criminal history record information system.

(5) Each employee working with or having access to criminal history record information shall be made familiar with the substance and intent of these regulations.

(g) *Access and review*. Insure the individual's right to access and review of criminal history information for purposes of accuracy and completeness by instituting procedures so that—

(1) Any individual shall, upon satisfactory verification of his identity, be entitled to review without undue burden to either the criminal justice agency or the individual, any criminal history record information maintained about the individual and obtain a copy thereof when necessary for the purpose of challenge or correction;

(2) Administrative review and necessary correction of any claim by the individual to whom the information relates that the information is inaccurate or incomplete is provided;

(3) The State shall establish and implement procedures for administrative appeal where a criminal justice agency refuses to correct challenged information to the satisfaction of the individual to whom the information relates;

(4) Upon request, an individual whose record has been corrected shall be given the names of all non-criminal justice agencies to whom the data has been given;

(5) The correcting agency shall notify all criminal justice recipients of corrected information; and

(6) The individual's right to access and review of criminal history record information shall not extend to data contained in intelligence, investigatory, or other related files and shall not be construed to include any other information than that defined by §20.3(b).

[41 FR 11715, Mar. 19, 1976, as amended at 42 FR 61595, Dec. 6, 1977]

§20.22 Certification of compliance.

(a) Each State to which these regulations are applicable shall with the submission of its plan provide a certification that to the maximum extent feasible action has been taken to comply with the procedures set forth in the plan. Maximum extent feasible, in this subsection, means actions which can be

taken to comply with the procedures set forth in the plan that do not require additional legislative authority or involve unreasonable cost or do not exceed existing technical ability.

(b) The certification shall include—

(1) An outline of the action which has been instituted. At a minimum, the requirements of access and review under § 20.21(g) must be completely operational;

(2) A description of any legislation or executive order, or attempts to obtain such authority that has been instituted to comply with these regulations;

(3) A description of the steps taken to overcome any fiscal, technical, and administrative barriers to the development of complete and accurate criminal history record information;

(4) A description of existing system capability and steps being taken to upgrade such capability to meet the requirements of these regulations; and

(5) A listing setting forth categories of non-criminal justice dissemination. See § 20.21(b).

§ 20.23 Documentation: Approval by OJARS.

Within 90 days of the receipt of the plan, OJARS shall approve or disapprove the adequacy of the provisions of the plan and certification. Evaluation of the plan by OJARS will be based upon whether the procedures set forth will accomplish the required objectives. The evaluation of the certification(s) will be based upon whether a good faith effort has been shown to initiate and/or further compliance with the plan and regulations. All procedures in the approved plan must be fully operational and implemented by March 1, 1978. A final certification shall be submitted on March 1, 1978.

Where a State finds it is unable to provide final certification that all required procedures as set forth in § 20.21 will be operational by March 1, 1978, a further extension of the deadline will be granted by OJARS upon a showing that the State has made a good faith effort to implement these regulations to the maximum extent feasible. Documentation justifying the request for the extension including a proposed timetable for full compliance must be submitted to OJARS by March 1, 1978. Where a State submits a request for an extension, the implementation date will be extended an additional 90 days while OJARS reviews the documentation for approval or disapproval. To be approved, such revised schedule must be consistent with the timetable and procedures set out below:

(a) July 31, 1978—Submission of certificate of compliance with:

(1) Individual access, challenge, and review requirements;

(2) Administrative security;

(3) Physical security to the maximum extent feasible.

(b) Thirty days after the end of a State's next legislative session—Submission to OJARS of a description of State policy on dissemination of criminal history record information.

(c) Six months after the end of a State's legislative session—Submission to OJARS of a brief and concise description of standards and operating procedures to be followed by all criminal justice agencies covered by OJARS regulations in complying with the State policy on dissemination.

(d) Eighteen months after the end of a State's legislative session—Submission to OJARS of a certificate attesting to the conduct of an audit of the State central repository and of a random number of other criminal justice agencies in compliance with OJARS regulations.

[41 FR 11715, Mar. 19, 1976, as amended at 42 FR 61596, Dec. 6, 1977]

§ 20.24 State laws on privacy and security.

Where a State originating criminal history record information provides for sealing or purging thereof, nothing in these regulations shall be construed to prevent any other State receiving such information, upon notification, from complying with the originating State's sealing or purging requirements.

§ 20.25 Penalties.

Any agency or individual violating subpart B of these regulations shall be subject to a civil penalty not to exceed $10,000 for a violation occurring before September 29, 1999, and not to exceed $11,000 for a violation occurring on after September 29, 1999. In addition,

OJARS may initiate fund cut-off procedures against recipients of OJARS assistance.

[41 FR 11715, Mar. 19, 1976, as amended by Order No. 2249-99, 64 FR 47102, Aug. 30, 1999]

Subpart C—Federal Systems and Exchange of Criminal History Record Information

SOURCE: Order No. 2258-99, 64 FR 52227, Sept. 28, 1999, unless otherwise noted.

§20.30 Applicability.

The provisions of this subpart of the regulations apply to the III System and the FIRS, and to duly authorized local, state, tribal, federal, foreign, and international criminal justice agencies to the extent that they utilize the services of the III System or the FIRS. This subpart is applicable to both manual and automated criminal history records.

§20.31 Responsibilities.

(a) The Federal Bureau of Investigation (FBI) shall manage the NCIC.

(b) The FBI shall manage the FIRS to support identification and criminal history record information functions for local, state, tribal, and federal criminal justice agencies, and for noncriminal justice agencies and other entities where authorized by federal statute, state statute pursuant to Public Law 92-544, 86 Stat. 1115, Presidential executive order, or regulation or order of the Attorney General of the United States.

(c) The FBI CJIS Division may manage or utilize additional telecommunication facilities for the exchange of fingerprints, criminal history record related information, and other criminal justice information.

(d) The FBI CJIS Division shall maintain the master fingerprint files on all offenders included in the III System and the FIRS for the purposes of determining first offender status; to identify those offenders who are unknown in states where they become criminally active but are known in other states through prior criminal history records; and to provide identification assistance in disasters and for other humanitarian purposes.

(e) The FBI may routinely establish and collect fees for noncriminal justice fingerprint-based and other identification services as authorized by Federal law. These fees apply to Federal, State and any other authorized entities requesting fingerprint identification records and name checks for noncriminal justice purposes.

(1) The Director of the FBI shall review the amount of the fee periodically, but not less than every four years, to determine the current cost of processing fingerprint identification records and name checks for noncriminal justice purposes.

(2) Fee amounts and any revisions thereto shall be determined by current costs, using a method of analysis consistent with widely accepted accounting principles and practices, and calculated in accordance with the provisions of 31 U.S.C. 9701 and other Federal law as applicable.

(3) Fee amounts and any revisions thereto shall be published as a notice in the FEDERAL REGISTER.

(f) The FBI will collect a fee for providing noncriminal name-based background checks of the FBI Central Records System through the National Name Check Program pursuant to the authority in Pub. L. 101-515 and in accordance with paragraphs (e)(1), (2) and (3) of this section.

[41 FR 11715, Mar. 19, 1976, as amended at 75 FR 18755, Apr. 13, 2010; 75 FR 24798, May 6, 2010]

§20.32 Includable offenses.

(a) Criminal history record information maintained in the III System and the FIRS shall include serious and/or significant adult and juvenile offenses.

(b) The FIRS excludes arrests and court actions concerning nonserious offenses, e.g., drunkenness, vagrancy, disturbing the peace, curfew violation, loitering, false fire alarm, non-specific charges of suspicion or investigation, and traffic violations (except data will be included on arrests for vehicular manslaughter, driving under the influence of drugs or liquor, and hit and run), when unaccompanied by a §20.32(a) offense. These exclusions may not be applicable to criminal history records maintained in state criminal

history record repositories, including those states participating in the NFF.

(c) The exclusions enumerated above shall not apply to federal manual criminal history record information collected, maintained, and compiled by the FBI prior to the effective date of this subpart.

§ 20.33 Dissemination of criminal history record information.

(a) Criminal history record information contained in the III System and the FIRS may be made available:

(1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies;

(2) To federal agencies authorized to receive it pursuant to federal statute or Executive order;

(3) For use in connection with licensing or employment, pursuant to Public Law 92–544, 86 Stat. 1115, or other federal legislation, and for other uses for which dissemination is authorized by federal law. Refer to § 50.12 of this chapter for dissemination guidelines relating to requests processed under this paragraph;

(4) For issuance of press releases and publicity designed to effect the apprehension of wanted persons in connection with serious or significant offenses;

(5) To criminal justice agencies for the conduct of background checks under the National Instant Criminal Background Check System (NICS);

(6) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/ information services for criminal justice agencies; and

(7) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

(b) The exchange of criminal history record information authorized by paragraph (a) of this section is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or service providers identified in paragraphs (a)(6) and (a)(7) of this section.

(c) Nothing in these regulations prevents a criminal justice agency from disclosing to the public factual information concerning the status of an investigation, the apprehension, arrest, release, or prosecution of an individual, the adjudication of charges, or the correctional status of an individual, which is reasonably contemporaneous with the event to which the information relates.

(d) Criminal history records received from the III System or the FIRS shall be used only for the purpose requested and a current record should be requested when needed for a subsequent authorized use.

§ 20.34 Individual's right to access criminal history record information.

The procedures by which an individual may obtain a copy of his or her identification record from the FBI to review and request any change, correction, or update are set forth in §§ 16.30–16.34 of this chapter. The procedures by which an individual may obtain a copy of his or her identification record from a state or local criminal justice agency are set forth in § 20.34 of the appendix to this part.

§ 20.35 Criminal Justice Information Services Advisory Policy Board.

(a) There is established a CJIS Advisory Policy Board, the purpose of which is to recommend to the FBI Director general policy with respect to the philosophy, concept, and operational principles of various criminal justice information systems managed by the FBI's CJIS Division.

(b) The Board includes representatives from state and local criminal justice agencies; members of the judicial, prosecutorial, and correctional segments of the criminal justice community; a representative of federal agencies participating in the CJIS systems; and representatives of criminal justice professional associations.

(c) All members of the Board will be appointed by the FBI Director.

(d) The Board functions solely as an advisory body in compliance with the provisions of the Federal Advisory Committee Act. Title 5, United States Code, Appendix 2.

§ 20.36 Participation in the Interstate Identification Index System.

(a) In order to acquire and retain direct access to the III System, each Control Terminal Agency and Federal Service Coordinator shall execute a CJIS User Agreement (or its functional equivalent) with the Assistant Director in Charge of the CJIS Division, FBI, to abide by all present rules, policies, and procedures of the NCIC, as well as any rules, policies, and procedures hereinafter recommended by the CJIS Advisory Policy Board and adopted by the FBI Director.

(b) Entry or updating of criminal history record information in the III System will be accepted only from state or federal agencies authorized by the FBI. Terminal devices in other agencies will be limited to inquiries.

§ 20.37 Responsibility for accuracy, completeness, currency, and integrity.

It shall be the responsibility of each criminal justice agency contributing data to the III System and the FIRS to assure that information on individuals is kept complete, accurate, and current so that all such records shall contain to the maximum extent feasible dispositions for all arrest data included therein. Dispositions should be submitted by criminal justice agencies within 120 days after the disposition has occurred.

§ 20.38 Sanction for noncompliance.

Access to systems managed or maintained by the FBI is subject to cancellation in regard to any agency or entity that fails to comply with the provisions of subpart C of this part.

Appendix to Part 20—Commentary on Selected Sections of the Regulations on Criminal History Record Information Systems

Subpart A–§ 20.3(d). The definition of criminal history record information is intended to include the basic offender-based transaction statistics/III System (OBTS/III) data elements. If notations of an arrest, disposition, or other formal criminal justice transaction occurs in records other than the traditional "rap sheet," such as arrest reports, any criminal history record information contained in such reports comes under the definition of this subsection.

The definition, however, does not extend to other information contained in criminal justice agency reports. Intelligence or investigative information (e.g., suspected criminal activity, associates, hangouts, financial information, and ownership of property and vehicles) is not included in the definition of criminal history information.

§ 20.3(g). The definitions of criminal justice agency and administration of criminal justice in § 20.3(b) of this part must be considered together. Included as criminal justice agencies would be traditional police, courts, and corrections agencies, as well as subunits of noncriminal justice agencies that perform the administration of criminal justice pursuant to a federal or state statute or executive order and allocate a substantial portion of their budgets to the administration of criminal justice. The above subunits of noncriminal justice agencies would include, for example, the Office of Investigation of the Food and Drug Administration, which has as its principal function the detection and apprehension of persons violating criminal provisions of the Federal Food, Drug and Cosmetic Act. Also included under the definition of criminal justice agency are umbrella-type administrative agencies supplying criminal history information services, such as New York's Division of Criminal Justice Services.

§ 20.3(i). Disposition is a key concept in section 524(b) of the Act and in §§ 20.21(a)(1) and 20.21(b) of this part. It therefore is defined in some detail. The specific dispositions listed in this subsection are examples only and are not to be construed as excluding other, unspecified transactions concluding criminal proceedings within a particular agency.

§ 20.3(q). The different kinds of acquittals and dismissals delineated in § 20.3(i) are all considered examples of nonconviction data.

Subpart B—§ 20.20(a). These regulations apply to criminal justice agencies receiving funds under the Omnibus Crime Control and Safe Streets Act for manual or automated

systems subsequent to July 1, 1973. In the hearings on the regulations, a number of those testifying challenged LEAA's authority to promulgate regulations for manual systems by contending that section 524(b) of the Act governs criminal history information contained in automated systems.

The intent of section 524(b), however, would be subverted by only regulating automated systems. Any agency that wished to circumvent the regulations would be able to create duplicate manual files for purposes contrary to the letter and spirit of the regulations.

Regulation of manual systems, therefore, is authorized by section 524(b) when coupled with section 501 of the Act which authorizes the Administration to establish rules and regulations "necessary to the exercise of its functions * * *."

The Act clearly applies to all criminal history record information collected, stored, or disseminated with LEAA support subsequent to July 1, 1973.

Limitations as contained in subpart C also apply to information obtained from the FBI Identification Division or the FBI/NCIC System.

§ 20.20 (b) and (c). Section 20.20 (b) and (c) exempts from regulations certain types of records vital to the apprehension of fugitives, freedom of the press, and the public's right to know. Court records of public judicial proceedings are also exempt from the provisions of the regulations.

Section 20.20(b)(2) attempts to deal with the problem of computerized police blotters. In some local jurisdictions, it is apparently possible for private individuals and/or newsmen upon submission of a specific name to obtain through a computer search of the blotter a history of a person's arrests. Such files create a partial criminal history data bank potentially damaging to individual privacy, especially since they do not contain final dispositions. By requiring that such records be accessed solely on a chronological basis, the regulations limit inquiries to specific time periods and discourage general fishing expeditions into a person's private life.

Subsection 20.20(c) recognizes that announcements of ongoing developments in the criminal justice process should not be precluded from public disclosure. Thus, announcements of arrest, convictions, new developments in the course of an investigation may be made. It is also permissible for a criminal justice agency to confirm certain matters of public record information upon specific inquiry. Thus, if a question is raised: "Was X arrested by your agency on January 3, 1975" and this can be confirmed or denied by looking at one of the records enumerated in subsection (b) above, then the criminal justice agency may respond to the inquiry. Conviction data as stated in § 20.21(b) may be disseminated without limitation.

§ 20.21. The regulations deliberately refrain from specifying who within a State should be responsible for preparing the plan. This specific determination should be made by the Governor. The State has 90 days from the publication of these revised regulations to submit the portion of the plan covering §§ 20.21(b) and 20.21(f).

§ 20.21(a)(1). Section 524(b) of the Act requires that LEAA insure criminal history information be current and that, to the maximum extent feasible, it contain disposition as well as current data.

It is, however, economically and administratively impractical to maintain complete criminal histories at the local level. Arrangements for local police departments to keep track of dispositions by agencies outside of the local jurisdictions generally do not exist. It would, moreover, be bad public policy to encourage such arrangements since it would result in an expensive duplication of files.

The alternatives to locally kept criminal histories are records maintained by a central State repository. A central State repository is a State agency having the function pursuant to a statute or executive order of maintaining comprehensive statewide criminal history record information files. Ultimately, through automatic data processing the State level will have the capability to handle all requests for in-State criminal history information.

Section 20.20(a)(1) is written with a centralized State criminal history repository in mind. The first sentence of the subsection states that complete records should be retained at a central State repository. The word "should" is permissive; it suggests but does not mandate a central State repository.

The regulations do require that States establish procedures for State and local criminal justice agencies to query central State repositories wherever they exist. Such procedures are intended to insure that the most current criminal justice information is used.

As a minimum, criminal justice agencies subject to these regulations must make inquiries of central State repositories whenever the repository is capable of meeting the user's request within a reasonable time. Presently, comprehensive records of an individual's transactions within a State are maintained in manual files at the State level, if at all. It is probably unrealistic to expect manual systems to be able immediately to meet many rapid-access needs of police and prosecutors. On the other hand, queries of the State central repository for most noncriminal justice purposes probably can and should be made prior to dissemination of criminal history record information.

§ 20.21(b). The limitations on dissemination in this subsection are essential to fulfill the

mandate of section 524(b) of the Act which requires the Administration to assure that the "privacy of all information is adequately provided for and that information shall only be used for law enforcement and criminal justice and other lawful purposes." The categories for dissemination established in this section reflect suggestions by hearing witnesses and respondents submitting written commentary.

The regulations distinguish between conviction and nonconviction information insofar as dissemination is concerned. Conviction information is currently made available without limitation in many jurisdictions. Under these regulations, conviction data and pending charges could continue to be disseminated routinely. No statute, ordinance, executive order, or court rule is necessary in order to authorize dissemination of conviction data. However, nothing in the regulations shall be construed to negate a State law limiting such dissemination.

After December 31, 1977, dissemination of nonconviction data would be allowed, if authorized by a statute, ordinance, executive order, or court rule, decision, or order. The December 31, 1977, deadline allows the States time to review and determine the kinds of dissemination for non-criminal justice purposes to be authorized. When a State enacts comprehensive legislation in this area, such legislation will govern dissemination by local jurisdictions within the State. It is possible for a public record law which has been construed by the State to authorize access to the public of all State records, including criminal history record information, to be considered as statutory authority under this subsection. Federal legislation and executive orders can also authorize dissemination and would be relevant authority.

For example, Civil Service suitability investigations are conducted under Executive Order 10450. This is the authority for most investigations conducted by the Commission. Section 3(a) of 10450 prescribes the minimum scope of investigation and requires a check of FBI fingerprint files and written inquiries to appropriate law enforcement agencies.

§ 20.21(b)(3). This subsection would permit private agencies such as the Vera Institute to receive criminal histories where they perform a necessary administration of justice function such as pretrial release. Private consulting firms which commonly assist criminal justice agencies in information systems development would also be included here.

§ 20.21(b)(4). Under this subsection, any good faith researchers including private individuals would be permitted to use criminal history record information for research purposes. As with the agencies designated in § 20.21(b)(3) researchers would be bound by an agreement with the disseminating criminal justice agency and would, of course, be subject to the sanctions of the Act.

The drafters of the regulations expressly rejected a suggestion which would have limited access for research purposes to certified research organizations. Specifically "certification" criteria would have been extremely difficult to draft and would have inevitably led to unnecessary restrictions on legitimate research.

Section 524(a) of the Act which forms part of the requirements of this section states:

"Except as provided by Federal law other than this title, no officer or employee of the Federal Government, nor any recipient of assistance under the provisions of this title shall use or reveal any research or statistical information furnished under this title by any person and identifiable to any specific private person for any purpose other than the purpose for which it was obtained in accordance with this title. Copies of such information shall be immune from legal process, and shall not, without the consent of the person furnishing such information, be admitted as evidence or used for any purpose in any action suit, or other judicial or administrative proceedings."

LEAA anticipates issuing regulations, pursuant to section 524(a) as soon as possible.

§ 20.21(c)(2). Presently some employers are circumventing State and local dissemination restrictions by requesting applicants to obtain an official certification of no criminal record. An employer's request under the above circumstances gives the applicant the unenviable choice of invasion of his privacy or loss of possible job opportunities. Under this subsection routine certifications of no record would no longer be permitted. In extraordinary circumstances, however, an individual could obtain a court order permitting such a certification.

§ 20.21(c)(3). The language of this subsection leaves to the States the question of who among the agencies and individuals listed in § 20.21(b) shall actually receive criminal records. Under these regulations a State could place a total ban on dissemination if it so wished. The State could, on the other hand, enact laws authorizing any member of the private sector to have access to non-conviction data.

§ 20.21(d). Non-criminal justice agencies will not be able to receive records of juveniles unless the language of a statute or court order, rule, or court decision specifies that juvenile records shall be available for dissemination. Perhaps the most controversial part of this subsection is that it denies access to records of juveniles by Federal agencies conducting background investigations for eligibility to classified information under existing legal authority.

§ 20.21(e) Since it would be too costly to audit each criminal justice agency in most

States (Wisconsin, for example, has 1075 criminal justice agencies) random audits of a "representative sample" of agencies are the next best alternative. The term "representative sample" is used to insure that audits do not simply focus on certain types of agencies. Although this subsection requires that there be records kept with the names of all persons or agencies to whom information is disseminated, criminal justice agencies are not required to maintain dissemination logs for "no record" responses.

§ 20.21(f). Requirements are set forth which the States must meet in order to assure that criminal history record information is adequately protected. Automated systems may operate in shared environments and the regulations require certain minimum assurances.

§ 20.21(g)(1). A "challenge" under this section is an oral or written contention by an individual that his record is inaccurate or incomplete; it would require him to give a correct version of his record and explain why he believes his version to be correct. While an individual should have access to his record for review, a copy of the record should ordinarily only be given when it is clearly established that it is necessary for the purpose of challenge.

The drafters of the subsection expressly rejected a suggestion that would have called for a satisfactory verification of identity by fingerprint comparison. It was felt that States ought to be free to determine other means of identity verification.

§ 20.21(g)(5). Not every agency will have done this in the past, but henceforth adequate records including those required under 20.21(e) must be kept so that notification can be made.

§ 20.21(g)(6). This section emphasizes that the right to access and review extends only to criminal history record information and does not include other information such as intelligence or treatment data.

§ 20.22(a). The purpose for the certification requirement is to indicate the extent of compliance with these regulations. The term "maximum extent feasible" acknowledges that there are some areas such as the completeness requirement which create complex legislative and financial problems.

NOTE: In preparing the plans required by these regulations, States should look for guidance to the following documents: National Advisory Commission on Criminal Justice Standards and Goals, Report on the Criminal Justice System; Project SEARCH: Security and Privacy Considerations in Criminal History Information Systems, Technical Reports No. 2 and No. 13; Project SEARCH: A Model State Act for Criminal Offender Record Information, Technical Memorandum No. 3; and Project SEARCH: Model Administrative Regulations for Criminal Offender Record Information, Technical Memorandum No. 4.

Subpart C–§ 20.31. This section defines the criminal history record information system managed by the Federal Bureau of Investigation. Each state having a record in the III System must have fingerprints on file in the FBI CJIS Division to support the III System record concerning the individual.

Paragraph (b) is not intended to limit the identification services presently performed by the FBI for local, state, tribal, and federal agencies.

§ 20.32. The grandfather clause contained in paragraph (c) of this section is designed, from a practical standpoint, to eliminate the necessity of deleting from the FBI's massive files the non-includable offenses that were stored prior to February, 1973. In the event a person is charged in court with a serious or significant offense arising out of an arrest involving a non-includable offense, the non-includable offense will also appear in the arrest segment of the III System record.

§ 20.33(a)(3). This paragraph incorporates provisions cited in 28 CFR 50.12 regarding dissemination of identification records outside the federal government for noncriminal justice purposes.

§ 20.33(a)(6). Noncriminal justice governmental agencies are sometimes tasked to perform criminal justice dispatching functions or data processing/information services for criminal justice agencies as part, albeit not a principal part, of their responsibilities. Although such inter-governmental delegated tasks involve the administration of criminal justice, performance of those tasks does not convert an otherwise non-criminal justice agency to a criminal justice agency. This regulation authorizes this type of delegation if it is effected pursuant to executive order, statute, regulation, or interagency agreement. In this context, the noncriminal justice agency is servicing the criminal justice agency by performing an administration of criminal justice function and is permitted access to criminal history record information to accomplish that limited function. An example of such delegation would be the Pennsylvania Department of Administration's Bureau of Consolidated Computer Services, which performs data processing for several state agencies, including the Pennsylvania State Police. Privatization of the data processing/information services or dispatching function by the noncriminal justice governmental agency can be accomplished pursuant to § 20.33(a)(7) of this part.

§ 20.34. The procedures by which an individual may obtain a copy of his manual identification record are set forth in 28 CFR 16.30–16.34.

The procedures by which an individual may obtain a copy of his III System record are as follows: If an individual has a criminal record supported by fingerprints and that

record has been entered in the III System, it is available to that individual for review, upon presentation of appropriate identification, and in accordance with applicable state and federal administrative and statutory regulations. Appropriate identification includes being fingerprinted for the purpose of insuring that he is the individual that he purports to be. The record on file will then be verified as his through comparison of fingerprints.

Procedure. 1. All requests for review must be made by the subject of the record through a law enforcement agency which has access to the III System. That agency within statutory or regulatory limits can require additional identification to assist in securing a positive identification.

2. If the cooperating law enforcement agency can make an identification with fingerprints previously taken which are on file locally and if the FBI identification number of the individual's record is available to that agency, it can make an on-line inquiry through NCIC to obtain his III System record or, if it does not have suitable equipment to obtain an on-line response, obtain the record from Clarksburg, West Virginia, by mail. The individual will then be afforded the opportunity to see that record.

3. Should the cooperating law enforcement agency not have the individual's fingerprints on file locally, it is necessary for that agency to relate his prints to an existing record by having his identification prints compared with those already on file in the FBI, or, possibly, in the state's central identification agency.

4. The subject of the requested record shall request the appropriate arresting agency, court, or correctional agency to initiate action necessary to correct any stated inaccuracy in his record or provide the information needed to make the record complete.

§20.36. This section refers to the requirements for obtaining direct access to the III System.

§20.37. The 120-day requirement in this section allows 30 days more than the similar provision in subpart B in order to allow for processing time that may be needed by the states before forwarding the disposition to the FBI.

[Order No. 662–76, 41 FR 34949, Aug. 18, 1976, as amended by Order No. 1438–90, 55 FR 32075, Aug. 7, 1990; Order No. 2258–99, 64 FR 52229, Sept. 28, 1999]

PART 21—WITNESS FEES

Sec.

21.1 Definitions.
21.2 Employees of the United States serving as witnesses.
21.3 Aliens.
21.4 Fees and allowances of fact witnesses.
21.5 Use of table of distances.
21.6 Proceedings *in forma pauperis.*
21.7 Certification of witness attendance.

AUTHORITY: 28 U.S.C. 509, 510, 1821–1825, 5 U.S.C. 301.

SOURCE: 51 FR 16171, May 1, 1986, unless otherwise noted.

§21.1 Definitions.

(a) *Agency proceeding.* An agency process as defined by 5 U.S.C. 551 (5), (7) and (9).

(b) *Alien.* Any person who is not a citizen or national of the United States.

(c) *Judicial proceeding.* Any action or suit, including any condemnation, preliminary, informational or other proceeding of a judicial nature. Examples of the latter include, but are not limited to, hearings and conferences before a committing court, magistrate, or commission, grand jury proceedings, pre-trial conferences, depositions, and coroners' inquests. It does not include information or investigative proceedings conducted by a prosecuting attorney for the purpose of determining whether an information or charge should be made in a particular case. The judicial proceeding may be in the District of Columbia, a State, or a territory or possession of the United States including the Commonwealth of Puerto Rico or the Trust Territory of the Pacific Islands.

(d) *Pre-trial conference.* A conference between the Government Attorney and a witness to discuss the witness' testimony. The conference must take place after a trial, hearing or grand jury proceeding has been scheduled but prior to the witness' actual appearance at the proceeding.

(e) *Residence.* The term *residence* is not limited to the legal residence, but includes any place at which the witness is actually residing and at which the subpoena or summons is served. If the residence of the witness at the time of appearance is different from the place of subpoena or summons, the new place of residence shall be considered the witness' residence for computation of the transportation allowance; but, if the witness is on a business or vacation trip at the time of appearance, the witness shall be paid for travel from the place of service if this does not result

2016
RSJI COMMUNITY SURVEY

SEATTLE OFFICE FOR CIVIL RIGHTS

APRIL 2017

Acknowledgements

The RSJI Community Survey is the result of collaboration among researchers, community leaders and the City of Seattle who worked together as part of a Race and Social Justice Community Survey Steering Committee. We thank the Steering Committee for guiding the development of the survey questions and outreach.

Thank you to Gabriela Quintana for overall project coordination, including managing outreach. Outreach also was made possible through the support of our Community Survey Partners, City employees, and students from the University of Washington. Special thanks to Sarah Leyrer, Margaret Weihs, Brian Cedeno, Kelsey McGuire, Hillary Jaregui, Cornetta Mosley, Tucker Richards, Kathryn Peebles, Junyi Zhang, Violet Lavatai, Darcy White and Fadumo Nurdin.

Thank you to Pacific Market Research for fielding the phone survey.

Special thanks to Chris Hess at the University of Washington Sociology Department for providing data analysis and an early draft that laid the foundation for the final report.

2016 Race and Social Justice Initiative
Community Survey
Steering Committee Members

Derrick Belgarde, Chief Seattle Club

Kyle Crowder, University of Washington

Ben Danielson, Odessa Brown Medical Center

Patricia Hayden, Seattle Human Services Coalition

Marcos Martinez, Entre Hermanos

Xochitl Maykovich, Washington Community Action Network

India Ornelas, University of Washington

Rebecca Saldaña, Puget Sound Sage

Michael Ramos, Church Council of Greater Seattle

Jenny Romich, University of Washington

Rich Stolz, OneAmerica

Executive Summary

The Seattle Race and Social Justice Initiative (RSJI) is the City of Seattle's commitment to ending racial disparities and achieving racial equity in Seattle. In 2014, the City affirmed and expanded RSJI via an Executive Order requiring City staff to assess progress made on racial equity. It also called on the Race and Social Justice Initiative to deepen the City's support for community-led racial justice work through projects and programs that increase the City's accountability to the community. The RSJI Community Survey is a key part of assessing the impact of our collective efforts for racial equity.

The RSJI Community Survey, first fielded in 2013, measures the perspectives of those who live, work, and go to school in Seattle, including satisfaction with City services, neighborhood quality, housing affordability, feelings about the state of racial equity in the city, and the role of government in addressing racial inequities. The 2016 survey provides updated information on the state of racial equity in Seattle.

Key Findings

1 **Ending racial inequity is a responsibility of government.**

Seattle respondents feel strongly that government should prioritize ending the racial equity gaps that impact our communities. Nearly all respondents (96%) said government should prioritize addressing racial inequities.

2 **To achieve equity, resources must be allocated based on need.**

Eighty-seven percent of all respondents agreed when asked whether a greater portion of resources should go to those most in need.

3 **Economic prosperity is not felt by all -- Seattle's Black community experiences a disproportionate lack of opportunity.**

More than half (53%) of all Black/African American survey respondents said they are *not* experiencing economic opportunities; Black/African American women cite the highest rates of economic exclusion.

4 **Environmental inequities persist by race and gender.**

People of color and transgender respondents were more likely to say their neighborhoods are unhealthy places to live; close to half of all American Indian/Alaska Native respondents do not feel they have benefited from Seattle's environmental progress.

5 **Communities of color do not feel they experience equal treatment by the City's criminal justice system.**

The number of people across the board reporting greater confidence in the police has increased since the last survey, but communities of color continue to have less confidence in the police than White

respondents do. More than half of all African American/Black respondents (56.1%), and nearly half of all Multiracial respondents (47.3%) and American Indian/Alaska Native (47%) respondents have little to no confidence in the police to do a good job enforcing the law.

There is a strong lack of confidence in the courts to treat people of color and Whites equally, with nearly 70% of people of color reporting a lack of confidence.

6 **Communities of color and other vulnerable groups struggle to remain in our high-cost city.**

Thirty-four percent (34.4%) of those surveyed responded that they or someone in their family have moved out of Seattle in the past two years due to the rising cost of housing. American Indian/Alaska Native, Black/African American, Multiracial, and Latino respondents were most likely to say so than other groups.

Every racial group rated the number one reason they personally had moved out of Seattle to be the need to find lower rent or a less expensive house to maintain. At the same time, people of color cited other economic reasons (such as foreclosure or eviction) more often than White respondents.

7 **Seattle Public Schools struggle to make the grade with communities of color.**

Despite some mixed opinions regarding performance and preparation of students for the future, Seattle respondents were united in support of ending punitive discipline measures and improving schools and after-school programs to promote racial equity. Differences in perceptions of Seattle Public Schools (SPS) emerged along racial lines. The web survey showed that while 44.5% of young people ages 15-25 rated SPS favorably, youth of color were less likely to rate Seattle Public Schools favorably compared to their White counterparts.

8 **City efforts to be inclusive are making some inroads, but more work needs to be done.**

In both phone and web surveys, we saw a decline in the number of people who felt their participation in City processes was valued. Despite this overall decline, the web survey found communities of color and lesbian, gay and bisexual respondents felt their participation was valued at a greater rate than reported in 2013. This did not hold for transgender respondents who were less likely to say their participation was valued compared to 2013.

9 **Progress towards racial equity is not being felt by all. Urgency and action is necessary to make a difference in people's lives.**

Both phone and web surveys revealed a decline in the percentage of people agreeing that Seattle is making progress at eliminating racial inequity. Seventy-two percent of phone and 43% of web respondents agree that Seattle is making progress. This is a decline by a margin of 7% points in the web survey and a margin of 14% in the web survey. When disaggregated by race, the percent stayed consistent for communities of color compared to 2013, while an increasing number of White respondents do not believe the City is making progress.

Conclusion

Seattle remains a City with much work to do to achieve racial equity. The Race and Social Justice Initiative is tasked with leading municipal government's efforts to put our value of racial equity into action. The 2013 survey provided us with baseline data on the experiences of people who live, work, and go to school in Seattle. The 2016 survey reveals sobering information that the City cannot afford to ignore: despite our efforts to address inequities, **we continue to see disparate outcomes** for our communities by race and other factors. If we are going to truly see a difference in people's lives, we must invest in community-driven strategies that hold us accountable to those most impacted by structural racism and other biases. We can and we must do better.

Methodology

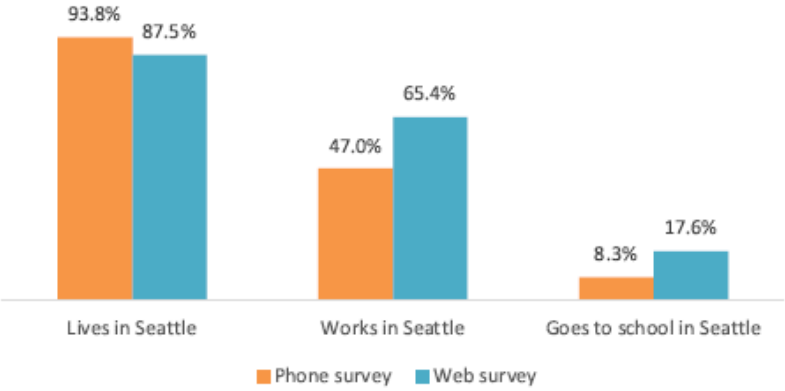
The Race and Social Justice Community Survey was developed in partnership with a steering committee comprised of researchers from the University of Washington, community based organizations and local government. Steering Committee members guided question development and outreach.

Survey data was collected via phone and internet. The phone survey included 400 respondents and the web survey included 1,295 for a total of 1,695 respondents. Phone and web surveys differed in a few key ways: the phone survey was fielded using random digit dialing (with a 60/40 split between landline and wireless phones), while the web survey was composed of self-selected respondents. Outreach efforts for the web survey were conducted by City staff and a team of student volunteers from the University of Washington who asked community partners to send the survey link to their clients and members, visited homeless shelters and community centers and posted the survey link at libraries.

Who we heard from

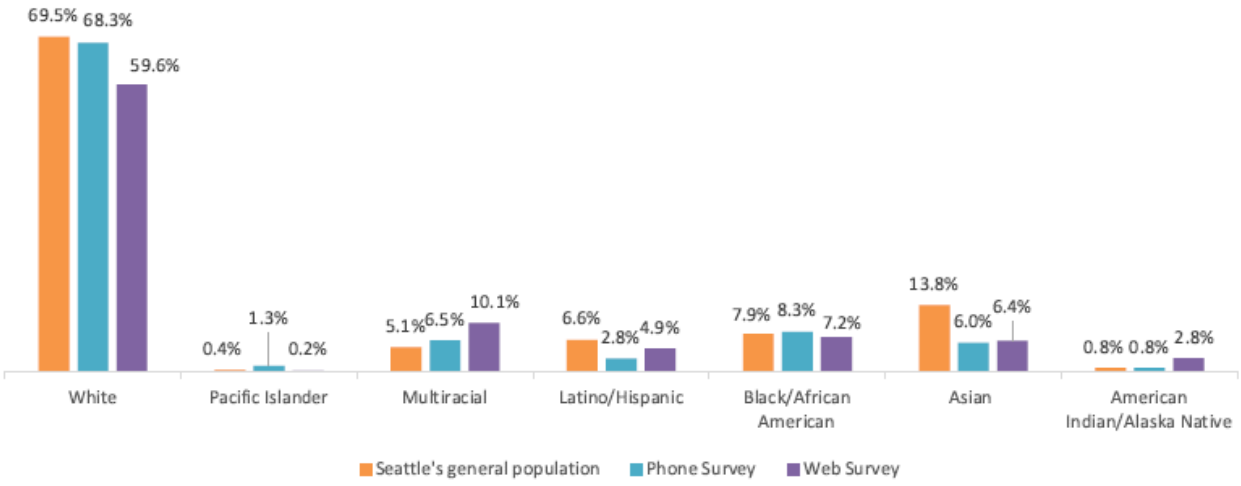
The survey was open to anyone who lives, works, or goes to school in Seattle. Nearly all respondents live in Seattle and nearly half of all phone respondents and more than half of all web respondents work in Seattle. Eighteen percent of those surveyed by web go to school in Seattle, slightly more than twice the rate of those surveyed by phone [Figure 1].

Figure 1. Percent of respondents by survey type who live, work and go to school in Seattle



In terms of race, the phone survey most closely matched the demographics of Seattle for White respondents, Black/African American respondents, Multiracial respondents, and American Indian/Alaska Native respondents. Both surveys received an under representation of Latino and Asian/Pacific Islander respondents compared to their percent of the overall population [Figure 2].

Figure 2. Comparison of survey respondents to overall Seattle population by race



*Note: Survey only fielded to those over the age of 15. Seattle general population data above includes those under 15.

In terms of age, the phone survey respondents skewed older. For reference, the Census Bureau's most recent American Community Survey (ACS) found that about 10% of the Seattle population is 65 years of age or older. Of those surveyed by phone, 35% of the phone survey respondents was 65 or older. In terms of gender, the ACS only records male and female genders and estimates a 50/50 split in the Seattle population. This suggests that the web data over-surveyed females, with 65% identifying as female.

The report uses a combination of individual and pooled in lieu of weighting tabulations to account for variations in sample sizes. Web surveying had an explicit goal of reaching subpopulations across many dimensions, including those experiencing homelessness. Researchers providing guidance on this survey, were concerned that weighting might undermine that study design goal. Without the certainty that weighting would improve the substantive conclusions, researchers opted to analyze the data as observed/collected, and use pooled estimates as an alternative way to show overall distributions, with the non-response bias of each dataset to some extent cancelling the other's out. Pooling the data potentially averages out some of the differences in demographic composition relative to the overall Seattle population.

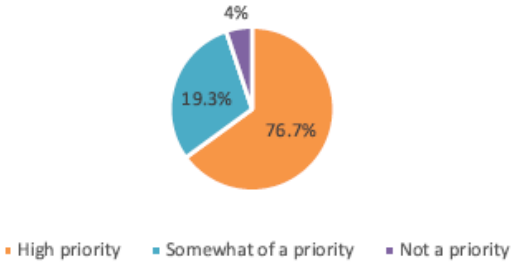
1 Ending racial inequity is a responsibility of government.

Survey respondents feel strongly that government should prioritize the racial equity gaps impacting our communities. More people see this is a high priority than two years ago.

- Nearly all respondents (96%) said government should prioritize addressing racial inequities, with **nearly 8 in 10 people saying racial equity should be a "high priority" of government** [Figure 3].

- The number respondents stating that racial equity work should be a "high priority" for government has increased over time. In our 2013 phone survey, 51% rated it as such. In the 2016 phone survey, it increased by 13 percentage points to 64%. The web responses increased only slightly from 74% in 2013 to 77% in 2016.

Figure 3. How high a priority should it be for government to address racial equity gaps in education, criminal justice, jobs, health, housing and other areas?
(Pooled data, N=1621)



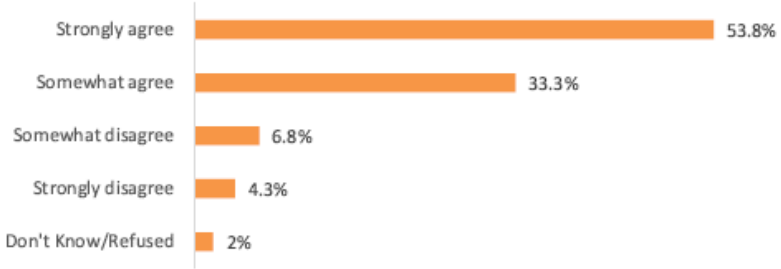
- **The urgency and responsibility for government to act was clearly reflected in responses of Black/African American and Latino respondents,** 95% and 80% of whom said addressing these gaps should be a high priority (pooled data).

2 To get to equity, resources must be allocated based on need.

- When asked if a greater portion of resources should go to those most in need to create equity for all, 87% agreed [pooled data].

- Over half (53.8%) of all phone respondents strongly agreed [Figure 4].

Figure 4. Responses to statement, "To create equity and opportunity for all, I believe a greater portion of resources should go to those who are most in need."
(Phone survey, N=400)



3 Economic prosperity is not felt by all -- Seattle's Black community experiences a disproportionate lack of opportunity.

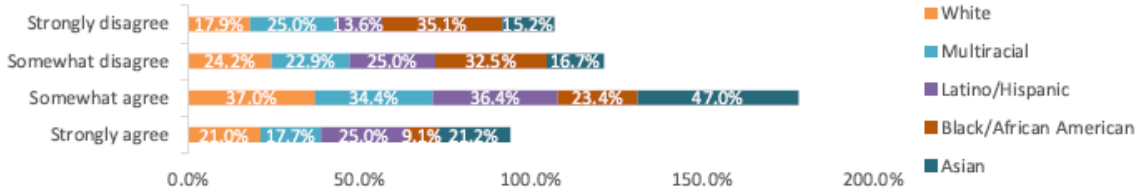
Overall, the percentage of people experiencing opportunities to get ahead economically in Seattle has decreased over time. While over half of survey respondents (62% phone and 52% web) agreed that Seattle offers good economic opportunities, these figures are a significant decrease from prior phone surveys where in 2013, 80% and in 2001, 86% of respondents reported favorable opportunities.

- The impact of a lack of economic opportunities felt by the Black community cannot be understated. **More than half (58.5%) of all Black/African American surveyed said they are *not* experiencing economic opportunities.** No other racial group reported this high a lack of opportunity [Figure 5].

Figure 5. Percent of individuals by race who disagree that Seattle has offered good opportunties for them to get ahead economically
(Pooled data, N=1448)

- An analysis of responses across race among female respondents found that **a strong majority (67%) of Black/African American women were dissatisfied with the opportunities Seattle affords them to get ahead economically** [Figure 6]**.** Considering the 2013 survey observed a similar differential for women of color, the surveys together suggest differences in economic opportunity for Black/African American women have remained prominent post-recession.

Figure 6. Female respondents by race who responded to the question, "To what extent do you agree that Seattle has offered you good opportunities to get ahead economically?"
(Pooled data, N=916)

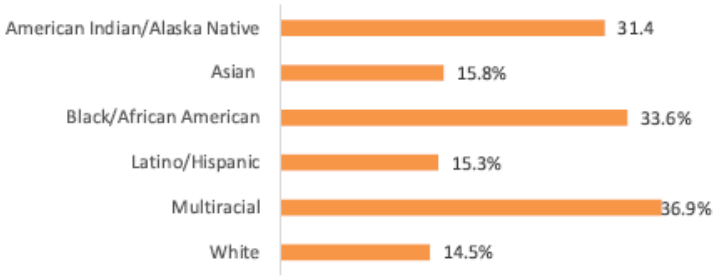


4 Environmental inequities persist by race and gender.

Seattle is noted nationally for its strong environmental efforts and as a healthy place to live. Strong majorities of phone and web survey respondents agree (88.5% phone/76.7% web). Yet when disaggregated by race and by gender, inequities emerge. People of color and transgender respondents were more likely not to find their neighborhood a healthy place to live.

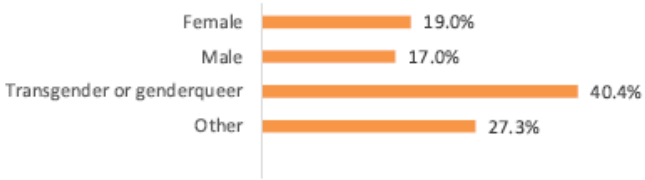
- Multiracial, Black/African American and American Indian/Alaska Native respondents were less likely to report than other groups that their neighborhood is a healthy place to live [Figure 7].

Figure 7. Percent of respondents by race who disagree with the statement, "My neighborhood is a healthy place to live."
(Pooled data, N=1480)



- In the web survey, transgender and genderqueer respondents were significantly less likely to report that their neighborhood is a healthy place to live [Figure 8].

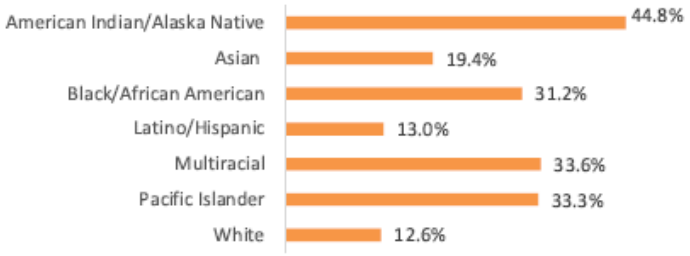
Figure 8. Percent of respondents by gender who disagree with the statement, "My neighborhood is a healthy place to live."
(Web survey, N=1195)



Similarly, while most respondents felt they benefited from the city's environmental progress (71% phone/ 67% web), the feeling was not shared across race.

- White survey respondents were more than twice as likely to *strongly agree* that they have benefited compared to American Indian/Alaska Native, Black/African American, and Multiracial respondents.
- Close to half (44.8%) of all American Indian/Alaska Native people who completed the web survey felt they did not benefit [Figure 9].

Figure 9. Percent of web respondents by race who disagree with the statement, "I have benefited from Seattle's environmental progress."
(Web survey, N=1033)

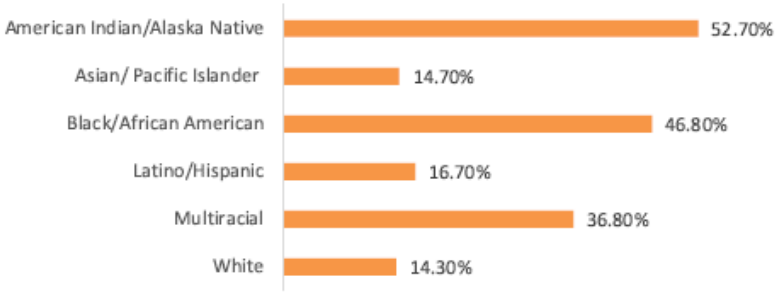


5 Criminal justice -- equal treatment not felt by communities of color.

The survey reflected strong difference in how people of color and White respondents are experiencing the criminal justice system. Confidence in the police to do a good job enforcing the law and in the police and courts to treat people of color and Whites equally found mixed evaluations—particularly when analyzed across race.

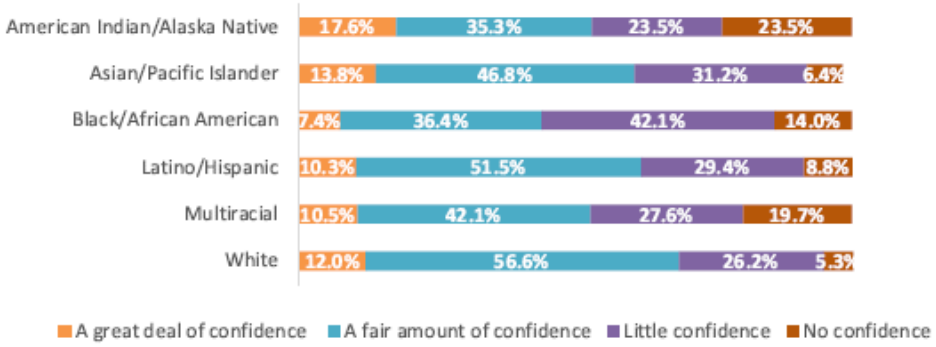
- **More than half of American Indian/Alaska Native (52.7%)** and **nearly half of all Black/African American (46.8%)** respondents surveyed reported being questioned by the police, charged or arrested when they had not committed a crime [Figure 10].

Figure 10. Responded "Yes" to the question, "Have you ever been questioned by the police, charged, or arrested when you had not committted a crime?"
(Pooled data, N = 1602)



- **More people reported confidence in the police to do a good job enforcing the law.** Seventy-eight percent of phone respondents had at least fair confidence in the police to enforce the law, an increase in the phone survey responses from 2013, when only 66% of phone respondents reported at least fair confidence. The web responses over time have not shifted in the same way. The percentage of web respondents reporting a fair amount of confidence in the police increased only 1% in the last two years, from 53% in 2013 to 54% in 2015.

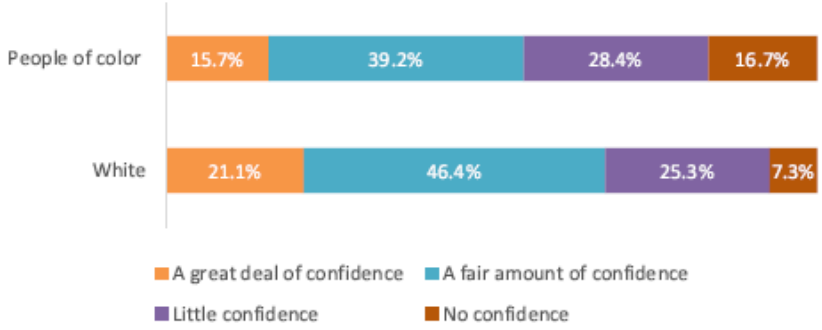
Figure 11. Confidence in police to do a good job enforcing the law?
(Pooled data, N=1,986)



- **Despite the increase, communities of color continue to have less confidence in the police than White respondents.** More than half of all African American/Black respondents (56.1%), nearly half of all Multiracial respondents (47.3%), and American Indian/Alaska Native (47%) respondents had little to no confidence in the police to do a good job enforcing the law [Figure 11].

- **People of color are more likely than White respondents to report a lack of confidence in equal treatment by the police.** Close to half (45.1%) of people of color surveyed by phone had little to no confidence in police officers treating people of color and Whites equally, compared to 32.6% of White respondents [Figure 12].

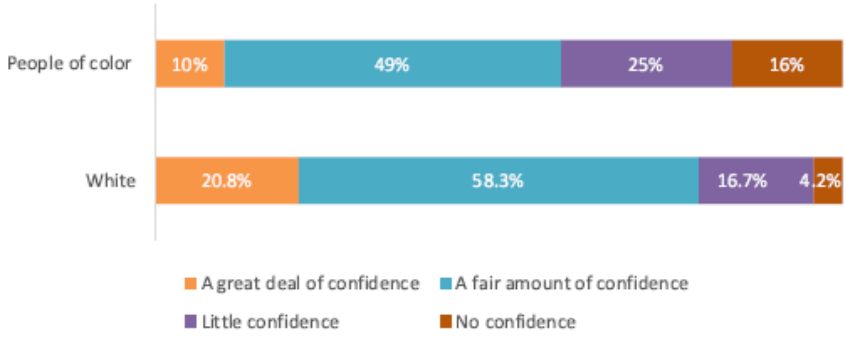
Figure 12. Confidence in police officers to treat people of color and White people equally?
(Phone data, N = 372)



The pooled data showed an even higher lack of confidence (68.8% for people of color and 61.4% for White respondents) but a smaller disparity between the two groups.

- When it came to the court system, the differences in perceptions were starker between people of color and White respondents who were surveyed by phone. **People of color were twice as likely as White respondents to lack confidence in the courts to treat people equally across race.** Forty-one percent of people of color had little to no confidence in equal treatment, compared to 20.9% of White respondents [Figure 13]. Like the data regarding confidence in police, the pooled data showed across race, a greater rate of lack of confidence in equal treatment with 70% of people of color and 63% of White respondents reporting little to no confidence.

Figure 13. Confidence in courts to treat people of color and White people equally?
(Phone data, N=370)



- When asked what top three things the City should prioritize to reduce racial disproportionately in the criminal justice system, respondents were most likely to name better schools and after school programs, requiring anti-bias training for police and courts and community-based alternatives to arrest and detention [Figure 14]. This held for youth ages 15-25, and generally across race.

Figure 14. Top three actions City government should prioritize to reduce racial disproportionality in the criminal justice system
(Pooled data, N=1674)

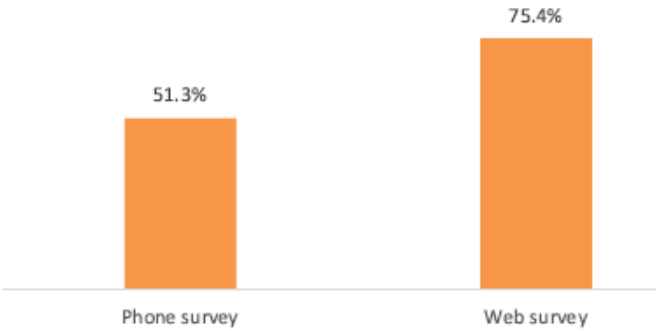
6 Housing: Communities struggle to remain in the city.

Housing Affordability: – While across race people regard Seattle's housing affordability as poor, people of color and lesbian, gay, bisexual, and transgender respondents are disproportionately feeling pushed out.

- **Since the 2013 survey, more people regard Seattle's housing as unaffordable.** In the two years between phone surveys, those reporting affordability as "only fair" or "poor" grew by 4% from 78% in 2013 to 82% in 2016.

- The majority surveyed by phone and web rated Seattle's housing affordability as "poor" [Figure 15].

Figure 15. Percent rating Seattle's housing affordability as "poor"



- **Both surveys found people of color *more likely* than White respondents to say that it was "not very likely" or "unlikely" that they would be able to afford to live in Seattle in 5 years.** The web survey found a greater percentage of respondents across the board stating that they would likely not be able to afford living in Seattle in five years. Both surveys showed a difference of 11% between people of color and White respondents, with people of color more likely to report not being able to afford living in Seattle in five years.

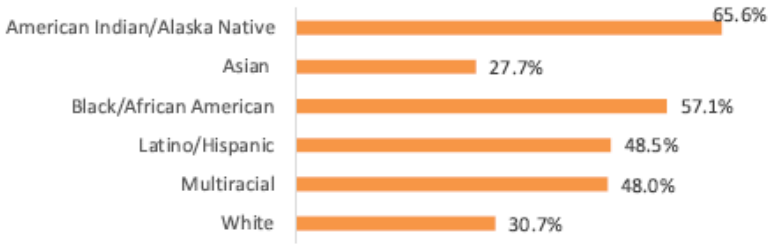
- **Nearly 70% of renters in the web survey said it was "very unlikely" to "unlikely" that they would be able to afford to live in Seattle in the next 5 years, compared to 28% of home owners.** While being a renter in Seattle clearly signals a sense of uncertainty in the ability to live in our high-cost city, **race continues to be a factor** in determining people's beliefs that they will be displaced. **African American and Black renters were disproportionately more likely than White renters to feel they will not be able to remain in Seattle in the next 5 years.** (In the web survey, 78.6% of African American/Black renters said they are not very likely or unlikely to remain in Seattle, compared to 65.4% of White renters).

- **In the web survey, transgender people of color were most likely to say they would be unable to afford living in Seattle in the next 5 years. In the web survey,** 80% of transgender/genderqueer people of color stating that it was unlikely they would be able to remain in Seattle in the next five years. Sixty-two percent (63%) of white

transgender/genderqueer respondents and 58% of lesbian, gay and bisexual respondents across race agreed.

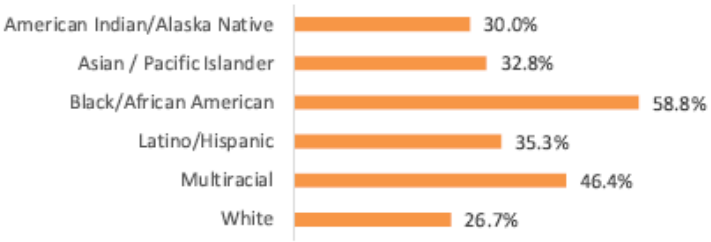
- **Thirty-four percent (34.4%) surveyed responded that they or someone in their family had moved out of Seattle in the past two years due to the rising cost of housing**. American Indian/Alaska Native, Black/African American, Multiracial, and Latino respondents were most likely to say so [Figure 16].

Figure 16. Percent by race responding "yes" to the question, "Have you or someone in your family moved out of Seattle in the past two years due to the rising cost of housing?"
(Pooled data, N=1,526)



- Places of worship, gathering places and cultural centers are often community anchors, grounding a community and providing a strong network of support. **More than half of African Americans/Black respondents (58.8%) to the web survey said it was "not very likely" or "unlikely" for their cultural center, place of worship or gathering place to remain located in Seattle in 5 years** [Figure 17].

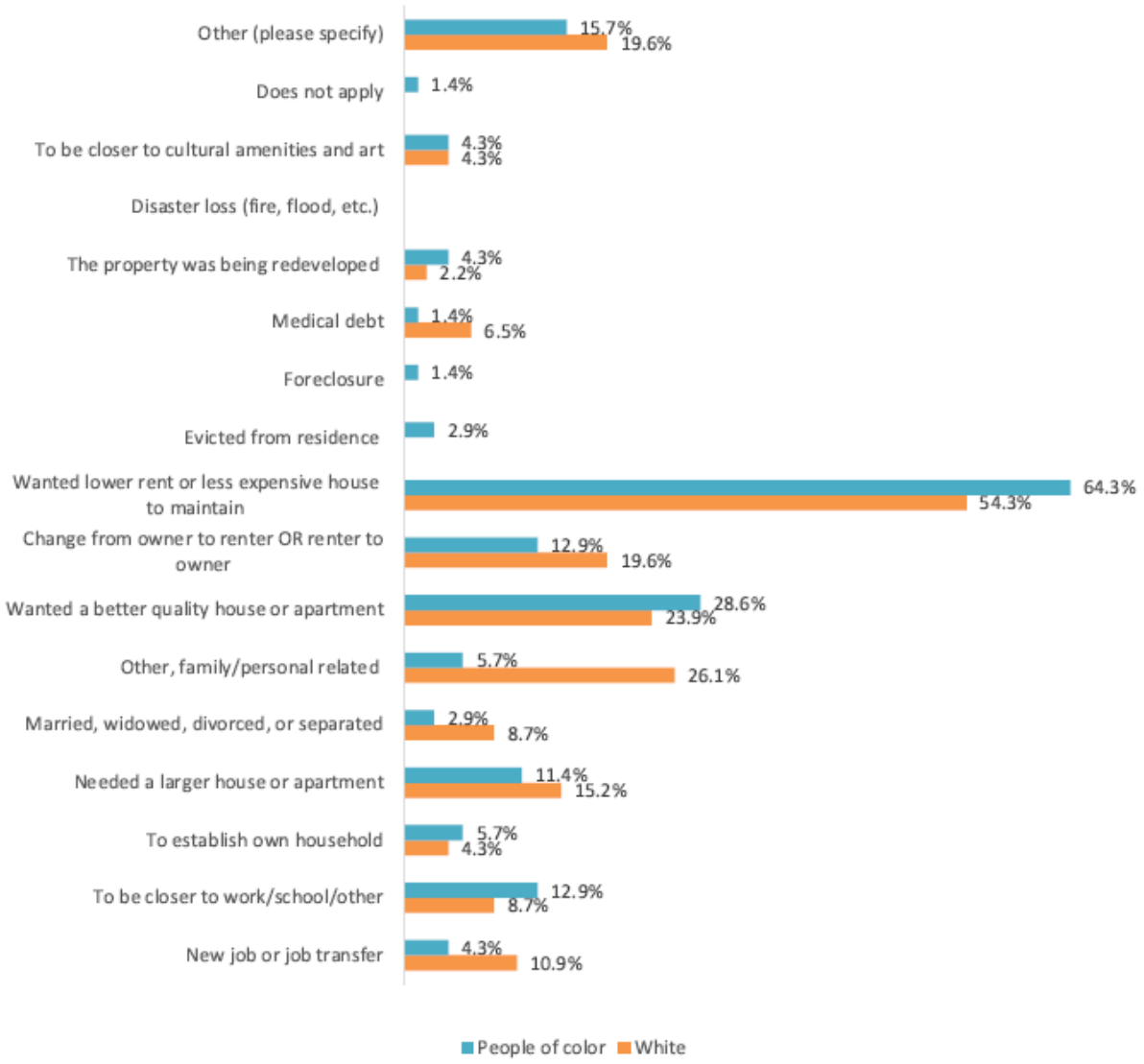
Figure 17. "Not very" or "unlikely" for your cultural center, place of worship or gathering place will be located in Seattle in 5 years
(web survey, N=342)



The web survey showed that across race, the number one reason people moved out of Seattle was for less expensive housing. People of color were more likely to cite, property redevelopment, foreclosure or eviction for having to move than White residents [Figure 18].

Figure 18. Main reasons people moved out of Seattle in last two years

(Web survey, N = 498)



Is the City doing enough to ensure people can afford to stay in Seattle?

- When asked whether the City was doing enough to ensure people can afford to stay living in Seattle, strong majorities in both the phone and web surveys (71% and 82.8% respectively) disagreed.

The role of City investments.

- The survey asked respondents if they felt City of Seattle public investments (such as transportation and utilities) have created housing affordability problems in certain neighborhoods. While 60.2% of web respondents agreed that they had, the distribution by race of those agreeing was for the most part similar, except for Asian/Pacific Islanders, who were most likely to agree by at least 7% points higher than other groups.

Quality of life is not always high for people of color, renters and people with disabilities.

- People with disabilities were nearly twice as likely to be dissatisfied with Seattle's quality of life compared to those without disabilities, 22.6% compared to 11% (pooled data).

- While all groups had a strong proportion reporting satisfaction, African Americans and American Indian/Alaska Natives who completed the web survey were nearly three times as likely as White respondents to say they were dissatisfied or very dissatisfied with the quality of life in their neighborhoods (23% and 24% compared to 8% respectively).

- Renters (29.7%) were more likely than home owners (17.6%) to be dissatisfied with Seattle as a place to raise children (web survey).

7 Education – Seattle Public Schools struggles to make the grade with communities of color.

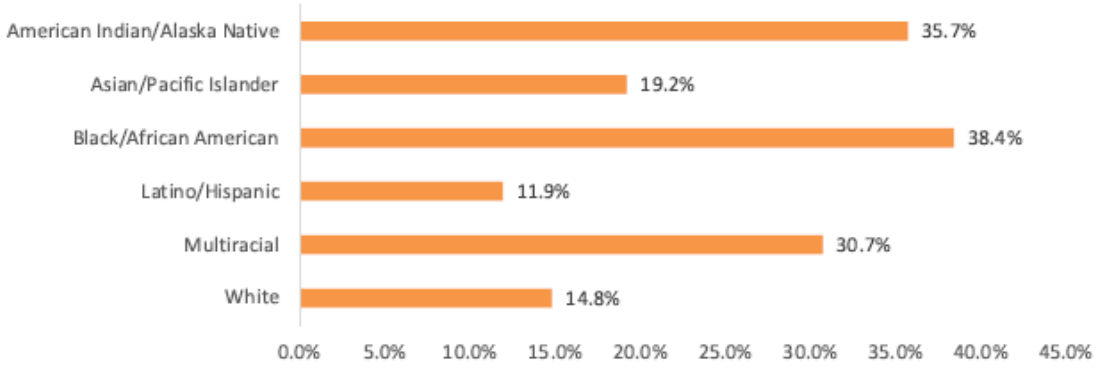
Ratings of Seattle Public Schools (SPS) were mixed across both the phone and web surveys, particularly among people of color. Despite some mixed opinions regarding SPS's performance and preparation of students for the future, responses were united in support of ending punitive discipline measures and improving schools and after-school programs to promote racial equity.

- When asked, "How do you rate Seattle Public Schools?", responses from the phone survey were nearly split in terms of favorable and unfavorable ratings (40% very good/good to 39%

fair/poor). Responses from the web data tended towards less favorable evaluations with 38.6% rating SPS as fair/poor and only 23.4% rating as good to very good [see attachment, Q 23, p11].

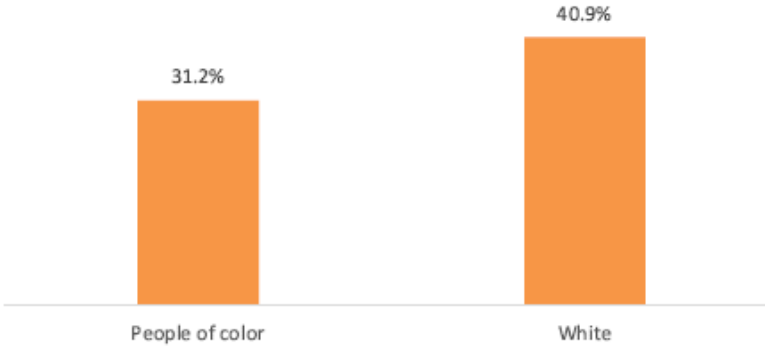
- In terms of race, Black, Native American, and Multiracial respondents gave SPS a "poor" rating more than other groups" [Figure 19].

Figure 19. Percent by race who rated Seattle Public Schools as "Poor"
(Pooled data, N=1071)



- The web survey showed that while 44.5% of young people ages 15-25 rated SPS favorably, when disaggregated by race, differences emerge. Youth of color were less likely to rate Seattle Public Schools favorably compared to their White counterparts [Figure 20].

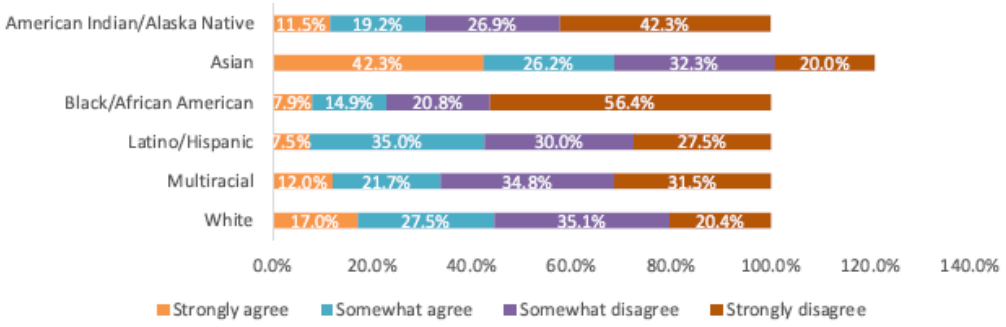
Figure 20. Percent of young people ages 15 to 25 rating SPS favorably (good/very good)
(Web survey, N=753)



- About 75% of each sample reported agreement with the statement, "Shifting from punitive discipline measures in Seattle Public Schools to measures that address harm and repair relationships is important to making sure all students, regardless of their race, receive fair and just treatment." [see Attachment, Q25] When analyzed by race, gender and sexual orientation, there was strong consensus across groups.

- Over half (56.4%) of all Black/African Americans surveyed and 42.3% of Native Americans surveyed strongly disagreed that staff and teachers at Seattle Public Schools treat students of color the same as white students [Figure 21].

Figure 21. Response by race to the statement, "Staff and teachers at Seattle Public Schools treat students of color with as much respect as white students"
(Pooled data, N=945)

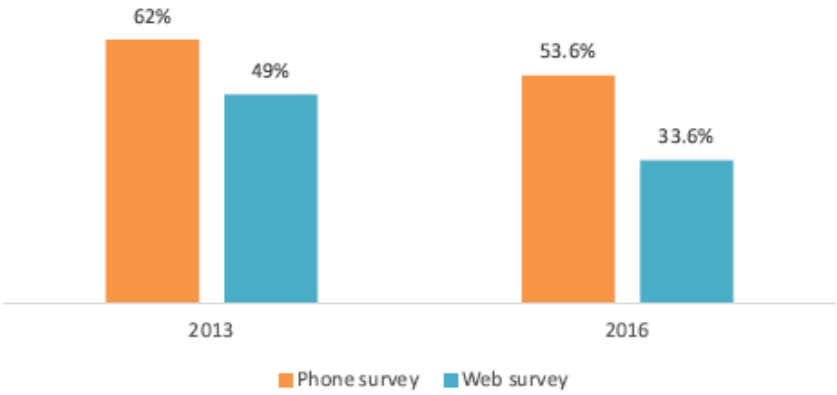


8 City efforts to be inclusive in outreach is having an impact on some groups, with more work to be done.

About half of those surveyed by phone and web (48.8% phone/51.5% web) were aware of the City of Seattle's outreach to the community on policies or projects, yet only 35.4% of those surveyed by phone and just about a quarter of those surveyed by web (26.4%) had participated.

- **Fewer people felt the City valued their participation.** Of those who had participated, over half of phone respondents (53.6%) said they felt their participation was valued a fair amount to a great deal while only 33.6% said the same in the web survey. This is a significant drop in the web responses since 2013, when 49% said they felt their participation was valued a fair amount to a great deal [Figure 22].

Figure 22. Felt participation in outreach engagement efforts was valued by the City of Seattle



- While overall, fewer people felt the City valued their participation, the racial disparity that existed in the 2013 web survey did not appear in 2016. In the 2016 web survey, **people of color were slightly more likely to say their participation was valued** a fair amount to a great deal compared to white respondents (35.1% to 32.8% respectively). This held true across race/ethnicities except for Asian Pacific Islander respondents who were approximately as likely as white respondents to say their participation was valued (32.2%).

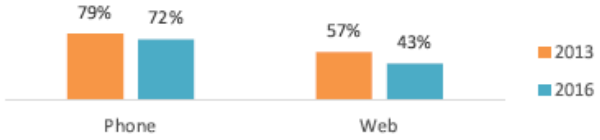
- Similarly, the disparities that existed in the 2013 web survey for lesbian, gay and bisexual respondents compared to straight respondents in terms of their participation feeling valued was not reported in the 2016 survey. Rather, **lesbian, gay, and bisexual respondents were more likely to feel their participation was valued** compared to their straight counterparts (37.3% to 32.6% respectively). This held for LGB people of color as well, of whom 39.1% said they felt their participation was valued, compared to 36% of LGB White respondents. **This did not hold for transgender respondents who were less likely to say their participation was valued** compared to 2013 (44.5% of transgender respondents said their participation was valued in 2013 which dropped to 27.3% in 2016).

- **Immigrants and refugees were slightly less likely to be aware of the City's outreach efforts than two years ago.** In 2013, 51% of web survey respondents born outside the U.S. were aware of the City's outreach efforts but fell to 46.5% in 2016.

9 Progress towards racial equity is not felt by all. Urgency and action is necessary to make a difference in people's lives.

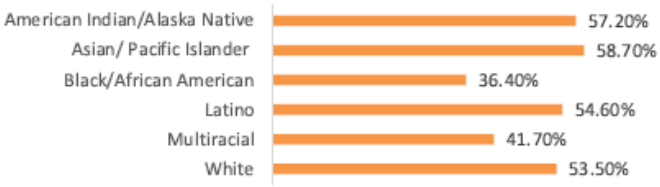
In 2016, fewer people said they believe Seattle is making progress eliminating racial inequities and creating a city where social, economic, and political opportunities and outcomes are not predicted upon a person's race than reported so in 2013 [Figure 23 and Figure 24].

Figure 23. Percent agreeing that Seattle is making progress eliminating racial inequities 2013 to 2016



Web survey data overtime shows that across race, the same or more people respond less favorably than they had in the previous survey. For example, while the percent of Black/African Americans who strongly disagreed that we are making progress held the same since the last survey (around 32%), White people were also more likely than they had been in 2013 to strongly disagree, moving from 11% in 2013 to 15% in 2016.

Figure 24. Percent agreeing that Seattle is making progress eliminating racial inequities
(web survey, N=1074)



Conclusion

For more than a decade the Race and Social Justice Initiative (RSJI) has been working to achieving racial equity within government. The 2013 Community Survey provided baseline data about who lives, works and goes to school in Seattle. The 2016 Community Survey reveals sobering facts that we cannot ignore. Despite our efforts to address the manifestations of institutional and structural racism, our communities of color continue to experience disparate outcomes in every quality of life indicator. If we are going to truly change the lives of the most impacted community members, **we must center community leadership, we must resource community-owned strategies and we must be accountable to our communities.**

We can and we must do better.

Appendix - 2016 Community Survey Frequency Tables

Question 1 — Which of the following applies to you? (Select all that apply):

Table 1: Respondent lives in Seattle

	Phone Survey	WebSurvey
Live in Seattle	375 (93.75%)	1133 (87.49%)
Does not live in Seattle	25 (6.25%)	162 (12.51%)

Table 2: Respondent works in Seattle

	Phone Survey	WebSurvey
Work in Seattle	188 (47%)	847 (65.41%)
Does not work in Seattle	212 (53%)	448 (34.59%)

Table 3: Respondent goes to school in Seattle

	Phone Survey	WebSurvey
Go to school in Seattle	33 (8.25%)	228 (17.61%)
Does not go to school in Seattle	367 (91.75%)	1067 (82.39%)

Question 2 — Please select which most closely matches your satisfaction with the quality of life in Seattle:

Table 4: Seattle as a place to live

	Phone Survey	Web Survey
Very satisfied	178 (44.5%)	434 (33.51%)
Somewhat satisfied	164 (41%)	645 (49.81%)
Dissatisfied	41 (10.25%)	115 (8.88%)
Very dissatisfied	13 (3.25%)	37 (2.86%)

Does not apply	1 (0.25%)	46 (3.55%)
Don't know / Refused	3 (0.75%)	18 (1.39%)

Table 5: Your neighborhood as a place to live

	Phone Survey	Web Survey
Very satisfied	221 (55.25%)	506 (39.07%)
Somewhat satisfied	150 (37.5%)	552 (42.63%)
Dissatisfied	21 (5.25%)	107 (8.26%)
Very dissatisfied	6 (1.5%)	30 (2.32%)
Does not apply	2 (0.5%)	66 (5.1%)
Don't know / Refused	0 (0%)	34 (2.63%)

Table 6: Seattle as a place to raise children

	Phone Survey	Web Survey
Very satisfied	134 (33.5%)	244 (18.84%)
Somewhat satisfied	139 (34.75%)	430 (33.2%)
Dissatisfied	34 (8.5%)	148 (11.43%)
Very dissatisfied	6 (1.5%)	47 (3.63%)
Does not apply	71 (17.75%)	380 (29.34%)
Don't know / Refused	16 (4%)	46 (3.55%)

Table 7: Seattle as a place to work

	Phone Survey	Web Survey
Very satisfied	186 (46.5%)	429 (33.13%)
Somewhat satisfied	131 (32.75%)	611 (47.18%)
Dissatisfied	36 (9%)	107 (8.26%)
Very dissatisfied	9 (2.25%)	31 (2.39%)
Does not apply	32 (8%)	90 (6.95%)
Don't know / Refused	6 (1.5%)	27 (2.08%)

Table 8: Seattle as a place to retire

	Phone Survey	Web Survey
Very satisfied	122 (30.5%)	179 (13.82%)
Somewhat satisfied	132 (33%)	317 (24.48%)
Dissatisfied	73 (18.25%)	243 (18.76%)
Very dissatisfied	43 (10.75%)	185 (14.29%)
Does not apply	16 (4%)	333 (25.71%)
Don't know / Refused	14 (3.5%)	38 (2.93%)

Question 3 — In comparison to other neighborhoods in the city, how do you rate your neighborhood's availability of City services, such as libraries, parks and recreation facilities?

	Phone Survey	Web Survey
Very good	235 (58.75%)	511 (39.46%)
Good	105 (26.25%)	456 (35.21%)
Fair	43 (10.75%)	217 (16.76%)
Poor	14 (3.5%)	69 (5.33%)
Don't know / Refused	3 (0.75%)	42 (3.24%)

Question 4 — Please state whether you strongly agree, somewhat agree, somewhat disagree or strongly disagree with the following statements: My neighborhood is a healthy place to live.

	Phone Survey	Web Survey
Strongly agree	207 (51.75%)	405 (31.27%)
Somewhat agree	147 (36.75%)	588 (45.41%)
Somewhat disagree	33 (8.25%)	188 (14.52%)
Strongly disagree	9 (2.25%)	56 (4.32%)
Don't know / Refused	4 (1%)	58 (4.48%)

Question 5 — Please state whether… : I have benefited from Seattle's environmental progress.

	Phone Survey	Web Survey
Strongly agree	108 (27%)	312 (24.09%)
Somewhat agree	174 (43.5%)	560 (43.24%)
Somewhat disagree	56 (14%)	146 (11.27%)
Strongly disagree	35 (8.75%)	55 (4.25%)
Don't know / Refused	27 (6.75%)	222 (17.14%)

Question 6 — Please state whether... : To what extent do you agree that Seattle has offered good opportunities for you to get ahead economically?

	Phone Survey	Web Survey
Strongly agree	120 (30%)	238 (18.38%)
Somewhat agree	128 (32%)	451 (34.83%)
Somewhat disagree	69 (17.25%)	278 (21.47%)
Strongly disagree	56 (14%)	229 (17.68%)
Don't know / Refused	27 (6.75%)	99 (7.64%)

Question 7 — Please state whether... : And over the last two years do you think Seattle has gotten better, stayed the same, or gotten worse in terms of providing you with opportunities to get ahead economically?

	Phone Survey	Web Survey
Gotten better	171 (42.75%)	191 (14.75%)
Stayed the same	91 (22.75%)	429 (33.13%)
Gotten worse	108 (27%)	517 (39.92%)
Refused	3 (0.75%)	18 (1.39%)
Don't know	27 (6.75%)	140 (10.81%)

Question 8 — How often does your family have money left after paying your monthly bills?

	Phone Survey	Web Survey
Often	199 (49.75%)	503 (39.39%)
Sometimes	84 (21%)	245 (19.19%)
Occasionally	53 (13.25%)	297 (23.26%)
Never	56 (14%)	216 (16.91%)
Refused	8 (2%)	16 (1.25%)

Question 9 — How do you rate Seattle's housing affordability?

	Phone Survey	Web Survey
Very good	18 (4.5%)	8 (0.63%)
Good	46 (11.5%)	39 (3.06%)
Only fair	125 (31.25%)	246 (19.28%)
Poor	205 (51.25%)	962 (75.39%)
Refused	6 (1.5%)	21 (1.65%)

Question 10 — How likely is it that you will be able to afford to live in Seattle in five years?

	Phone Survey	Web Survey
Highly likely	164 (41%)	221 (17.29%)
Likely	101 (25.25%)	365 (28.56%)
Not very likely	71 (17.75%)	325 (25.43%)
Unlikely	55 (13.75%)	283 (22.14%)
Don't know / Refused	9 (2.25%)	84 (6.57%)

Question 11 — Have you or someone in your family moved out of Seattle in the past two years due to the rising cost of housing?

	Phone Survey	Web Survey
Yes	76 (19%)	498 (39.21%)
No	324 (81%)	680 (53.54%)
Refused	0 (0%)	92 (7.24%)

Question 12 — If you have moved in that last two years, which of the following describes your move? (Select all that apply)

	Phone Survey	Web Survey
Stayed in the same zip code	43 (10.75%)	148 (11.43%)
Moved out of Seattle	35 (8.75%)	113 (8.73%)
Moved into Seattle	18 (4.5%)	149 (11.51%)
Does not apply	304 (76%)	885 (68.34%)

Question 13 — And what were the main reasons you moved? (Select top two reasons)

	Phone Survey	Web Survey
New job or job transfer	12 (10.53%)	71
To be closer to work/school/other	5 (4.39%)	104
To establish own household	6 (5.26%)	53
Needed a larger house or apartment	4 (3.51%)	65
Married, widowed, divorced, or separated	5 (4.39%)	30
Other, family/personal related	4 (3.51%)	73
Wanted a better quality house or apartment	8 (7.02%)	94
Change from owner to renter OR renter to owner	1 (0.88%)	65
Wanted lower rent or less expensive house to maintain	21 (18.42%)	11
Evicted from residence	1 (0.88%)	11
Foreclosure	0 (0%)	2
Medical debt	1 (0.88%)	7
The property was being redeveloped	0 (0%)	28
Disaster loss (fire, flood, etc.)	0 (0%)	1
To be closer to cultural amenities and art	0 (0%)	40
Other	41 (35.96%)	91
Refused	5 (4.39%)	644
N	114	1541
Total Respondents	96	1130

Question 14 — What do you like most about where you live? (Please select your top two from the list)

	Phone Survey	Web Survey
Access to public transit	118 (19.44%)	581
Affordable rent/mortgage	22 (3.62%)	289
Near people who share my culture	71 (11.7%)	220
Easy to get to my job	58 (9.56%)	422
Quality of schools	32 (5.27%)	123
Safety	43 (7.08%)	231
Quality of apartment or house	51 (8.4%)	351
Access to art and culture	91 (14.99%)	301
Other	106 (17.46%)	278
None	15 (2.47%)	43
N	607	2779
Total Respondents	400	1276

Question 15 — How likely do you think it is that your cultural center, place of worship, or gathering place will be located in Seattle in five years?

	Phone Survey	Web Survey
Highly likely	193 (48.25%)	320 (24.71%)
Somewhat Likely	92 (23%)	313 (24.17%)
Not very likely	32 (8%)	187 (14.44%)
Unlikely	37 (9.25%)	141 (10.89%)
Don't know / Refused	46 (11.5%)	334 (25.79%)

Question 16 — Please state whether you strongly agree, somewhat agree, somewhat disagree, or strongly disagree with the following statements. The City of Seattle's public investments (transportation, utilities, etc) have created housing affordability problems in certain neighborhoods.

	Phone Survey	Web Survey
Strongly agree	153 (38.25%)	458 (35.37%)
Somewhat agree	118 (29.5%)	322 (24.86%)
Somewhat disagree	46 (11.5%)	144 (11.12%)
Strongly disagree	40 (10%)	105 (8.11%)
Don't know / Refused	43 (10.75%)	266 (20.54%)

Question 17 — Please state whether... : The City of Seattle is doing enough to ensure people can afford to stay living in Seattle.

	Phone Survey	Web Survey
Strongly agree	21 (5.25%)	38 (2.93%)
Somewhat agree	74 (18.5%)	90 (6.95%)
Somewhat disagree	104 (26%)	326 (25.17%)
Strongly disagree	180 (45%)	747 (57.68%)
Don't know / Refused	21 (5.25%)	94 (7.26%)

Question 18 — Please state whether... : I feel like I can rely on public transportation to get where I need to go in a reasonable amount of time.

	Phone Survey	Web Survey
Strongly agree	97 (24.25%)	142 (10.97%)
Somewhat agree	121 (30.25%)	508 (39.23%)
Somewhat disagree	63 (15.75%)	313 (24.17%)
Strongly disagree	96 (24%)	283 (21.85%)
Don't know / Refused	23 (5.75%)	49 (3.78%)

Question 19 — Please state whether... : How do you rate Seattle in terms of ability to get around by public transportation?

	Phone Survey	Web Survey
Very good	84 (21%)	113 (8.73%)
Good	116 (29%)	348 (26.87%)
Only fair	130 (32.5%)	517 (39.92%)
Poor	58 (14.5%)	275 (21.24%)
Refused	12 (3%)	42 (3.24%)

Question 20 — Please state whether... : And over the last two years, do you think Seattle has gotten better, stayed the same, or gotten worse in terms of access to public transportation?

	Phone Survey	Web Survey
Gotten better	137 (34.25%)	336 (25.95%)
Stayed the same	130 (32.5%)	444 (34.29%)
Gotten worse	121 (30.25%)	369 (28.49%)
Refused	12 (3%)	146 (11.27%)

Question 21 — Please state whether... : How do you rate Seattle in terms of your ability to access affordable health care?

	Phone Survey	Web Survey
Very good	111 (27.75%)	184 (14.21%)
Good	144 (36%)	462 (35.68%)
Fair	88 (22%)	328 (25.33%)
Poor	28 (7%)	129 (9.96%)
Don't know / Refused	29 (7.25%)	192 (14.83%)

Question 22 — And over the last two years, do you think Seattle has gotten better, stayed the same, or gotten worse in terms of access to affordable health care?

	Phone Survey	Web Survey
Gotten better	114 (28.5%)	191 (14.75%)
Stayed the same	172 (43%)	480 (37.07%)
Gotten worse	71 (17.75%)	175 (13.51%)
Refused	43 (10.75%)	449 (34.67%)

Question 23 — How do you rate Seattle's public schools?

	Phone Survey	Web Survey
Very good	33 (8.25%)	38 (2.93%)
Good	127 (31.75%)	265 (20.46%)
Fair	116 (29%)	316 (24.4%)
Poor	41 (10.25%)	184 (14.21%)
Don't know / Refused	83 (20.75%)	492 (37.99%)

Question 24 — And over the last two years, do you think Seattle has gotten better, stayed the same, or gotten worse in terms of public schools?

	Phone Survey	Web Survey
Gotten better	63 (15.75%)	72 (5.56%)
Stayed the same	178 (44.5%)	345 (26.64%)
Gotten worse	81 (20.25%)	247 (19.07%)
Refused	78 (19.5%)	631 (48.73%)

Question 25. Please state whether…: Shifting from punitive discipline measures in Seattle Public Schools to measures that address harm and repair relationships is important to making sure all students, regardless of their race, receive fair and just treatment.

	Phone Survey	WebSurvey
Strongly agree	183 (45.75%)	802 (61.93%)
Somewhat agree	127 (31.75%)	191 (14.75%)
Somewhat disagree	20 (5%)	47 (3.63%)
Strongly disagree	26 (6.5%)	33 (2.55%)
Don't know / Refused	44 (11%)	222 (17.14%)

Question 26 — Please state whether… : Staff and teachers at Seattle Public Schools treat students of color with as much respect as white students.

	Phone Survey	WebSurvey
Strongly agree	73 (18.25%)	83 (6.41%)
Somewhat agree	116 (29%)	133 (10.27%)
Somewhat disagree	58 (14.5%)	263 (20.31%)
Strongly disagree	30 (7.5%)	228 (17.61%)
Don't know / Refused	123 (30.75%)	588 (45.41%)

Question 27 — Please state whether… : Seattle Public Schools are preparing students well for the future.

	Phone Survey	WebSurvey
Strongly agree	38 (9.5%)	36 (2.78%)
Somewhat agree	169 (42.25%)	287 (22.16%)
Somewhat disagree	68 (17%)	274 (21.16%)
Strongly disagree	48 (12%)	154 (11.89%)
Don't know / Refused	77 (19.25%)	544 (42.01%)

Question 28 — How much confidence do you have in police officers in your community to do a good job of enforcing the law?

	Phone Survey	Web Survey
A great deal of confidence	99 (24.75%)	94 (7.26%)
A fair amount of confidence	213 (53.25%)	605 (46.72%)
No confidence	20 (5%)	116 (8.96%)
Refused	2 (0.5%)	89 (6.87%)

Question 29 — How much confidence do you have in police officers in your community to treat Black people and white people equally?

	Phone Survey	Web Survey
A great deal of confidence	55 (13.75%)	54 (4.17%)
A fair amount of confidence	177 (44.25%)	249 (19.23%)
Little confidence	110 (27.5%)	531 (41%)
No confidence	46 (11.5%)	324 (25.02%)
Refused	12 (3%)	137 (10.58%)

Question 30 — And what about people of color in general, how much confidence do you have in police officers in your community to treat people of color and white people equally?

	Phone Survey	Web Survey
A great deal of confidence	77 (19.25%)	50 (3.86%)
A fair amount of confidence	171 (42.75%)	267 (20.62%)
Little confidence	99 (24.75%)	543 (41.93%)
No confidence	37 (9.25%)	295 (22.78%)
Refused	16 (4%)	140 (10.81%)

Question 31 — How much confidence do you have in the courts treating people of color and white people equally?

	Phone Survey	Web Survey
A great deal of confidence	66 (16.5%)	59 (4.56%)
A fair amount of confidence	171 (42.75%)	239 (18.46%)
No confidence	39 (9.75%)	328 (25.33%)
Refused	18 (4.5%)	146 (11.27%)

Question 32 — Have you ever been questioned by the police, charged, or arrested when you had not committed a crime?

	Phone Survey	Web Survey
Yes	74 (18.5%)	270 (20.85%)
No	326 (81.5%)	993 (76.68%)
Refused	0 (0%)	32 (2.47%)

Question 33 — Have you or a family member ever experienced incarceration (jail, prison, juvenile detention)?

	Phone Survey	Web Survey
Myself	33 (8.25%)	69 (5.33%)
Family member	53 (13.25%)	327 (25.25%)
Both	—	46 (3.55%)
Neither	313 (78.25%)	821 (63.4%)
Refused	1 (0.25%)	32 (2.47%)

Question 34 — Which of the following should the City prioritize to reduce racial disproportionality in the criminal justice system? [Select top three]

	Phone Survey	Web Survey
Better schools and after school programs	233 (22.47%)	577
Ending out of school suspensions and expulsions	94 (9.06%)	356
Requiring anti-bias training for police and courts	171 (16.49%)	610
Family wage jobs	110 (10.61%)	429
Better mental health services	114 (10.99%)	450
More affordable housing	71 (6.85%)	472
More parks and community centers	36 (3.47%)	127
Community-based alternatives to arrest and detention	70 (6.75%)	597
Restorative justice	30 (2.89%)	394
More police of color	72 (6.94%)	270
Other	13 (1.25%)	67
Don't know	23 (2.22%)	45
N	1037	4411
Total Respondents	400	1274

Question 35 — In the last 12 months, did you or a member of your immediate household experience discrimination, were refused services or treated unfairly because of: [Select all that apply]

	Phone Survey	Web Survey
Race or Color	32 (13.39%)	236 (19.81%)
Disability	21 (8.79%)	86 (7.22%)
Sexual orientation	10 (4.18%)	70 (5.88%)
National origin	10 (4.18%)	40 (3.36%)
Religion	15 (6.28%)	35 (2.94%)
Gender	19 (7.95%)	192 (16.12%)
Gender Identity	6 (2.51%)	64 (5.37%)
Marital status	12 (5.02%)	35 (2.94%)
Because children live in your household	11 (4.6%)	34 (0.03%)
Age	52 (21.76%)	145 (12.17%)
Veteran or military status	5 (2.09%)	11 (.01%)
A prior juvenile or criminal record	8 (3.35%)	32 (2.85%)
Credit history	20 (8.37%)	110 (9.2%)
Use of a Section 8 Housing Voucher	4 (1.67%)	11 (0.92%)
Breastfeeding in a public place	6 (2.51%)	14 (1.18%)
Other reason	8 (3.35%)	73 (6.13%)
N	239	1191
Total Respondents	113	528

Question 36 — If you said "Yes" to at least one item in the previous question, please check the box for each area that you or a member of your immediate household experienced discrimination or unfair treatment with: [Select all that apply]

	Phone Survey	Web Survey
Employment	36 (18%)	192 (18.32%)
Rental housing	18 (9%)	105 (10.02%)
Home ownership	3 (1.5%)	41 (3.91%)
Utility services	9 (4.5%)	25 (2.39%)
Law enforcement and policing	24 (12%)	110 (10.50%)
Consumer, financial services and credit	23 (11.5%)	106 (10.11%)
Health care	14 (7%)	108 (10.31%)
Access to governmental assistance, programs or services	10 (5%)	83 (7.92%)
Education	17 (8.5%)	86 (8.21%)
Private business	22 (11%)	147 (14.03%)
None	24 (12%)	46 (4.39%)
N	200	1048
Total Respondents	113	527

Question 37 — The City of Seattle conducts outreach and engagement on many projects and policies. Are you aware of such outreach, or is this your first time hearing about it?

	Phone Survey	Web Survey
Aware	195 (48.75%)	667 (51.51%)
First time hearing about it	202 (50.5%)	595 (45.95%)
Refused	3 (0.75%)	33 (2.55%)

Question 38 — Have you participated?

	Phone Survey	Web Survey
Yes	69 (35.38%)	342 (26.41%)
No	126 (64.62%)	907 (70.04%)
N	195	1249

Question 39 — If you participated, did you feel your participation was valued?

	Phone Survey	Web Survey
A great deal	13 (18.84%)	38 (2.93%)
A fair amount	24 (34.78%)	85 (6.56%)
Just some	17 (24.64%)	137 (10.58%)
Very little	5 (7.25%)	80 (6.18%)
None	7 (10.14%)	26 (2.01%)
Refused	3 (4.35%)	929 (71.74%)
N	69	1295

Question 40 — How would you rate race relations in Seattle?

	Phone Survey	Web Survey
Very good	42 (10.5%)	28 (2.16%)
Good	143 (35.75%)	234 (18.07%)
Only fair	175 (43.75%)	665 (51.35%)
Poor	31 (7.75%)	290 (22.39%)
Refused	9 (2.25%)	78 (6.02%)

Question 41 — And over the last two years, do you think Seattle has gotten better, stayed the same, or gotten worse in terms of race relations?

	Phone Survey	Web Survey
Gotten better	101 (25.25%)	161 (12.43%)
Stayed the same	212 (53%)	714 (55.14%)
Gotten worse	70 (17.5%)	360 (27.8%)
Refused	17 (4.25%)	60 (4.63%)

Question 42 — How high of a priority should it be for government to address the racial equity gaps in education, criminal justice, jobs, health, housing and other areas?

	Phone Survey	Web Survey
High priority	254 (63.5%)	989 (76.37%)
Somewhat of a priority	117 (29.25%)	196 (15.14%)
Not a priority	20 (5%)	45 (3.47%)
Refused	9 (2.25%)	65 (5.02%)

Question 43 — Please state whether... : To create equity and opportunity for all, I believe a greater portion of resources should go to those who are most in need.

	Phone Survey	Web Survey
Strongly agree	215 (53.75%)	813 (62.78%)
Somewhat agree	133 (33.25%)	329 (25.41%)
Somewhat disagree	27 (6.75%)	51 (3.94%)
Strongly disagree	17 (4.25%)	32 (2.47%)
Don't know / Refused	8 (2%)	70 (5.41%)

Question 44 — Please state whether... : In Seattle we are making progress in eliminating racial inequities and creating a city where social, economic and political opportunities and outcomes are not predicted based upon a person's race.

	Phone Survey	Web Survey
Strongly agree	78 (19.5%)	83 (6.41%)
Somewhat agree	211 (52.75%)	470 (36.29%)
Somewhat disagree	62 (15.5%)	353 (27.26%)
Strongly disagree	32 (8%)	200 (15.44%)
Don't know / Refused	17 (4.25%)	189 (14.59%)

Question 45 — Please state whether... : Compared with five years ago, do you think there is a wider gap or a narrower gap between African American residents and White residents in terms of average incomes?

	Phone Survey	Web Survey
Wider gap	180 (45%)	693 (53.51%)
Narrower gap	71 (17.75%)	87 (6.72%)
About the same	67 (16.75%)	169 (13.05%)
Don't know / Refused	82 (20.5%)	346 (26.72%)

Question 46 — Which of the following have you done over the last year? (select all that apply)

	Phone Survey	Web Survey
Voted in an election	348 (25.4%)	1113
Signed a petition	252 (18.39%)	949
Organized neighbors or community members on an issue	83 (6.06%)	353
Joined a community organization or faith-based group to g...	137 (10%)	506
Written or spoken to a local elected official	179 (13.07%)	621
Attended a protest, march or demonstration	85 (6.2%)	502
Given money or volunteered time to support a community or...	266 (19.42%)	978
None of the above	20 (1.46%)	49
N	1370	5071
Total Respondents	400	1260

Question 47 — What do you think is the most important problem facing your community today?

	Phone Survey
Crime	32 (8%)
Development Impacts	19 (4.75%)
Education	23 (5.75%)
Employment	1 (0.25%)
Environment	8 (2%)
Healthcare	3 (0.75%)
Homelessness	30 (7.5%)
Housing	72 (18%)
Inequality	66 (16.5%)
Neighborhood Quality	2 (0.5%)
None	15 (3.75%)
Other	81 (20.25%)
Police brutality	1 (0.25%)
Traffic / Infrastructure	47 (11.75%)

Question 48 — What is your gender?

	Phone Survey	Web Survey
Female	223 (55.75%)	854 (65.95%)
Male	174 (43.5%)	330 (25.48%)
Transgender	0 (0%)	5 (0.39%)
Genderqueer/Gender non-conforming	0 (0%)	29 (2.24%)
Other (SPECIFY)	1 (0.25%)	26 (2.01%)
Refused	2 (0.5%)	51 (3.94%)

Question 49 — How do you identify yourself by race or ethnicity?

	Phone Survey	Web Survey
American Indian / Alaska Native	3 (0.75%)	36 (2.78%)
Asian American	24 (6%)	83 (6.41%)
Pacific Islander	5 (1.25%)	3 (0.23%)
Black / African American	33 (8.25%)	93 (7.18%)
Hispanic / Latino	11 (2.75%)	63 (4.86%)
Middle Eastern	2 (0.5%)	1 (0.08%)
White, non-Hispanic	273 (68.25%)	772 (59.61%)
Multiracial	26 (6.5%)	131 (10.12%)
Other (SPECIFY)	10 (2.5%)	55 (4.25%)
Refused	13 (3.25%)	58 (4.48%)

Question 50 — Were you born in the United States or another country?

	Phone Survey	Web Survey
United States	351 (87.75%)	1121 (86.56%)
Another country	43 (10.75%)	119 (9.19%)
Refused	6 (1.5%)	55 (4.25%)

If responding another country:

	Phone Survey
Africa	1 (2.22%)
Argentina	1 (2.22%)
Australia	1 (2.22%)
Austria	1 (2.22%)
Barbados	1 (2.22%)
Canada	6 (13.33%)
China	1 (2.22%)
Cuba	1 (2.22%)
England	2 (4.44%)
Germany	6 (13.33%)
Great Britain	1 (2.22%)
Hong Kong	1 (2.22%)
Indonesia	1 (2.22%)
Japan	3 (6.67%)
Limerick, Ireland	1 (2.22%)
Mexico	1 (2.22%)
Netherlands	1 (2.22%)
Nigeria	1 (2.22%)
None of my business.	1 (2.22%)
Norway	1 (2.22%)
Panama	2 (4.44%)
Philippines	1 (2.22%)
Refused	1 (2.22%)
Scandinavian	1 (2.22%)
Seoul, South Korea	1 (2.22%)
Sweden	1 (2.22%)
Swiss	1 (2.22%)
The Netherlands	1 (2.22%)
UK	1 (2.22%)
United Kingdom	2 (4.44%)
N	45

Question 51 — Were your parents born in the United States or in another country?

	Phone Survey	Web Survey
Both parents born in the United States	281 (70.25%)	924 (71.35%)
Both parents born in another country	73 (18.25%)	190 (14.67%)
1 parent born in the US, 1 born in another country	39 (9.75%)	124 (9.58%)
Refused	7 (1.75%)	57 (4.4%)

Question 52 — What is your sexual orientation?

	Phone Survey	Web Survey
Straight	327 (81.75%)	926 (71.51%)
Lesbian	10 (2.5%)	33 (2.55%)
Gay	11 (2.75%)	36 (2.78%)
Bisexual	7 (1.75%)	87 (6.72%)
Queer	1 (0.25%)	74 (5.71%)
Other	17 (4.25%)	62 (4.79%)
Refused	27 (6.75%)	77 (5.95%)

Question 53 — Are you a person with a disability?

	Phone Survey	Web Survey
Yes	75 (18.75%)	152 (11.74%)
No	318 (79.5%)	1083 (83.63%)
Refused	7 (1.75%)	60 (4.63%)

Question 54 — What is your housing situation?

	Phone Survey	Web Survey
Own	274 (68.5%)	585 (45.17%)
Rent	98 (24.5%)	556 (42.93%)
Transitional housing	0 (0%)	3 (0.23%)
Homeless / shelter	0 (0%)	21 (1.62%)
Live with someone	12 (3%)	49 (3.78%)
Other	8 (2%)	26 (2.01%)
Refused	8 (2%)	55 (4.25%)

Question 55 — How many people live in your household?

	Phone Survey	Web Survey
1	127 (31.75%)	243 (18.76%)
2	136 (34%)	496 (38.3%)
3	50 (12.5%)	239 (18.46%)
4	45 (11.25%)	174 (13.44%)
5 or more	29 (7.25%)	83 (6.41%)
Refused	13 (3.25%)	60 (4.63%)

Question 56 — How many children under the age of 18 live in your household?

	Phone Survey	Web Survey
0	164 (63.08%)	893 (68.96%)
1	49 (18.85%)	173 (13.36%)
2	37 (14.23%)	123 (9.5%)
3	8 (3.08%)	30 (2.32%)
4	1 (0.38%)	5 (0.39%)
5 or more	0 (0%)	2 (0.15%)
Refused	1 (0.38%)	69 (5.33%)

Question 57 — What is your zip code?

	Phone Survey
98004	1 (0.25%)
98018	1 (0.25%)
98026	1 (0.25%)
98031	2 (0.5%)
98038	1 (0.25%)
98055	1 (0.25%)
98057	1 (0.25%)
98077	1 (0.25%)
98101	7 (1.75%)
98102	10 (2.5%)
98103	23 (5.75%)
98104	3 (0.75%)
98105	16 (4%)
98106	8 (2%)
98107	12 (3%)
98108	5 (1.25%)
98109	8 (2%)
98112	9 (2.25%)
98114	1 (0.25%)
98115	36 (9%)
98116	16 (4%)
98117	11 (2.75%)
98118	23 (5.75%)
98119	17 (4.25%)
98121	2 (0.5%)
98122	15 (3.75%)
98125	32 (8%)
98126	16 (4%)
98133	13 (3.25%)
98136	16 (4%)
98139	1 (0.25%)
98144	18 (4.5%)
98145	1 (0.25%)
98146	7 (1.75%)
98148	1 (0.25%)
98155	6 (1.5%)
98166	2 (0.5%)
98168	7 (1.75%)
98177	4 (1%)
98178	15 (3.75%)
98188	2 (0.5%)
98199	11 (2.75%)
98223	1 (0.25%)
98275	1 (0.25%)
99999	15 (3.75%)

Question 58 — Is your age between:

	Phone Survey	Web Survey
15 and 25	15 (3.75%)	85 (6.56%)
26 and 35	24 (6%)	370 (28.57%)
36 and 50	72 (18%)	395 (30.50%)
51 and 64	140 (35%)	243 (18.76%)
65 year of age or older	143 (35.75%)	141 (10.88%)
Refused	6 (1.5%)	61 (4.71%)

Question 59 — What is the highest level of education you have completed?

	Phone Survey	Web Survey
Grade school or some high school	7 (1.75%)	29 (2.24%)
High school graduate	33 (8.25%)	26 (2.01%)
Some college, technical, vocational or two year degree	95 (23.75%)	212 (16.37%)
Four year college graduate	116 (29%)	380 (29.34%)
Post graduate work or graduate degree	141 (35.25%)	589 (45.48%)
Refused	8 (2%)	59 (4.56%)

Question 60 — How long have you lived, worked or gone to school in Seattle?

	Phone Survey	Web Survey
One year or less	15 (3.75%)	63 (4.86%)
1 to 2 years	—	71 (5.48%)
2 to 5 years	25 (6.25%)	164 (12.66%)
5 to 10 years	23 (5.75%)	187 (14.44%)
10 years or more	328 (82%)	756 (58.38%)
Refused	9 (2.25%)	54 (4.17%)

Question 61 — What is your current employment status?

	Phone Survey	Web Survey
Employed full time	150 (37.5%)	642 (49.58%)
Employed part time	32 (8%)	133 (10.27%)
Self employed	36 (9%)	90 (6.95%)
Currently unemployed	38 (9.5%)	63 (4.86%)
Student	3 (0.75%)	63 (4.86%)
Other	132 (33%)	249 (19.23%)
Refused	9 (2.25%)	55 (4.25%)

Question 62 — When it comes to politics, do you usually think of yourself as a Liberal, a Conservative, a Moderate, or have you not thought about it much?

	Phone Survey	Web Survey
Liberal	207 (51.75%)	808 (62.39%)
Conservative	42 (10.5%)	25 (1.93%)
Moderate	60 (15%)	158 (12.2%)
Haven't thought about it much	47 (11.75%)	65 (5.02%)
Other (SPECIFY)	29 (7.25%)	171 (13.2%)
Refused	15 (3.75%)	68 (5.25%)

Table 9: If responding other to Q62:

	Phone Survey
Always vote for the best candidate and independently.	1 (3.33%)
Democrat	3 (10%)
Democratic Socialist	1 (3.33%)
I don't agree with politics at all.	1 (3.33%)
In between conservative and liberal.	1 (3.33%)
Independent	14 (46.67%)
Liberal and moderate.	1 (3.33%)
Liberal in the classical sense, as in liberal education.	1 (3.33%)
Progressive	4 (13.33%)
Radical	1 (3.33%)
Socialist Party	1 (3.33%)
Sometimes depends on candidate or election, won't lump myself in one.	1 (3.33%)
N	30

	Phone Survey	Web Survey
Less than $20,000	38 (9.5%)	141 (10.89%)
$20,000 to less than $40,000	46 (11.5%)	149 (11.51%)
$40,000 to less than $60,000	43 (10.75%)	198 (15.29%)
$60,000 to less than $75,000	37 (9.25%)	151 (11.66%)
$75,000 to less than $100,000	54 (13.5%)	157 (12.12%)
$100,000 to less than $150,000	43 (10.75%)	219 (16.91%)
$150,000 to less than $200,000	19 (4.75%)	97 (7.49%)
$200,000 or above	38 (9.5%)	77 (5.95%)
Refused	82 (20.5%)	106 (8.19%)

Question 64 — If you live in Seattle, what is your City Council district?

	Phone Survey	Web Survey
District 1	24 (6%)	82 (6.82%)
District 2	5 (1.25%)	97 (8.06%)
District 3	15 (3.75%)	141 (11.72%)
District 4	13 (3.25%)	71 (5.9%)
District 5	13 (3.25%)	53 (4.41%)
District 6	10 (2.5%)	94 (7.81%)
District 7	20 (5%)	64 (5.32%)
Don't know	278 (69.5%)	470 (39.07%)
Does not apply / Don't live in Seattle	22 (5.5%)	131 (10.89%)

Chapter Listing

Chapter 10.97 RCW

WASHINGTON STATE CRIMINAL RECORDS PRIVACY ACT

Sections

10.97.010	Declaration of policy.
10.97.020	Short title.
10.97.030	Definitions.
10.97.040	Information required—Exceptions.
10.97.045	Disposition data to initiating agency and state patrol.
10.97.050	Restricted, unrestricted information—Records.
10.97.060	Deletion of certain information, conditions.
10.97.070	Disclosure of suspect's identity to victim.
10.97.080	Inspection of information by subject—Challenges and corrections.
10.97.090	Administration by state patrol.
10.97.100	Fees.
10.97.110	Civil remedies—Criminal prosecution not affected.
10.97.120	Criminal penalties—Civil action not affected.
10.97.130	Child victims of sexual assaults, identification confidential.
10.97.140	Construction.

NOTES:

*Public records: Chapter **42.56** RCW.*

*Records of community sexual assault program and underserved populations provider not available as part of discovery: RCW **70.125.065**.*

10.97.010
Declaration of policy.

The legislature declares that it is the policy of the state of Washington to provide for the completeness, accuracy, confidentiality, and security of criminal history record information and victim, witness, and complainant record information as defined in this chapter.

[1977 ex.s. c 314 § 1.]

10.97.020
Short title.

This chapter may be cited as the Washington State Criminal Records Privacy Act.

[1977 ex.s. c 314 § 2.]

NOTES:

Reviser's note: The phrase "This 1977 amendatory act" has been changed to "This chapter." This 1977 amendatory act [1977 ex.s. c 314] consists of chapter **10.97** RCW and the amendments of RCW **42.17.310**, **43.43.705**, **43.43.710**, **43.43.730**, and **43.43.810**.

10.97.030
Definitions.

For purposes of this chapter, the definitions of terms in this section shall apply.

(1) "The administration of criminal justice" means performance of any of the following activities: Detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The term also includes criminal identification activities and the collection, storage, dissemination of criminal history record information, and the compensation of victims of crime.

(2) "Conviction or other disposition adverse to the subject" means any disposition of charges other than: (a) A decision not to prosecute; (b) a dismissal; or (c) acquittal; with the following exceptions, which shall be considered dispositions adverse to the subject: An acquittal due to a finding of not guilty by reason of insanity and a dismissal by reason of incompetency, pursuant to chapter **10.77** RCW; and a dismissal entered after a period of probation, suspension, or deferral of sentence.

(3) "Conviction record" means criminal history record information relating to an incident which has led to a conviction or other disposition adverse to the subject.

(4) "Criminal history record information" means information contained in records collected by criminal justice agencies, other than courts, on individuals, consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, including acquittals by reason of insanity, dismissals based on lack of competency, sentences, correctional supervision, and release.

The term includes any issued certificates of restoration of opportunities and any information contained in records maintained by or obtained from criminal justice agencies, other than courts, which records provide individual identification of a person together with any portion of the individual's record of involvement in the criminal justice system as an alleged or convicted offender, except:

(a) Posters, announcements, or lists for identifying or apprehending fugitives or wanted persons;

(b) Original records of entry maintained by criminal justice agencies to the extent that such records are compiled and maintained chronologically and are accessible only on a chronological basis;

(c) Court indices and records of public judicial proceedings, court decisions, and opinions, and information disclosed during public judicial proceedings;

(d) Records of traffic violations which are not punishable by a maximum term of imprisonment of more than ninety days;

(e) Records of any traffic offenses as maintained by the department of licensing for the purpose of regulating the issuance, suspension, revocation, or renewal of drivers' or other operators' licenses and pursuant to RCW **46.52.130**;

(f) Records of any aviation violations or offenses as maintained by the department of transportation for the purpose of regulating pilots or other aviation operators, and pursuant to RCW **47.68.330**;

(g) Announcements of executive clemency;

(h) Intelligence, analytical, or investigative reports and files.

(5) "Criminal justice agency" means: (a) A court; or (b) a government agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice.

(6) "Disposition" means the formal conclusion of a criminal proceeding at whatever stage it occurs in the criminal justice system.

(7) "Dissemination" means disclosing criminal history record information or disclosing the absence of criminal history record information to any person or agency outside the agency possessing the information, subject to the following exceptions:

(a) When criminal justice agencies jointly participate in the maintenance of a single recordkeeping department as an alternative to maintaining separate records, the furnishing of information by that department to personnel of any participating agency is not a dissemination;

(b) The furnishing of information by any criminal justice agency to another for the purpose of processing a matter through the criminal justice system, such as a police department providing information to a prosecutor for use in preparing a charge, is not a dissemination;

(c) The reporting of an event to a recordkeeping agency for the purpose of maintaining the record is not a dissemination.

(8) "Nonconviction data" consists of all criminal history record information relating to an incident which has not led to a conviction or other disposition adverse to the subject, and for which proceedings are no longer actively pending. There shall be a rebuttable presumption that proceedings are no longer actively pending if more than one year has elapsed since arrest, citation, charge, or service of warrant and no disposition has been entered.

[2016 c 81 § 4; 2012 c 125 § 1; 1999 c 49 § 1; 1998 c 297 § 49; 1990 c 3 § 128; 1979 ex.s. c 36 § 1; 1979 c 158 § 5; 1977 ex.s. c 314 § 3.]

NOTES:

Reviser's note: The definitions in this section have been alphabetized pursuant to RCW **1.08.015**(2)(k).

Finding—Conflict with federal requirements—2016 c 81: See notes following RCW 9.97.010.

Effective dates—Severability—Intent—1998 c 297: See notes following RCW 71.05.010.

Index, part headings not law—Severability—Effective dates—Application—1990 c 3: See RCW 18.155.900 through 18.155.902.

10.97.040
Information required—Exceptions.

No criminal justice agency shall disseminate criminal history record information pertaining to an arrest, detention, indictment, information, or other formal criminal charge made after December 31, 1977, unless the record disseminated states the disposition of such charge to the extent dispositions have been made at the time of the request for the information: PROVIDED, HOWEVER, That if a disposition occurring within ten days immediately preceding the dissemination has not been reported to the agency disseminating the criminal history record information, or if information has been received by the agency within the seventy-two hours immediately preceding the dissemination, that information shall not be required to be included in the dissemination: PROVIDED FURTHER, That when another criminal justice agency requests criminal history record information, the disseminating agency may disseminate specific facts and incidents which are within its direct knowledge without furnishing disposition data as otherwise required by this section, unless the disseminating agency has received such disposition data from either: (1) the state patrol, or (2) the court or other criminal justice agency required to furnish disposition data pursuant to RCW 10.97.045.

No criminal justice agency shall disseminate criminal history record information which shall include information concerning a felony or gross misdemeanor without first making inquiry of the identification section of the Washington state patrol for the purpose of obtaining the most current and complete information available, unless one or more of the following circumstances exists:

(1) The information to be disseminated is needed for a purpose in the administration of criminal justice for which time is of the essence and the identification section is technically or physically incapable of responding within the required time;

(2) The full information requested and to be disseminated relates to specific facts or incidents which are within the direct knowledge of the agency which disseminates the information;

(3) The full information requested and to be disseminated is contained in a criminal history record information summary received from the identification section by the agency which is to make the dissemination not more than thirty days preceding the dissemination to be made;

(4) The statute, executive order, court rule, or court order pursuant to which the information is to be disseminated refers solely to information in the files of the agency which makes the dissemination;

(5) The information requested and to be disseminated is for the express purpose of research, evaluative, or statistical activities to be based upon information maintained in the files of the agency or agencies from which the information is directly sought; or

(6) A person who is the subject of the record requests the information and the agency complies with the requirements in RCW 10.97.080 as now or hereafter amended.

[1979 ex.s. c 36 § 2; 1977 ex.s. c 314 § 4.]

10.97.045
Disposition data to initiating agency and state patrol.

Whenever a court or other criminal justice agency reaches a disposition of a criminal proceeding, the court or other criminal justice agency shall furnish the disposition data to the agency initiating the criminal history record for that charge and to the identification section of the Washington state patrol as required under RCW 43.43.745.

[1979 ex.s. c 36 § 6.]

10.97.050
Restricted, unrestricted information—Records.

(1) Conviction records may be disseminated without restriction.

(2) Any criminal history record information which pertains to an incident that occurred within the last twelve months for which a person is currently being processed by the criminal justice system, including the entire period of correctional supervision extending through final discharge from parole, when applicable, may be disseminated without restriction.

(3) Criminal history record information which includes nonconviction data may be disseminated by a criminal justice agency to another criminal justice agency for any purpose associated with the administration of criminal justice, or in connection with the employment of the subject of the record by a criminal justice or juvenile justice agency. A criminal justice agency may respond to any inquiry from another criminal justice agency without any obligation to ascertain the purpose for which the information is to be used by the agency making the inquiry.

(4) Criminal history record information which includes nonconviction data may be disseminated by a criminal justice agency to implement a statute, ordinance, executive order, or a court rule, decision, or order which expressly refers to records of arrest, charges, or allegations of criminal conduct or other nonconviction data and authorizes or directs that it be available or accessible for a specific purpose.

(5) Criminal history record information which includes nonconviction data may be disseminated to individuals and agencies pursuant to a contract with a criminal justice agency to provide services related to the administration of criminal justice. Such contract must specifically authorize access to criminal history record information, but need not specifically state that access to nonconviction data is included. The agreement must limit the use of the criminal history record information to stated purposes and insure the confidentiality and

security of the information consistent with state law and any applicable federal statutes and regulations.

(6) Criminal history record information which includes nonconviction data may be disseminated to individuals and agencies for the express purpose of research, evaluative, or statistical activities pursuant to an agreement with a criminal justice agency. Such agreement must authorize the access to nonconviction data, limit the use of that information which identifies specific individuals to research, evaluative, or statistical purposes, and contain provisions giving notice to the person or organization to which the records are disseminated that the use of information obtained therefrom and further dissemination of such information are subject to the provisions of this chapter and applicable federal statutes and regulations, which shall be cited with express reference to the penalties provided for a violation thereof.

(7) Every criminal justice agency that maintains and disseminates criminal history record information must maintain information pertaining to every dissemination of criminal history record information except a dissemination to the effect that the agency has no record concerning an individual. Information pertaining to disseminations shall include:

(a) An indication of to whom (agency or person) criminal history record information was disseminated;

(b) The date on which the information was disseminated;

(c) The individual to whom the information relates; and

(d) A brief description of the information disseminated.

The information pertaining to dissemination required to be maintained shall be retained for a period of not less than one year.

(8) In addition to the other provisions in this section allowing dissemination of criminal history record information, RCW **4.24.550** governs dissemination of information concerning offenders who commit sex offenses as defined by RCW **9.94A.030**. Criminal justice agencies, their employees, and officials shall be immune from civil liability for dissemination on criminal history record information concerning sex offenders as provided in RCW **4.24.550**.

[2012 c 125 § 2; 2005 c 421 § 9; 1990 c 3 § 129; 1977 ex.s. c 314 § 5.]

NOTES:

Index, part headings not law—Severability—Effective dates—Application—1990 c 3: See RCW **18.155.900** through **18.155.902**.

10.97.060
Deletion of certain information, conditions.

Criminal history record information which consists of nonconviction data only shall be subject to deletion from criminal justice agency files which are available and generally searched for the purpose of responding to inquiries concerning the criminal history of a named or otherwise identified individual when two years or longer have elapsed since the record became nonconviction data as a result of the entry of a disposition favorable to the defendant, or upon the passage of three years from the date of arrest or issuance of a citation or warrant

for an offense for which a conviction was not obtained unless the defendant is a fugitive, or the case is under active prosecution according to a current certification made by the prosecuting attorney.

Such criminal history record information consisting of nonconviction data shall be deleted upon the request of the person who is the subject of the record: PROVIDED, HOWEVER, That the criminal justice agency maintaining the data may, at its option, refuse to make the deletion if:

(1) The disposition was a deferred prosecution or similar diversion of the alleged offender;

(2) The person who is the subject of the record has had a prior conviction for a felony or gross misdemeanor;

(3) The individual who is the subject of the record has been arrested for or charged with another crime during the intervening period.

Nothing in this chapter is intended to restrict the authority of any court, through appropriate judicial proceedings, to order the modification or deletion of a record in a particular cause or concerning a particular individual or event.

[1977 ex.s. c 314 § 6.]

10.97.070
Disclosure of suspect's identity to victim.

(1) Criminal justice agencies may, in their discretion, disclose to persons who have suffered physical loss, property damage, or injury compensable through civil action, the identity of persons suspected as being responsible for such loss, damage, or injury together with such information as the agency reasonably believes may be of assistance to the victim in obtaining civil redress. Such disclosure may be made without regard to whether the suspected offender is an adult or a juvenile, whether charges have or have not been filed, or a prosecuting authority has declined to file a charge or a charge has been dismissed.

(2) Unless the agency determines release would interfere with an ongoing criminal investigation, in any action brought pursuant to this chapter, criminal justice agencies shall disclose identifying information, including photographs of suspects, if the acts are alleged by the plaintiff or victim to be a violation of RCW 9A.50.020.

(3) The disclosure by a criminal justice agency of investigative information pursuant to subsection (1) of this section shall not establish a duty to disclose any additional information concerning the same incident or make any subsequent disclosure of investigative information, except to the extent an additional disclosure is compelled by legal process.

[1993 c 128 § 10; 1977 ex.s. c 314 § 7.]

NOTES:

Effective date—1993 c 128: See RCW 9A.50.902.

10.97.080
Inspection of information by subject—Challenges and corrections.

All criminal justice agencies shall permit an individual who is, or who believes that he or she may be, the subject of a criminal record maintained by that agency, to appear in person during normal business hours of that criminal justice agency and request to see the criminal history record information held by that agency pertaining to the individual. The individual's right to access and review of criminal history record information shall not extend to data contained in intelligence, investigative, or other related files, and shall not be construed to include any information other than that defined as criminal history record information by this chapter.

Every criminal justice agency shall adopt rules and make available forms to facilitate the inspection and review of criminal history record information by the subjects thereof, which rules may include requirements for identification, the establishment of reasonable periods of time to be allowed an individual to examine the record, and for assistance by an individual's counsel, interpreter, or other appropriate persons.

No person shall be allowed to retain or mechanically reproduce any nonconviction data except for the person who is the subject of the record. Such person may retain a copy of their personal nonconviction data information on file, if the criminal justice agency has verified the identities of those who seek to inspect them. Criminal justice agencies may impose such additional restrictions, including fingerprinting, as are reasonably necessary both to assure the record's security and to verify the identities of those who seek to inspect them. The criminal justice agency may charge a reasonable fee for fingerprinting or providing a copy of the personal nonconviction data information pursuant to this section. The provisions of chapter 42.56 RCW shall not be construed to require or authorize copying of nonconviction data for any other purpose.

The Washington state patrol shall establish rules for the challenge of records which an individual declares to be inaccurate or incomplete, and for the resolution of any disputes between individuals and criminal justice agencies pertaining to the accuracy and completeness of criminal history record information. The Washington state patrol shall also adopt rules for the correction of criminal history record information and the dissemination of corrected information to agencies and persons to whom inaccurate or incomplete information was previously disseminated. Such rules may establish time limitations of not less than ninety days upon the requirement for disseminating corrected information.

[2012 c 125 § 3; 2010 c 8 § 1093; 2005 c 274 § 206; 1979 ex.s. c 36 § 3; 1977 ex.s. c 314 § 8.]

10.97.090
Administration by state patrol.

The Washington state patrol is hereby designated the agency of state government responsible for the administration of the 1977 Washington State Criminal Records Privacy Act.

The Washington state patrol may adopt any rules and regulations necessary for the performance of the administrative functions provided for in this chapter.

The Washington state patrol shall have the following specific administrative duties:

(1) To establish by rule and regulation standards for the security of criminal history information systems in order that such systems and the data contained therein be adequately protected from fire, theft, loss, destruction, other physical hazard, or unauthorized access;

(2) To establish by rule and regulation standards for personnel employed by criminal justice of other state and local government agencies in positions with responsibility for maintenance and dissemination of criminal history record information; and

(3) To contract with the Washington state auditor or other public or private agency, organization, or individual to perform audits of criminal history record information systems.

[1979 ex.s. c 36 § 4; 1977 ex.s. c 314 § 9.]

10.97.100
Fees.

Criminal justice agencies shall be authorized to establish and collect reasonable fees for the dissemination of criminal history record information to agencies and persons other than criminal justice agencies.

[1977 ex.s. c 314 § 10.]

10.97.110
Civil remedies—Criminal prosecution not affected.

Any person may maintain an action to enjoin a continuance of any act or acts in violation of any of the provisions of this chapter, and if injured thereby, for the recovery of damages and for the recovery of reasonable attorneys' fees. If, in such action, the court shall find that the defendant is violating or has violated any of the provisions of this chapter, it shall enjoin the defendant from a continuance thereof, and it shall not be necessary that actual damages to the plaintiff be alleged or proved. In addition to such injunctive relief, the plaintiff in said action shall be entitled to recover from the defendant the amount of the actual damages, if any, sustained by him or her if actual damages to the plaintiff are alleged and proved. In any suit brought to enjoin a violation of this chapter, the prevailing party may be awarded reasonable attorneys' fees, including fees incurred upon appeal. Commencement, pendency, or conclusion of a civil action for injunction or damages shall not affect the liability of a person or agency to criminal prosecution for a violation of this chapter.

[2010 c 8 § 1094; 1979 ex.s. c 36 § 5; 1977 ex.s. c 314 § 11.]

10.97.120
Criminal penalties—Civil action not affected.

Violation of the provisions of this chapter shall constitute a misdemeanor, and any person whether as principal, agent, officer, or director for himself or herself or for another person, or for any firm or corporation, public or private, or any municipality who or which shall violate any of the provisions of this chapter shall be guilty of a misdemeanor for each single violation. Any criminal prosecution shall not affect the right of any person to bring a civil action as authorized by this chapter or otherwise authorized by law.

[2010 c 8 § 1095; 1977 ex.s. c 314 § 12.]

10.97.130
Child victims of sexual assaults, identification confidential.

Information identifying child victims under age eighteen who are victims of sexual assaults is confidential and not subject to release to the press or public without the permission of the child victim or the child's legal guardian. Identifying information includes the child victim's name, addresses, location, photographs, and in cases in which the child victim is a relative or stepchild of the alleged perpetrator, identification of the relationship between the child and the alleged perpetrator. Information identifying the child victim of sexual assault may be released to law enforcement, prosecutors, judges, defense attorneys, or private or governmental agencies that provide services to the child victim of sexual assault. Prior to release of any criminal history record information, the releasing agency shall delete any information identifying a child victim of sexual assault from the information except as provided in this section.

[1992 c 188 § 8.]

NOTES:

Findings—Intent—Severability—1992 c 188: See notes following RCW 7.69A.020.

10.97.140
Construction.

Nothing in RCW 40.14.060 or 40.14.070 or chapter 42.56 RCW precludes dissemination of criminal history record information, including nonconviction data, for the purposes of this chapter.

[2005 c 274 § 207; 1999 c 326 § 4.]

Chapter 11.35 - IMMOBILIZATION

Sections:

11.35.010 - Scofflaw list

A. When there are four or more parking citations issued against a vehicle for each of which a person has failed to respond, failed to appear at a requested hearing, or failed to pay amounts due for at least 45 days from the date of the filing of each of those citations, the Seattle Municipal Court shall place the vehicle on a list of scofflaws, and shall mail, by first class mail, a notice to the last known registered owner of the vehicle, as disclosed by the vehicle license number as provided by the Washington State Department of Licensing or equivalent vehicle licensing agency of the state in which the vehicle is registered. If there is no last known address that can be ascertained from the Washington Department of Licensing, or if the vehicle has no Washington vehicle license number or is not registered in the State of Washington, the notice, in the form of a readily visible notification sticker, may be affixed to the vehicle while left within a public right-of-way or other publicly owned or controlled property. A notification sticker may be used in lieu of mailing even if the last known address is ascertainable for vehicles registered in the State of Washington.

B. The registered vehicle owner may request an administrative review at the Seattle Municipal Court at any time that the vehicle is on the scofflaw list until the vehicle has been immobilized or impounded. The review should only examine whether the vehicle is properly on the scofflaw list and shall not review the underlying citations that caused the vehicle to be included on the scofflaw list. The vehicle shall be removed from the list only upon a showing by the registered owner that either:

1. fewer than four of the citations that caused the vehicle to be included on the scofflaw list were committed while the current registered owner was the legal owner of the vehicle; or

2. all amounts due pertaining to the citations that met the criteria for scofflaw under Section 11.35.010 A have been satisfied in full.

C. A vehicle shall remain on the scofflaw list until all outstanding parking infraction penalties, court costs (including but not limited to collection agency remuneration authorized under RCW 3.02.045), default penalties on parking traffic infractions imposed under Section 11.31.120, immobilization release fees imposed under subsection 11.35.020.H, costs of impoundment (including removal, towing and storage fees) imposed under Section 11.30.120, towing administrative fees imposed under Section 11.30.290 and immobilization administrative fees under subsection 11.35.020.H, and interest, have been paid, or a time payment plan has been arranged with the Seattle Municipal Court or their authorized agent.

D. When a time payment plan is created, the subject vehicle shall be temporarily removed from the scofflaw list and the payment amounts shall be applied on a pro rata basis until all penalties, fines or fees owed relating to all parking citations are satisfied. A vehicle that has been temporarily removed from the scofflaw list shall be returned to the list if the owner defaults on the time payment agreement, in accordance with guidelines adopted by the Seattle Municipal Court.

(Ord. 124558, § 1, 2014; Ord. 123563, § 1, 2011; Ord. 123447, § 1, 2010)

11.35.020 - Immobilization

A. Effective July 1, 2011 and thereafter, if the notice requirements under Section 11.35.010 A have been met, and if parked in public right-of-way or on other publicly owned or controlled property, a vehicle on the scofflaw list may be immobilized by installing on such vehicle a device known as a "boot," which clamps and locks onto the vehicle wheel and impedes vehicle movement. If a vehicle is immobilized, it shall not be released until full payment has been made, or a time payment agreement has been entered into for all outstanding penalties, fines, or fees owed for all parking citations, plus all immobilization, towing, and storage charges and administrative fees.

B. Any vehicle that remains booted for 48 hours or more, not including any of the 48 hours from the beginning of Saturday until the end of Sunday, or which becomes illegally parked while booted, shall be subject to towing and impoundment pursuant to Section 11.30.040. The Seattle Department of Transportation and Seattle Police Department shall issue joint guidelines for vehicle towing related to immobilization, based on Sections 11.30.040 and 11.16.320.

C. The person installing the boot shall leave under the windshield wiper or otherwise attach to the vehicle a notice advising the owner that the vehicle has been booted by the City of Seattle for failure to respond, failure to appear at a requested hearing, and failure to pay amounts due for four or more adjudicated parking infractions for at least 45 days from the date of the last such adjudication issued against the vehicle; that release of the boot may be obtained by paying all outstanding penalties, fines, or forfeitures owed relating to all adjudicated violations, plus all booting, removal, towing, and storage charges and administrative fees; that unless such payment is made within two business days of the date of the notice, the vehicle will be impounded; that it is unlawful for any person to remove or attempt to remove the boot, to damage the boot, or to move the vehicle with the boot attached, unless authorized by the Seattle Police Department or an authorized agent of the City; and that the owner may seek an administrative review of the booting by submitting a request to the Seattle Municipal Court within ten days of the release of the boot. The notice shall further state that the vehicle remains subject to impoundment regardless of whether the owner requests an appeal.

D. The vehicle may be released from immobilization when the vehicle owner or an agent of the owner pays all outstanding parking infraction penalties, court costs (including but not limited to collection agency remuneration authorized under RCW 3.02.045), default penalties on parking traffic infractions imposed under Section 11.31.120, immobilization release fees imposed under subsection 11.35.020.H, costs of impoundment (including removal, towing and storage fees) imposed under Section 11.30.120, towing administrative fees imposed under Section 11.30.290 and immobilization administrative fees under subsection 11.35.020.H, and interest, or enters into a time payment agreement for the payment thereof. Upon full payment or upon entry into a time payment agreement, the Seattle Police Department or other authorized agent of the City shall promptly remove or enable the removal of the boot from the vehicle. If payment is made in full, the vehicle shall be removed from the scofflaw list and shall not be subject to immobilization or impoundment for the paid citations. Upon entry into a time payment agreement, the vehicle shall be temporarily removed from the scofflaw list and shall not be subject to immobilization, provided, however, that the vehicle shall be returned to the scofflaw list and be subject to immobilization if the owner defaults on the time payment agreement. A registered owner who defaults on a time payment agreement shall not be given another opportunity to make a time payment arrangement and therefore, payment for all outstanding amounts above shall be made in full before the vehicle may be removed from the scofflaw list or released from immobilization or impound. Any person who has previously removed or enabled removal of a booting device in violation of subsection E while on the scofflaw list for any four or more parking infractions, and subsequently is booted a second time while on the scofflaw list for the same parking infractions, shall not be eligible for a time payment plan.

E. No person other than an authorized employee of the Seattle Police Department or an authorized agent of the City shall remove or enable the removal of the boot described in subsection A of this Section from any vehicle on which it has been installed unless the requirements of subsection D have been met.

F. If the Seattle Police Department or an authorized agent of the City enables the vehicle owner to remove the boot, the owner shall return the boot to a location designated by the Department within two calendar days of the removal.

G. No person, other than an authorized employee of the Seattle Police Department or other authorized agent of the City, shall move, by towing or other means, any vehicle after it has been immobilized but before the boot has been removed.

H. The Director of Finance and Administrative Services shall determine and set an immobilization fee and an administrative fee in amounts such that the sum of such fees do not exceed the sum of the lowest impound fee, minimum storage fee, and administrative fee for vehicle impoundment under Section 11.30.120. An administrative fee, if any, shall be levied when the boot is removed. The

administrative fee shall be collected by the contractor releasing the vehicle from immobilization, shall be remitted to the Department of Finance and Administrative Services, and shall be deposited in an appropriate account.

I. A person who fails to return the booting device within the time frame required by subsection F of this section may be charged a late fee as determined by the Director of Finance and Administrative Services.

J. A person who intentionally damages the booting device may be charged a replacement fee as determined by the Director of Finance and Administrative Services and also may be prosecuted for the crime of property destruction under section 12A.08.020.

K. The Director of Finance and Administrative Services shall adopt rules governing the imposition of fees under this Section 11.35.020.

(Ord. 124558, § 2, 2014; Ord. 123563, § 2, 2011; Ord. 123447, § 1, 2010)

11.35.030 - Post-immobilization review

The registered vehicle owner may seek a post-deprivation review of the immobilization by submitting a written request to the Seattle Municipal Court within ten days of the placement of the notice on the vehicle, as established by the notice date. Upon timely receipt of such written request, the Seattle Municipal Court shall, within a reasonable time as established by the Court, conduct a review on the issue of whether the immobilization was proper and shall issue a written decision setting forth the reasons on which the decision is based, provided, however, that any previously adjudicated parking infractions that formed the basis of the vehicle's scofflaw status shall not be subject to the review. The person seeking review shall have an opportunity to present evidence on his or her behalf in accordance with requirements established by the Court.

(Ord. 123447, § 1, 2010)

Chapter 11.35 - IMMOBILIZATION

Sections:

11.35.010 - Scofflaw list

A. When there are four or more parking citations issued against a vehicle for each of which a person has failed to respond, failed to appear at a requested hearing, or failed to pay amounts due for at least 45 days from the date of the filing of each of those citations, the Seattle Municipal Court shall place the vehicle on a list of scofflaws, and shall mail, by first class mail, a notice to the last known registered owner of the vehicle, as disclosed by the vehicle license number as provided by the Washington State Department of Licensing or equivalent vehicle licensing agency of the state in which the vehicle is registered. If there is no last known address that can be ascertained from the Washington Department of Licensing, or if the vehicle has no Washington vehicle license number or is not registered in the State of Washington, the notice, in the form of a readily visible notification sticker, may be affixed to the vehicle while left within a public right-of-way or other publicly owned or controlled property. A notification sticker may be used in lieu of mailing even if the last known address is ascertainable for vehicles registered in the State of Washington.

B. The registered vehicle owner may request an administrative review at the Seattle Municipal Court at any time that the vehicle is on the scofflaw list until the vehicle has been immobilized or impounded. The review should only examine whether the vehicle is properly on the scofflaw list and shall not review the underlying citations that caused the vehicle to be included on the scofflaw list. The vehicle shall be removed from the list only upon a showing by the registered owner that either:

1. fewer than four of the citations that caused the vehicle to be included on the scofflaw list were committed while the current registered owner was the legal owner of the vehicle; or

2. all amounts due pertaining to the citations that met the criteria for scofflaw under Section 11.35.010 A have been satisfied in full.

C. A vehicle shall remain on the scofflaw list until all outstanding parking infraction penalties, court costs (including but not limited to collection agency remuneration authorized under RCW 3.02.045), default penalties on parking traffic infractions imposed under Section 11.31.120, immobilization release fees imposed under subsection 11.35.020.H, costs of impoundment (including removal, towing and storage fees) imposed under Section 11.30.120, towing administrative fees imposed under Section 11.30.290 and immobilization administrative fees under subsection 11.35.020.H, and interest, have been paid, or a time payment plan has been arranged with the Seattle Municipal Court or their authorized agent.

D. When a time payment plan is created, the subject vehicle shall be temporarily removed from the scofflaw list and the payment amounts shall be applied on a pro rata basis until all penalties, fines or fees owed relating to all parking citations are satisfied. A vehicle that has been temporarily removed from the scofflaw list shall be returned to the list if the owner defaults on the time payment agreement, in accordance with guidelines adopted by the Seattle Municipal Court.

(Ord. 124558, § 1, 2014; Ord. 123563, § 1, 2011; Ord. 123447, § 1, 2010)

11.35.020 - Immobilization

A. Effective July 1, 2011 and thereafter, if the notice requirements under Section 11.35.010 A have been met, and if parked in public right-of-way or on other publicly owned or controlled property, a vehicle on the scofflaw list may be immobilized by installing on such vehicle a device known as a "boot," which clamps and locks onto the vehicle wheel and impedes vehicle movement. If a vehicle is immobilized, it shall not be released until full payment has been made, or a time payment agreement has been entered into for all outstanding penalties, fines, or fees owed for all parking citations, plus all immobilization, towing, and storage charges and administrative fees.

B. Any vehicle that remains booted for 48 hours or more, not including any of the 48 hours from the beginning of Saturday until the end of Sunday, or which becomes illegally parked while booted, shall be subject to towing and impoundment pursuant to Section 11.30.040. The Seattle Department of Transportation and Seattle Police Department shall issue joint guidelines for vehicle towing related to immobilization, based on Sections 11.30.040 and 11.16.320.

C. The person installing the boot shall leave under the windshield wiper or otherwise attach to the vehicle a notice advising the owner that the vehicle has been booted by the City of Seattle for failure to respond, failure to appear at a requested hearing, and failure to pay amounts due for four or more adjudicated parking infractions for at least 45 days from the date of the last such adjudication issued against the vehicle; that release of the boot may be obtained by paying all outstanding penalties, fines, or forfeitures owed relating to all adjudicated violations, plus all booting, removal, towing, and storage charges and administrative fees; that unless such payment is made within two business days of the date of the notice, the vehicle will be impounded; that it is unlawful for any person to remove or attempt to remove the boot, to damage the boot, or to move the vehicle with the boot attached, unless authorized by the Seattle Police Department or an authorized agent of the City; and that the owner may seek an administrative review of the booting by submitting a request to the Seattle Municipal Court within ten days of the release of the boot. The notice shall further state that the vehicle remains subject to impoundment regardless of whether the owner requests an appeal.

D. The vehicle may be released from immobilization when the vehicle owner or an agent of the owner pays all outstanding parking infraction penalties, court costs (including but not limited to collection agency remuneration authorized under RCW 3.02.045), default penalties on parking traffic infractions imposed under Section 11.31.120, immobilization release fees imposed under subsection 11.35.020.H, costs of impoundment (including removal, towing and storage fees) imposed under Section 11.30.120, towing administrative fees imposed under Section 11.30.290 and immobilization administrative fees under subsection 11.35.020.H, and interest, or enters into a time payment agreement for the payment thereof. Upon full payment or upon entry into a time payment agreement, the Seattle Police Department or other authorized agent of the City shall promptly remove or enable the removal of the boot from the vehicle. If payment is made in full, the vehicle shall be removed from the scofflaw list and shall not be subject to immobilization or impoundment for the paid citations. Upon entry into a time payment agreement, the vehicle shall be temporarily removed from the scofflaw list and shall not be subject to immobilization, provided, however, that the vehicle shall be returned to the scofflaw list and be subject to immobilization if the owner defaults on the time payment agreement. A registered owner who defaults on a time payment agreement shall not be given another opportunity to make a time payment arrangement and therefore, payment for all outstanding amounts above shall be made in full before the vehicle may be removed from the scofflaw list or released from immobilization or impound. Any person who has previously removed or enabled removal of a booting device in violation of subsection E while on the scofflaw list for any four or more parking infractions, and subsequently is booted a second time while on the scofflaw list for the same parking infractions, shall not be eligible for a time payment plan.

E. No person other than an authorized employee of the Seattle Police Department or an authorized agent of the City shall remove or enable the removal of the boot described in subsection A of this Section from any vehicle on which it has been installed unless the requirements of subsection D have been met.

F. If the Seattle Police Department or an authorized agent of the City enables the vehicle owner to remove the boot, the owner shall return the boot to a location designated by the Department within two calendar days of the removal.

G. No person, other than an authorized employee of the Seattle Police Department or other authorized agent of the City, shall move, by towing or other means, any vehicle after it has been immobilized but before the boot has been removed.

H. The Director of Finance and Administrative Services shall determine and set an immobilization fee and an administrative fee in amounts such that the sum of such fees do not exceed the sum of the lowest impound fee, minimum storage fee, and administrative fee for vehicle impoundment under Section 11.30.120. An administrative fee, if any, shall be levied when the boot is removed. The

administrative fee shall be collected by the contractor releasing the vehicle from immobilization, shall be remitted to the Department of Finance and Administrative Services, and shall be deposited in an appropriate account.

I. A person who fails to return the booting device within the time frame required by subsection F of this section may be charged a late fee as determined by the Director of Finance and Administrative Services.

J. A person who intentionally damages the booting device may be charged a replacement fee as determined by the Director of Finance and Administrative Services and also may be prosecuted for the crime of property destruction under section 12A.08.020.

K. The Director of Finance and Administrative Services shall adopt rules governing the imposition of fees under this Section 11.35.020.

(Ord. 124558, § 2, 2014; Ord. 123563, § 2, 2011; Ord. 123447, § 1, 2010)

11.35.030 - Post-immobilization review

The registered vehicle owner may seek a post-deprivation review of the immobilization by submitting a written request to the Seattle Municipal Court within ten days of the placement of the notice on the vehicle, as established by the notice date. Upon timely receipt of such written request, the Seattle Municipal Court shall, within a reasonable time as established by the Court, conduct a review on the issue of whether the immobilization was proper and shall issue a written decision setting forth the reasons on which the decision is based, provided, however, that any previously adjudicated parking infractions that formed the basis of the vehicle's scofflaw status shall not be subject to the review. The person seeking review shall have an opportunity to present evidence on his or her behalf in accordance with requirements established by the Court.

(Ord. 123447, § 1, 2010)

Seattle Police Department Manual

Carmen Best, Chief of Police

12.110 - USE OF DEPARTMENT E-MAIL & INTERNET SYSTEMS

Effective Date: 05/01/18

The Seattle Police Department provides email service and internet access to conduct Department business.

The guidelines in this section are not exclusive. They provide a general framework of prohibited and acceptable email and internet use.

This section applies to all employees and their access to the internet while on City equipment or while on duty and their use of City email by any means.

12.110-POL

1. The City of Seattle Owns the Email and Internet Systems and Determines Appropriateness

The City owns the computers, email, and internet access systems and may monitor email and internet use for policy compliance. The City retains the right to determine what is appropriate for the workplace.

Department supervisors ensure that their staff is familiar with and adhere to Department and City email and internet policy.

2. The Department Allows Limited Personal Use of Email and Internet

Recognizing the realities of the workplace, the Department allows limited personal use of email and the internet. Occasional personal use is permissible if it follows the policies and usage standards set by the Department and the City.

3. Department Email and Internet Use is Subject to Public Disclosure

There is no expectation of privacy in using Department email or internet services on Department-owned computers. All use of Department computers, whether official or personal, is subject to public disclosure laws and can be discoverable in a lawsuit.

4. All Email and Internet Communications Must be Professional, Appropriate, and Lawful

All email communications and internet use must comply with Department and City policies on professionalism and harassment in the workplace. Employees will clearly identify their personal opinions or preliminary observations.

All internet use on Department computers comply with all laws and policies. This includes policies on privacy issues, any release of confidential, sensitive, or classified information, or information exempt from public disclosure.

The Department acknowledges that email signatures and user photos may contribute to an employee's professional image. Employees wishing to include photos, emblems (other than the SPD patch), logos, quotations, or other similar items in their email signature must have their proposed email signature approved by their chain of command through the deputy chief in advance.

5. Employees May Send Criminal Justice Information (CJI) or Other

Sensitive Information via Office Message Encryption (OME)

Ensure the recipient is a member of a Criminal Justice Agency and allowed to receive CJI information.

Including the trigger word "COSSecure" in the subject line of an email message sent from an SPD Outlook email account.

- Inserting "COSSecure" within the subject line of an SPD Outlook email will activate OME for that email.

6. Employees Will Read Email at Least Once per Shift and Respond Appropriately

Employees are not required to read or respond to email when off duty or during a system outage or technical failure that prevents the receipt or sending of email.

Employees will respond (when applicable) to High Importance emails within four business days, or sooner if required by the subject matter.

Emails classified as High Importance are marked with an orange exclamation point and include the following subjects:

- Command Staff Communications
- Directives
- Special Orders
- Training Digests
- All other emails that are job-related, time sensitive, and mandatory for the recipient
- These include subpoenas, wanted bulletins, information bulletins, investigative follow-up requests, statement requests, pre-trial discovery requests, and seizure hearing notices.

A lieutenant or above must approve the use of the High Importance classification for any other email communication.

7. Employees Will Activate Automatic Email Replies for Extended Absences

Employees will activate their email Automatic Replies (Out of Office) in Outlook when they expect that they will be unable to respond to email for a period that exceeds four business days.

8. External Emails Will Contain Employee Contact Information

All email correspondence going outside the Department will contain the employee's contact information including email address, business address, and business phone numbers.

9. General Distribution Emails Require Lieutenant Approval

Emails going to large distribution lists such as SPDALL or SPDSWORN are general distribution emails. These emails require approval from a lieutenant or above, and must include the name of the approving employee in the email.

When sending a general distribution email, employees will enter the recipients using the "Bcc" (blind carbon copy) field. The "Bcc" field will prevent unnecessary disclosure of email addresses, reduce vulnerability to junk email, and improve the chances of the email being successfully sent. The "To" field is not designed to handle a large number of addresses.

10. Employees Must Use Caution When Opening Email Attachments

Employees may contact Seattle IT if they have questions about an email attachment. Due to the risk of computer virus attacks, employees should not open email attachments from an unknown source.

11. Section Captain or Director Approves "Send As" Privileges for Shared Email Accounts

Employees must request "Send As" privileges for a shared mailbox, and/or request that a shared mailbox be created, by submitting a request via email to their section captain or director.

Employees will forward the approval to Seattle IT and initiate a service request.

12. Employees Will Not use Department Email or Computers to Conduct a Personal For-Profit Business

13. Employees Will Not use Department Email or Computers to Review Personal Investments or to Transact any Investment Business

These types of transactions include trading in stocks, bonds, or mutual funds.

Exception: Employees may conduct infrequent, brief checks of their investments in the City's Deferred Compensation Program, since this is a City-sponsored and City-maintained program.

14. Employees Will Not use Department Email or Computers to Participate in any Campaign for Elected Office or for any Other Political Activity

This includes a prohibition on making any campaign contributions via a credit card and using a Department computer to do so. Similarly, employees may not "lobby" elected officials through Department computers.

15. Employees Will not use Department Email or Computers to Engage in Demeaning or Defamatory Conduct

Examples of such prohibited activities include knowingly accessing pornographic materials or sites that promote exclusivity, hatred, or positions which are contrary to the City's policy of valuing cultural diversity.

16. Employees Will Not Access Sites That Incur a Cost to the Department Without Prior Supervisor Approval

17. Employees Will Not Knowingly Access or Communicate any Material of an Obscene, Harassing, Discriminatory or Derogatory Nature

Examples of such material include sites or email containing racial or sexual slurs or jokes, or containing harassing, intimidating, abusive, or offensive material to or about others.

18. Certain Assignments May Require Access to Sensitive Sites

The Department recognizes that certain employees, such as Vice and Intelligence Unit detectives, may have a legitimate business purpose for accessing sites and information otherwise considered inappropriate or illegal.

If employees need to access such "sensitive sites", employees will abide by the following:

- Employees will obtain approval from an immediate supervisor before accessing sensitive sites. The supervisor will contact Seattle IT to request an exception to the web filtering protocols.

- Employees accessing such sites should exercise courtesy to others that may be present when doing so. This may include closing the door, turning the screen away, or notifying other employees beforehand.

19. Department Computer Usage is Subject to the Intelligence Ordinance

Employees will adhere to the following guidelines to avoid a violation of the investigation ordinance, SMC Chapter 14.12 ("Restricted information" is defined in SMC 14.12.030 (K)):

- Storage of "restricted information" (as defined in the ordinance) on disks or computer/network drives must comply with the ordinance.

- Employees may not create directories or subdirectories which organize/index "restricted information."

- Employees may not transmit "restricted information" including web addresses (URLs) to specific sites, via email.

- Employees may not create bookmarks or hotlists in web browsers which organize/index restricted information.

Site Disclaimer: The Seattle Police Department's website was developed to provide general information. Data contained at this location is generally not reviewed for legal sufficiency. SPD documents displayed are for reference purposes only. Their completeness or currency are not guaranteed. Links or references to other information or organizations are for reference only and do not constitute an endorsement.

ADA Notice

Notice of Nondiscrimination

Privacy

© Copyright 1995-2018 City of Seattle

Seattle Police Department Manual
Carmen Best, Chief of Police

5.001 - STANDARDS AND DUTIES

Effective Date: 03/01/18

5.001-POL

This policy provides the philosophy for employee conduct and professionalism. It is not the Department's intent to interfere with or constrain the freedoms, privacy, and liberties of employees; discipline will only be imposed where there is a connection between the conduct and the duties, rank, assignment, or responsibilities of the employee.

The Department expects all employees to treat all people with dignity; remember that community care-taking is at times the focus, not always command and control; and that the guiding principle is to treat everyone with respect and courtesy, guarding against employing an officious or overbearing attitude and refraining from language, demeanor, and actions that may cause the individual feeling belittled, ridiculed, or intimidated.

This section applies to all Department employees. The content is not all-inclusive. Employees must also comply with conduct expectations in other manual sections pertaining to them.

1. The Chief of Police Determines Employee Duty Status

The Chief of Police has final authority through the Charter of the City of Seattle to determine the on-duty status of any employee, and whether their actions are within the course and scope of their duties.

Completion of overtime or other Department forms by an employee does not establish the employee's duty status.

2. Employees Must Adhere to Laws, City Policy and Department Policy

Employees adhere to:

- Federal laws
- State laws
- Laws of the City of Seattle
- City of Seattle policies
- The Seattle Police Manual
- Published Directives and Special Orders
- Applicable collective bargaining agreements and relevant labor laws

3. Employees Use Training to Assist in Following Policy

Department training is intended to provide guidance on how to implement and follow policy.

Not following training, in itself, is not a policy violation.

Regardless of the result, an employee may need to explain, and possibly document, a substantial deviation from training

4. Employees Must Attend All Mandatory Training

Employees will attend mandatory training and follow the current curriculum during their duties.

Employees who have missed any mandatory training because of excused absences, such as a sick day or court appearance, will arrange through their immediate supervisor to complete that training within a reasonable time frame.

Employees on approved limited duty who cannot participate in a mandatory training program will request a waiver using SPD Memorandum (form 1.11), and an Insurer Activity Prescription Form (APF) through their chain of command.

Also See: 1.075-Failure to complete Required Training

5. Employees Complete Work in a Timely Manner

Absent exigent circumstances or supervisory approval, employees will complete all required duties and official reports before going off duty.

6. Employees May Use Discretion

Employees are authorized and expected to use discretion in a reasonable manner consistent with the mission of the Department and duties of their office and assignment.

Discretion is proportional to the severity of the crime or public safety issue being addressed.

7. Employees Engaged in Department-Related Activities Identify Themselves When Requested

Employees will provide their name and Department serial number verbally, or in writing if requested.

Employees may use a Department-issued business card that contains their name and serial number to satisfy the request for the information.

Employees will also show their department identification card and badge (sworn) when specifically requested to do so.

Exception: Employees are not required to immediately identify themselves if:

- An investigation is jeopardized
- A police function is hindered
- There is a safety consideration

8. On-Duty Officers in Civilian Attire Identify Themselves When Contacting Citizens

Officers will accomplish this verbally and/or by displaying their badge or Department-issued identification.

Exception: Employees are not required to immediately identify themselves if:

- An investigation is jeopardized
- A police function is hindered
- There is a safety consideration

9. Uniformed Employees Will Not Initiate Contact With Officers Dressed In Civilian Clothing

When any uniformed employee meets an officer dressed in civilian attire, that uniformed employee will not openly recognize the plain-clothes officer unless greeted first.

10. Employees Shall Strive to be Professional

Regardless of duty status, employees may not engage in behavior that undermines public trust in the Department, the officer, or other officers. Employees will avoid unnecessary escalation of events even if those events do not end in reportable uses of force.

Any time employees represent the Department or identify themselves as police officers or Department employees, they will not use profanity directed as an insult or any language that is derogatory, contemptuous, or disrespectful toward any person.

Employees on duty or in uniform will not publicly ridicule:

- The Department or its policies
- Other Department employees
- Other law enforcement agencies
- The criminal justice system or police profession

This applies where such expression is defamatory, obscene, undermines the effectiveness of the Department, interferes with the maintenance of discipline, or is made with reckless disregard for truth.

11. Employees Shall Be Truthful and Complete in All Communication

Exception: Employees may use deception for a specific and lawful purpose in certain circumstances, when:

- There is an exigent threat to life safety or public safety
- It is necessary due to the nature of the employee's assignment
- There is a need to acquire information for a criminal investigation

12. Employees Must Promptly Report Exonerating Information

Employees must report any information they discover that may exonerate a person who is under investigation, or has been charged with or convicted of a crime.

13. Employees Shall Not Use Their Position or Authority for Personal Gain

14. Retaliation is prohibited

No employee will retaliate against any person who:

- Exercises a constitutional right
- Records an incident
- Makes a public disclosure request
- Publicly criticizes an SPD employee or the Department
- Initiates litigation

- Opposes any practice reasonably believed to be unlawful or in violation of Department policy
- Files a complaint or provides testimony or information related to a complaint of misconduct
- Provides testimony or information for any other administrative criminal or civil proceeding involving the Department or an officer
- Communicates intent to engage in the above-described activities
- Otherwise engages in lawful behavior

Retaliation includes discouragement, intimidation, coercion, or adverse action against any person. This prohibition will include any interference with the conduct of an administrative, civil, or criminal investigation.

Such retaliation may be a criminal act, may give rise to personal civil liability, or constitute independent grounds for discipline, up to and including termination.

15. Employees Obey any Lawful Order Issued by a Superior Officer

Failure to obey lawful orders from a superior officer constitutes insubordination. Orders may be issued directly, relayed through a subordinate employee or current Department training, published in notices, and other forms of communication.

16. Supervisors Clarify Conflicts in Orders

Should any orders conflict with a previous order, or published regulation, employees may respectfully bring this to the supervisor's attention.

The supervisor who issued the conflicting order will try to correct the conflict in orders.

17. Employees May Object to Orders Under Certain Conditions

An employee may object to a supervisor's orders under these conditions:

- When such orders represent unjustified, substantial and/or reckless disregard for life or safety
- When such orders are illegal or unethical
- When the supervisor has been relieved of duty by an employee of higher rank
- When other circumstances are present that establish the supervisor's inability to discharge the duties of the assignment

Employees in this situation will, if practical, state the basis for objecting to the order to the supervisor.

If the situation remains unresolved, the employee will immediately contact the next higher ranking supervisor in the chain of command.

18. Employees Must Avoid Conflicts of Interest

Employees will not associate with persons or organizations where such association reasonably gives the appearance of conflict of interest.

Employees will not engage in enforcement, investigative, or administrative functions that create or give the appearance of conflicts of interest.

Employees will not investigate events where they are involved. This also applies where any person with whom the employee has a personal relationship is involved in the event.

Except in cases of emergency, officers will not arrest family members, business associates, or social acquaintances.

Employees will not show preference by recommending or suggesting the employment of any attorney, bondsman, or other business during the course of, or because of, their official business as employees of the Department.

See also SMC 4.16-City Code of Ethics and 5.120 – Off-Duty Employment.

19. Employees Must Disclose Conflicts

Employees will immediately disclose to the Chief of Police, via their supervisor, any activities or relationships that may present an actual, potential, or apparent conflict of interest for themselves or other Department employees.

20. Employees Shall Not Use a Department Mailing Address for Personal Reasons

This provision includes using a Department address for a driver license, vehicle registration, telephone service, etc.

21. Employees Shall Not Imply to Another Agency the Department's Approval or Disapproval of That Agency's Actions

22. Employees Shall Not Recommend Case Dispositions to Courts

No employee below Assistant Chief will make any recommendations to any court or other judicial agency regarding the disposition of any pending court case investigated by the Department.

Exception: This does not apply to agencies conducting pre-sentence investigations.

23. Employees Notify the Department Before Initiating any Claim for Damages Related to Their Official Position

Employees must report their intention to initiate a claim for damages sustained while working in a law enforcement capacity or by virtue of employment with the Department. This notification is to the Chief of Police via the employee's chain of command.

24. Officers Report any Off-Duty Assault on Themselves Related to Department Employment

If an employee is assaulted while working off-duty in a law enforcement capacity, that employee must report the assault. The employee must then notify the Department before seeking a No Contact or Restraining Order related to the assault. This notification is to the Chief of Police via the employee's chain of command.

25. Employees Report Their Intent to Initiate Lawsuits or Seek Court Orders

Employees must report to the Chief of Police their intention to sue for damages sustained while working in a law enforcement capacity or by virtue of employment with the Department.

Sworn employees will notify their supervisor prior to applying for a No Contact or Restraining Order stemming from an assault on the employee that occurred while the employee was working in a law enforcement capacity.

26. Employees Follow the Americans With Disabilities Act (ADA) in the Performance of their Job

Employees interacting with persons with disabilities will take steps to provide needed accommodations to provide police services or achieve a law enforcement goal.

See: Commonly asked questions about the Americans with Disabilities Act and Law Enforcement, ADA.gov, City of Seattle ADA.

Site Disclaimer: The Seattle Police Department's website was developed to provide general information. Data contained at this location is generally not reviewed for legal sufficiency. SPD documents displayed are for reference purposes only. Their completeness or currency are not guaranteed. Links or references to other information or organizations are for reference only and do not constitute an endorsement.

ADA Notice

Notice of Nondiscrimination

Privacy

© Copyright 1995-2018 City of Seattle

Seattle Police Department Manual
Carmen Best, Chief of Police

5.002 - RESPONSIBILITIES OF EMPLOYEES CONCERNING ALLEGED POLICY VIOLATIONS

Effective Date: 07/15/18

5.002-POL

This policy applies to the reporting of alleged policy violations identified by the public, employees of the Department, or others and related investigations by the Department and OPA.

The purpose of this policy and the related procedures is to provide a prompt, just, and open disposition of allegations of policy violation regarding the conduct of employees.

1. The Department Will Accept Allegations of Policy Violations from Any Source and by Any Means

2. Employees Will Assist Any Person Who Wishes to File a Complaint

In addition to obligations that may arise under other parts of this manual (e.g., See 5.140-Bias-Free Policing-6, 7) employees will assist the complainant by taking the complaint and passing it on to a supervisor or OPA (see also 6 below.)

If the complainant requests information on where and how to file the allegation, the employee will provide it. However, the employee is still responsible for passing the complaint on to a supervisor or OPA.

If the employee is unable to take the complaint (e.g., the allegation is made during a demonstration while the employee is on a line, etc.), while not interfering or compromising public safety interests, the employee will provide specific information to the complainant on where and how to file the allegation.

3. Employees Shall Not Discourage, Interfere With, Hinder, or Obstruct Any Person from Filing a Complaint or Conducting or Cooperating with an Investigation of an Allegation of a Policy Violation

4. Retaliation Is Prohibited

No employee will retaliate against any person who:

- Exercises a constitutional right
- Records an incident, including videotaping and photographing
- Makes a public disclosure request
- Publicly criticizes an SPD employee or the Department
- Initiates litigation
- Opposes any practice reasonably believed to be unlawful or in a violation of Department policy

- Files a complaint or provides testimony or information related to an allegation of policy violations, including but not limited to complaints made OPA, Human Resources, or the EEO Investigator

- Provides testimony or information for any other administrative criminal or civil proceeding involving the Department or a Department employee

-Files a whistle-blower claim pursuant to Seattle Municipal Code

- Communicates an intent to engage in the above-described activities

- Otherwise engages in lawful behavior

Retaliation includes discouragement, intimidation, coercion, or undertaking any adverse action against any person because the person engaged in any of the activity set forth above. This prohibition specifically includes interference with any administrative, civil, or criminal investigation.

Retaliation may constitute independent grounds for discipline, up to and including termination.

5. Supervisors Will Investigate or Refer Allegations of Policy Violations Depending on the Severity of the Violation

a. All allegations of serious policy violations will be referred to OPA for investigation.

The following are serious policy violations that must be referred to OPA:

- Unnecessary, unreasonable, or disproportionate use of force

- Biased policing, including use of language that is derogatory based on an individual's sex, race, ethnicity, religion, homeless status, or other protected class.

  - **Exception**: Supervisors will not report an allegation of biased policing directly to OPA in those circumstances where a Bias Review Blue Team Entry is appropriate under 5.140-POL-6 and 5.140-POL-7.

  - See 5.140-Bias-Free Policing, sections 6 & 7.

- Any other violation of SPD policy that may violate a suspect/person's constitutional rights to freedom of speech, to the free exercise of religion, to peaceably assemble, to due process of law, and to be secure against unreasonable search and seizure

- Violations of law enforcement authority

- Failure to use ICV when required

- Failure to report serious policy violations to OPA

- Violations of any policy that are intentional or reckless

- Serious neglect of duty

- Insubordination

- Potential criminal violations of law

  - Failure to fully cooperate in an internal investigation

- Dishonesty

- Misuse of authority, conflicts of interest, or improper use of position for personal gain

- Repeated minor policy violations

b. If the severity of the violation is unclear, the lieutenant or civilian equivalent will consult OPA.

The level of seriousness of an alleged policy violation is sometimes contingent upon the specific facts of an incident. The Department recognizes that even some minor violations may raise concerns of public trust and warrant a referral to OPA. Employees should consider the totality of the circumstances when determining the level of seriousness of an alleged policy violation, apply common sense, and consult with an OPA lieutenant or above if uncertain.

c. Minor policy violations (allegations of policy violations that do not rise to the level of "serious") must still be investigated by the chain of command.

Supervisors who witness, have reason to believe, or receive an allegation of a minor policy violation are expected to address the violation as they deem appropriate.

Supervisors also have the discretion to refer allegations of even minor policy violations to OPA for investigation where they deem it appropriate.

Allegations of minor policy violations may include administrative, procedural, or technical violations of SPD policies that are unrelated to:

(1) The use of force,

(2) Exercise of law enforcement authority, and/or

(3) The list of serious offenses outlined above or issues involving similarly serious potential violations.

Example of allegations of minor policy violations include, but are not limited to:

- Force reporting timeline violations

  - **Exception**: Willful violations of the force reporting timelines must be considered serious violations of policy and referred to OPA

- Failure to perform a system checks on ICV/BWV equipment that causes no failure to record officer actions

- Failure to seatbelt subjects who are being transported by an officer in a seatbelt equipped Department vehicle or during performing official duties where the detainee is not injured as the result of not being secured.

- Failure to identify tactical issues or document deficiencies in the use of force packet

- Failure to turn off the vehicle's AM/FM radio when the ICV is engaged

- Engaging in law enforcement related secondary employment without a valid secondary work permit on file with the Department

- Minor Rudeness (absent bias)

- Traffic and parking infractions

- Profanity not directed as an insult

- Employee tardiness

- Uniform, equipment, and personal appearance

- Failure to attend and/or complete required training (including mandatory e-Learning modules on Cornerstone) for which the employee is registered, unless the failure is:

  - Unjustified and/or

  - The employee fails to provide reasonable advance notice he or she will not attend a scheduled training

  (Supervisors may contact the Cornerstone lieutenant in ETS to research an employee's previous instances of missed training.)

- Failure of a supervisor to register employees for training, except when that failure results in the employees missing the opportunity to attend training

6. Employees Will Report Alleged Violations

Employees will report any alleged minor policy violation to a supervisor.

Employees will report any alleged serious violations to a supervisor or directly to OPA.

For sworn employees this reporting requirement also applies to allegations of uses of force not yet reported.

Employees who witness or learn of a violation of public trust or an allegation of a violation of public trust will take action to prevent aggravation of the incident or loss of evidence that could prove or disprove the allegation.

Any employee who observes another employee engaged in dangerous or criminal conduct or abuse will take reasonable action to intervene.

7. Employees Will Avoid Conflicts of Interest Regarding Allegations of Policy Violation

Employees' duty to avoid and disclose actual, potential, or apparent conflicts of interest (See 5.001-Standards and Duties) extends to the allegation process.

If a supervisor is the subject of an allegation of policy violation, the employee receiving the allegation will refer the allegation to the next highest level employee in the supervisor's chain of command.

If the subject of the allegation of policy violation is assigned to OPA, the employee receiving the report will forward the allegation to the OPA Director.

If the subject of the allegation of policy violation is the OPA Director, the allegation will be forwarded to the City Human Resources Director.

8. Employees Will Report Certain Events

Employees will report to their supervisor, in writing, as soon as practical (and before the start of their next work shift) any of these circumstances in any jurisdiction:

- They are the subject, or they believe they may be the subject of a criminal investigation, criminal traffic citation, arrest, or conviction

- They are the respondent of an order of protection, restraining order, no contact order, anti-harassment order

- Their Washington driver license is expired, suspended, revoked, or restricted, for example,

with an ignition interlock driver license

9. The OPA Manual Sets Forth OPA Procedures

10. OPA May Choose to Investigate Any Alleged Policy Violation

If a supervisor is informed that OPA is taking over an investigation, the supervisor will cease their investigation.

11. Employees Will Cooperate with Department Internal Investigations

Employees will truthfully answer all questions, render complete, comprehensive statements, and promptly provide all available material related to investigations of alleged policy violations. The statements will include all material facts and circumstances surrounding the subject matter of the investigation, which are known by the employee. Omissions of material facts known by the employee will be a failure to cooperate in an internal investigation.

12. OPA Maintains a Record of all Allegations Referred

All allegations of policy violations and any files related to these allegations will be secured within OPA offices for a period of time consistent with the Department's record retention policies.

5.002-TSK-1 Employee Reporting of Serious Policy Violations

When any employee is referring an allegation of serious policy violations to OPA, the employee:

1. **Provides** all of the following information to OPA, if possible:

- The nature, date and place of occurrence of the alleged incident

- Name of employee involved or their serial number and other description

- Name, address, and telephone number of the complainant, aggrieved party, and all known witnesses

- A detailed summary of the allegation

- Information about perishable and other known evidence, including video recordings

- Whether the investigation presents any actual, potential, or apparent conflicts of interest

2. **Assembles** any supporting documentation.

3. **Documents** the allegation on a Complaint Blue Team entry and forwards the entry to OPA via the chain of command.

Exception: If the employee named in the allegation is assigned to OPA, the allegation is sent directly to the OPA Director.

Exception: If the allegation involves the chain of command and the employee does not want it to be viewed by the chain of command, the employee may forward it directly to an OPA lieutenant.

Exception: If the allegation is an EEO complaint, the employee will refer to 5.040-PRO-1.

Site Disclaimer: The Seattle Police Department's website was developed to provide general information. Data contained at this location is generally not reviewed for legal sufficiency. SPD documents displayed are for reference purposes only. Their completeness or currency are not guaranteed. Links or references to other information or organizations are for reference only and do not constitute an endorsement.

ADA Notice

Notice of Nondiscrimination

Privacy

© Copyright 1995-2018 City of Seattle

Seattle Police Department Manual
Carmen Best, Chief of Police

6.060 - COLLECTION OF INFORMATION FOR LAW ENFORCEMENT PURPOSES

Effective Date: 5/19/2004

PHILOSOPHY

Information will be gathered and recorded in a manner that does not unreasonably infringe upon: individual rights, liberties, and freedoms guaranteed by the Constitution of the United States and the State of Washington, including freedom of speech, press, association, and assembly; liberty of conscience; the exercise of religion; the right to petition government for redress of grievances; and the right to privacy. Consistent with this policy, Department personnel shall comply with the dictates of the Investigations Ordinances and with the requirements of Department rules and regulations.

The Department will cooperate fully with the Investigations Ordinance auditor. The Auditor will be given total access to any and all files maintained by the Seattle Police Department except in the case of files or investigations which are specifically exempted from inspection by the Investigations Ordinances.

The Investigations Ordinance requires all Department personnel to safeguard the rights of persons involved in lawful political or religious activities and places restrictions on the documenting of certain types of information. While much of the Ordinances pertains to the activities of the Criminal Intelligence Section, the Ordinances is directed at the activities of the Department as a whole. Officers must keep the Ordinances in mind when writing reports. Any documentation of information concerning a person's sexual preferences or practices, or their political or religious activities must be for a relevant reason and serve a legitimate law enforcement purpose. Officers should also be aware of the Ordinances when photographing demonstrations or other lawful political activities. If demonstrators are not acting unlawfully, police can't photograph them. Periodic review of the Ordinances is worthwhile, as violations of the Ordinances could result in civil liability or disciplinary action, including discharge.

See SMC Chapter 14.12.

Site Disclaimer: The Seattle Police Department's website was developed to provide general information. Data contained at this location is generally not reviewed for legal sufficiency. SPD documents displayed are for reference purposes only. Their completeness or currency are not guaranteed. Links or references to other information or organizations are for reference only and do not constitute an endorsement.

ADA Notice

Notice of Nondiscrimination

Privacy

© Copyright 1995-2018 City of Seattle

Seattle Police Department Manual
Carmen Best, Chief of Police

12.040 - DEPARTMENT-OWNED COMPUTERS, DEVICES & SOFTWARE

Effective Date: 07/01/2018

12.040 - POL-1 General Policy

The Department follows the City's Information Systems Security Policy.

Employees using Department-owned devices or software will follow the City's security policy:

- Protect and never share access accounts, privileges, and associated passwords
- Maintain the confidentiality of sensitive information to which they are given access privileges
- Accept accountability for all activities associated with the use of their network accounts and related access privileges
- Ensure that use of City computers, email and other electronic communications (IM, etc.), Internet access, computer accounts, networks, and information stored, or used on any of these systems is restricted to authorized purposes and defined use limitations
- Maintain information security awareness.
- Report all suspected security and/or policy violations to an appropriate authority (e.g. manager, supervisor, system administrator or the Office of Information Security).

For this policy, the term device means any electronic equipment that has the capability to:

- Connect to the internet or department computer network and/or;
- Be used as a means of communication.

Exception: This policy does not apply to devices being used while conducting undercover operations. Employees will refer to their unit guidelines when using undercover devices.

12.040 - POL-2-Protecting Department Hardware, Software and Computer Systems

The City's Information Technology Department (ITD) ensures the security of computer systems and software. ITD will audit and monitor the use of the equipment and access to information.

1. Only Authorized Users Operating Authorized Devices May Access the Seattle Police Department's Computer Network

Employees will access the SPD network only with devices authorized by ITD.

- This requirement includes devices used by other agencies assisting SPD or vendors working with ITD.

2. ITD Controls Department-Owned Software

ITD will review and evaluate purchases of computer and device software. ITD will approve or reject the purchase of software based on internal policies and the City's ITD guidelines.

ITD will maintain the software licenses for Department-owned software.

3. ITD Monitors Software Use on Department Devices

ITD will audit the software used on Department computers and will remove unauthorized software.

4. Employees Will Not Violate the License Agreement of Department Software

Employees will not copy Department-owned software or install the software on any other computer.

5. Employees Will Not Install or Download Non-Department- Owned Software, Applications or Programs on Department Devices

6. With Approval from their Lieutenant/Civilian Equivalent or Above, Employees May Request New Applications and Software (including free technologies) by Completing the SPD Change or Enhancement Intake Request Form

This form is required for all requests to change any kind of IT system.

This includes, but is not limited to changes in hardware, network connections, addition or removal of applications, and additions or changes in application configurations, data elements, check lists, and drop down lists

The link to this form can be found below See 12.040-TSK-1 Submitting a Request for Change or Enhancement Intake Request

- Non-Department-owned software cannot interfere with the operation of any Department-owned software or hardware.

- The unit assigned the software will maintain the license agreement. A copy of the license agreement is sent to ITD by the unit.

7.Employees Will Report Malfunctions of IT, Systems or Software By Calling the Seattle ITD Service Desk at 4-HELP to Complete a HEAT Ticket

Seattle ITD (previously known as DoIT help desk) is available M-F, 8-5 for routine desktop equipment or software related issues. Seattle ITD can be reached via telephone at 4-HELP or 386-4011, or via e-mail at 4-Help@seattle.gov.

After hours assistance can also be requested via 4-HELP or 386-4011. After hours requests are handled by the on duty Seattle ITD personnel.

Seattle ITD assistance via SPD Radio is also available 24/7 via Zone 2 / ITS. This resource is for in-car equipment issues related to the VMDT. Assistance is also provided to patrol officers that need a password reset to complete their patrol related tasks.

8. Employees Will Not Use Unauthorized Encryption Tools on a Department Computer or Device

9. Employees Will Not Password-Protect a Work File or Hard Drive

Exception: A lieutenant or above may authorize an employee to password-protect a file or drive based on an investigative or operational need.

Exception: This does not apply to Department-required passwords for Department computers, programs or devices.

12.040 - POL-3-Using Department Devices

1. Employees Have No Expectation of Privacy When Using a Department Device

The Department has the right to review all records related to department devices including, but not limited to phone logs, text messages, photographs, email and internet usage.

2. Employees Use Devices in a Professional Manner

Employees will use Department devices to communicate in a professional, appropriate, and lawful manner both on and off-duty.

Employees are accountable for all transmissions made on department devices.

3. Personal Use of Department-Provided Devices Must Follow Department Guidelines

The Department allows limited, reasonable, personal use of Department devices with the knowledge that all use of Department devices may be monitored and subject to public disclosure.

Personal use of Department devices must not:

- Be illegal,
- Incur a cost to the City,
- Interfere with work responsibilities,
- Disrupt the workplace,
- Store unlicensed, copyrighted materials on any City-owned technology,
- Create a device-to-device connection between Non-City owned Technology and City-owned Technology,
- Comprise commercial or solicitation activities,

Or,

- Cause an embarrassment to the Department.

The Department may monitor and review all use of Department devices.

4. Department Devices Equipped with the VMobile Application Must Be Password Protected

Any use of the VMobile application must comply with Manual Section 12.050 - Criminal Justice Information Systems.

5. Employees Will Report Lost or Stolen Department Devices

In the event of a lost or stolen Department-issued device, the employee assigned the device must comply with 9.030-PRO-1 Reporting Destroyed, Lost, or Stolen Equipment.

6. Employees Will Not Access the VMobile Application in an Off-Duty, Unofficial Department Capacity

Off-duty use must comply with Manual Section 12.050 - Criminal Justice Information Systems.

7. The Act of Carrying a Department Device While Off-Duty Does Not, In Itself, Constitute Overtime

Overtime expectations vary by assignment. Supervisors will clarify their expectations for any off-duty use of Department devices. Unless an employee has been explicitly ordered by a supervisor to be available, check emails, or conduct other department business outside of normal shift hours, they are not expected or encouraged to do so.

See Manual Section 4.020-Reporting and Recording Overtime/Out-of-classification Pay

8. The Fiscal Unit Assists Employees with Cellular Phones

Employees making a request for a new or replacement cell phone will submit a 1.5 through their chain of command. Once approved, the Fiscal Unit will order the new phone and service.

9. The Department Telephone Coordinator Assists Employees with Desktop (Land-Line) Phones

Employees may contact the Telephone Coordinator at spd_telephone_coord@seattle.gov The Telephone Coordinator can assist employees in the acquisition of phones and moving phone numbers to new locations.

Section Captain or civilian equivalent will approve the acquisition or moving of desk phones.

10. Employees Will Not Use Department Devices Internationally Without the Approval of a Captain/Civilian Equivalent or Above

After captain or civilian equivalent approval, employees will contact ITD to upgrade their device plan for international use.

International travel with a Department device may incur roaming charges to the Department.

11. Employees Will Comply with All Department Public Disclosure Requests

See Manual Section 12.080 Department Records Access, Inspection and Dissemination.

12. When Receiving a Public Disclosure Request or Subpoena, Employees Must Retain All Requested Content

Employees will not delete requested items after receiving a public disclosure request or subpoena.

Department personnel may review content of any messages or photos contained on the device to make informed disclosure decisions.

13. Employees Will Retain Public Records According to the City Records Management Program

This includes, but is not limited to text messages and photographs.

Employees seeking long-term retention may elect to transfer the content from the device to an appropriate Department network or system.

14. Employees Will Hold and Preserve All Public Records Relating to Litigation or Anticipated Litigation

Employees will hold and preserve all requested records until the City Attorney's Office releases the legal hold.

Employees will retain all records, including transitory records, responsive to a pending public records request until the Department's response to the request has been completed.

15. Employees Acknowledge that Public Disclosure Laws Apply to Personally Owned Devices Used for Department Business

Employees using their personally-owned devices for official Department business and correspondence do so with the knowledge of this admonishment.

The Department prefers employees use Department-provided devices for Department-related matters.

Employees may request that their supervisor provide a Department-owned phone to make phone calls for official business.

16. The Department May Request Employees Review Their Own Personal Devices in Compliance with Public Disclosure Requests

The employee may be required to sign a declaration demonstrating the adequacy of the search of a personal cellphone or device regardless of whether the search resulted in responsive records.

Employees with questions regarding public disclosure may contact the Legal Unit.

17. Employees Will Not Charge Personally Owned Devices in Department USB Ports

Vehicle USB ports and USB ports that connect to a device may retain data from a personally owned device when plugged in.

Employees may use wall outlets or vehicle 12-volt DC sockets to charge personal devices.

12.040-TSK-1 Employees Submitting a Request for Change or Enhancement Intake Request

1. **Requests** approval for change via their chain of command to the level of Lieutenant/civilian equivalent or above

2. **Receives** approval for the request via their chain of command

3. **Clicks** here to complete an SPD Change or Enhancement Intake Form

4. **Completes** the fillable PDF form

5. **Clicks the "Click to Submit Form" button** on the request form PDF. An outlook email will automatically open.

6. **Selects** Default email application (Microsoft Outlook)

7. **Clicks Continue**

When the Outlook email opens, it auto-populates the email recipient as SPD_ChangeRequest@Seattle.gov. It will also automatically attach your completed PDF change request and auto-populate the subject line as "Form Returned: SPD_ChangeRequest.pdf"

8. **CCs** their approving chain of command within the email request and **clicks send** to forward your email change request to ChangeRequest@Seattle.gov.

Site Disclaimer: The Seattle Police Department's website was developed to provide general information. Data contained at this location is generally not reviewed for legal sufficiency. SPD documents displayed are for reference purposes only. Their completeness or currency are not guaranteed. Links or references to other information or organizations are for reference only and do not constitute an endorsement.

ADA Notice

Notice of Nondiscrimination

Privacy

© Copyright 1995-2018 City of Seattle

Seattle Police Department Manual
Carmen Best, Chief of Police

12.050 - CRIMINAL JUSTICE INFORMATION SYSTEMS

Effective Date: 05/01/2017

Criminal Justice Information Services Security Policy

WSP ACCESS/WACIC/NCIC/User Acknowledgement

1. Definitions

Criminal History Record Information: Information contained in records collected by criminal justice agencies, other than courts, on individuals, consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition arising there from, including sentences, correctional supervision, and release. The term includes information contained in records maintained by or obtained from criminal justice agencies, other than courts, which records provide individual identification of a person together with any portion of the individual's record of involvement in the criminal justice system as an alleged or convicted offender, except:

- Posters, announcements, or lists for identifying or apprehending fugitives or wanted persons,
- Original records of entry maintained by criminal justice agencies to the extent that such records are compiled and maintained chronologically and are accessible only on a chronological basis,
- Court indices and records of public judicial proceedings, court decisions, and opinions, and information disclosed during public judicial proceedings, and
- Records of traffic violations that are not punishable by a maximum term of imprisonment of more than ninety days.

For the purposes of this policy, the RideAlong Response application is considered a criminal justice record system that contains criminal history record information.

Dissemination: Disclosing criminal history record information, or the absence of criminal history record information, to any person or agency outside the agency possessing the information, subject to the following exceptions:

- Agencies participating in a single (joint) record-keeping department,
- Furnishing information to process a matter through the criminal justice system (information to a prosecutor), and
- Reporting events to a record-keeping agency.

NCIC III: The National Crime Information Center Interstate Identification Index, managed by the FBI and state law enforcement agencies. The NCIC Advisory Policy Board has established a set of standards and goals that the FBI and state agencies enforce. The information contained in the NCIC includes all records collected by criminal justice agencies on individuals including identifiable descriptions, notations of arrests, detentions, indictments, formal criminal charges, dispositions, sentences, correctional supervision, and release. Federal, state and local laws and regulations dictate that this information is to

be accessed and used only by authorized individuals within a criminal justice agency, that this information is to be used for criminal justice reasons, that this information is to be kept confidential, and that this information is to be stored in a secure location.

- Employees must be working for the Seattle Police Department in an on-duty or extra-duty capacity and investigating a criminal offense.

- Employees shall not run names or make inquiries through NCIC III, or any other criminal record system while working for an off-duty employer or on behalf of an off-duty employer.

2. Inquiries Through ACCESS, or Any Other Criminal Justice Record System, Are Only to Be Made for Legitimate Law Enforcement Purposes

This includes, but is not limited to, inquiries made to DOL, DOC, WACIC, WASIS, NCIC III, LInX, and any inquiries processed through NLETS to other states. Inquiries made for personal use, or inappropriate use or dissemination of the information, can result in internal discipline, as well as penalties under Federal and State law.

3. All Employees Who Use Terminals That Have Access to Information in WACIC/NCIC Files Must Be Certified

After initial certification, employees shall take a recertification test every two years.

- For inquiries only, employees shall attain Level I certification.

- If employees make data entries into the system, they shall attain Level II certification.

4. SPD Must Remain in Compliance With the ACCESS/WACIC/NCIC User Acknowledgement or Risk Termination of One or More of the Services Provided

The ACCESS/WACIC/NCIC User Acknowledgement is the formal agreement between WSP and SPD. This document acknowledges the standards established in the FBI's Criminal Justice Information Service Security Policy. The standards require accuracy, completeness, timeliness, and security in the dissemination and recording of information.

5. Data Center Manager is the Technical Agency Coordinator

The Department must designate a Technical Agency Coordinator (TAC) to act as the point of contact for the WSP and the Federal Bureau of Investigation (FBI). The individual designated to function as a TAC will be responsible to ensure compliance with state and National Crime Information Center (NCIC) policies and regulations. The TAC must maintain a Level II training certification and attend TAC training once every three years. Additionally, the TAC shall participate in and ensure that all appropriate records be available during the triennial audit conducted by the ACCESS audit staff. Responsibility for proper operator performance, strict adherence to regulations, prompt notification of CJIS violations to the ACCESS Section, and subsequent training rests with the TAC. The SPD TAC is the Data Center Manager.

6. All Employees Shall Adhere to WASIS and NCIC Policies

Use of WASIS (Washington State Identification System and Criminal History Section) and NCIC Interstate Identification Index (NCIC III) is regulated by the FBI and WSP in accordance with the 28 CFR Part 20, WAC 446-20-260, and RCW Chapter 10.97. Improper use of the system may result in severe penalties to the Department and the individual user.

All employees shall adhere to the following WASIS and NCIC policies:

1. Any information obtained through these systems shall not be disseminated to anyone outside the Department, except to a prosecutor. If necessary, officers may confirm to a criminal justice agency the WASIS or FBI number, if it is known.

a. Examples of agencies and/or organizations to whom we cannot release criminal history information include, DSHS, Passport Agencies, CPS, Adult Protective Services, Crimestoppers, victims, and witnesses.

b. Inquiries for criminal history information from outside agencies, organizations, and individuals should be referred to Washington State Patrol.

2. Inquiries into these systems shall not be made in response to a request by another criminal justice agency or by any retired employees, including those holding any extended authority, special police commission, or similar police commission.

3. The Department of Justice Criminal Justice Information System (CJIS) restricts the use of all criminal-related data bases to official investigations when conducted while working for a criminal justice organization. As a result, no employee shall run names or make inquiries through ACCESS, WACIC, WASIS, NCIC III, LInX, or any other criminal record system while working for an off-duty employer or on behalf of an off-duty employer.

4. All NCIC III queries made through Versadex are stored in the system. A program has been developed to create an automated user log from that data.

5. This log is audited by the Washington State Patrol, the FBI, and the Compliance Section, and shall be available for inspection by any of the agencies at any time. The following procedures must be followed when accessing the Criminal History Database:

a. All NCIC III queries should be made using Transaction Code CQCH – Common Query Criminal History

b. The Purpose Code box must be filled in with 1 of the 2 authorized Purpose Codes that appear in the pull-down. The query will not go through if the box is left blank. The only authorized Purpose Codes are:

C - Criminal Justice purposes as well as authorized uses in relation to the security of the criminal justice facility including, vendors/contractors who are not involved with administration of criminal justice; e.g. janitors, maintenance personnel, visitors, etc.

J – Criminal Justice employment/applicants and re-background requirement for criminal justice agency personnel as well as vendors, contractors, volunteers, and interns, who are involved with the administration of criminal justice for the agency.

c. The Reason field must be filled in with a specific criminal justice reason. The general offense number should always be listed in the reason field if available. If a general offense number has not been generated the specific criminal justice reason must be listed in the reason field such as theft, narcotics, homicide, missing person, or criminal justice applicant. Listing terms such as investigation, arrest, criminal history, or employment in the reason field are not valid. Listing abbreviations of any kind in the reason field is not authorized unless the abbreviation has been approved and is on file with the department TAC.

6. An automated user log for all queries made using the Omnixx system is maintained by the Washington State Patrol. Data Center and Public Request Unit Personnel may request access to this log via the "Request for Off-Line Search." The following information must be included in the Attention Field (ATN) when making a criminal history inquiry using Omnixx:

a. Requestor's SPD serial number.

b. Specific criminal justice reason such as theft, narcotics, homicide, or general offense number.

c. Examples:

ATN/4000 WP Entry

ATN/4000 Burglary

ATN/4000 14-16735

d. Use of abbreviations is acceptable but must be on file and approved by the Department TAC.

e. The proper purpose code must be used for all inquiries.

7. The NCIC III system is to only be used by personnel involved in criminal investigations, and background investigations. As of 2/11/15, a NICS check will be required for firearms returns. The Public Request Unit is the only unit authorized to complete NICS checks.

8. MDCs and PDTs (mobile and portable data computers/terminals) are not authorized to access NCIC III information because the terminals are unable to comply with NCIC audit requirements.

9. It is important to enter inquiries to the Criminal History Records system properly. The following information must be accurate and complete on the inquiry mask:

a. The "Purpose Code" must be entered correctly, "C", for criminal investigation, or another appropriate code. See NCIC manual for details.

b. The "Requestor Full Name/Serial" must contain the name and SPD serial number of the person making the inquiry. It is not acceptable to use "Det", "Off", or the "unit title" in this field.

7. Employees Shall Not Discuss or Provide Information to Any Person Who Is Not a Member of the Criminal Justice System Without the Permission of the Chief of Police, or By Due Process of Law

The Washington State Criminal Records Privacy Act (RCW 10.97) provides for the completeness, accuracy, confidentiality, and security of criminal history record information, as well as victim, witness, and complainant record information. Employees shall not discuss or provide information to any person who is not a member of the criminal justice system (prosecuting attorney, court, etc.) without the permission of the Chief of Police, or by due process of law. Violations may lead to criminal sanctions.

8. Criminal Records Releases Are Restricted

Requests for information shall be referred to the appropriate section.

- Criminal history record information dissemination to individuals, agencies, or groups outside the Department shall be administered by the Records File Unit and Data Center Unit.

- Juvenile record information dissemination to individuals, agencies, or groups outside the Department shall be administered by the Records File Unit.

Printouts of criminal history record information from the Department's computerized and manual files are prohibited except when:

- Required for a detective investigative file
- Required by a prosecuting attorney
- Required by agencies or individuals authorized by the Records, Evidence and Identification Section access procedures
- Required in a mutual criminal investigation with a court or government agency authorized by the Washington State Patrol to receive criminal history record information
    - The Records File Unit and Data Center Unit shall maintain a current list of agencies so authorized.
- Authorized by a watch, section, or unit supervisor as required for an investigation or in an emergency

When releasing criminal history information to a prosecutor the release tracking function in Versadex should always be used to indicate release to either King County Prosecutor's Office or the City Law Department. The release tracking serves as the automated secondary dissemination log.

In authorized instances when criminal history is secondarily disseminated to any agency or person the following information relating to secondary dissemination of criminal history record information shall be maintained by the appropriate section in the form of a manual log and will include the following:

- An indication of to whom (agency or person) criminal history information was released,
- The date of release, and
- A brief description of the information released

The disposal of printouts from computer terminals shall be by destruction.

9. Individuals Have the Right to Inspect and Review Their Criminal History Record Information Maintained By the Department

A copy of the Department Operating Instruction titled, "Inspection and Review of Criminal History Record Information" and "Challenge and Deletion of Criminal History Record Information" shall be maintained at locations where the public can make inquiries concerning Department procedures.

An individual's right to access and review of their criminal history record information shall not extend to data contained in intelligence, investigative, or other related files and shall not be construed to include any information other than that defined as Criminal History Record Information by RCW 10.97.030.

In order to inspect, review, or challenge and have deleted criminal history record information, the individual must appear in person at the 1st floor of the Police Headquarters Building 610 Fifth Avenue, Monday through Thursday (excluding holidays) between the hours of 8:00 a.m. and 4:30 p.m., and make a request in writing on the forms provided.

- Employees are responsible for directing individuals to the Records File Unit in order to facilitate review of their criminal history record information.

An individual will be provided an opportunity, following review of the criminal history record information collected, stored, and maintained by the Department, to challenge the accuracy and completeness of the data and request deletion of certain non-conviction arrests.

If the challenge is rejected, the individual has a right to appeal the decision to the Office of the Chief of Police.

It shall be the duty of the Records File Unit manager and supervisors to administer the rules pertaining to an individual's right to review their criminal history record information, concurrent with the aforementioned laws, regulations, and ordinances.

10. All SPD Personnel Must Have a Background Re-Investigation Every Five Years

To complete this compliance measure the Department must:

- Run a criminal history inquiry using purpose code "J". Use "Criminal Justice Re-background" as a reason. Log the date and SID# of the employee. Do not retain rap sheet information.

  - If there are felony findings within the employee's rap sheet they will be denied continued use and certification with ACCESS. The TAC must notify the WSP Information Security Officer of any findings.

  - If there are charges pending a disposition, the TAC must notify the WSP Information Security Officer (ISO).

  - If there are misdemeanor findings the TAC shall notify the WSP Information Security Officer. The Seattle Police Department will ultimately decide whether to limit ACCESS.

  - Keep a log of all personnel SID numbers and the date of the background re-investigation for future ACCESS audits.

11. SPD Must Comply With ACCESS/NCIC Security Requirements

All upper management and administrators/managers who are not ACCESS-certified but oversee certified ACCESS users must review the Upper Management and Administrator Overview Training. Upon review of the training, they must sign the Upper Management and Administrator Log. There is no requirement to reaffirm this training.

All employees must complete the Security Awareness Training within six months of initial hire. Any employee not Level I or Level II-certified must review the Security Awareness Training every two years.

Maintaining security of the terminal sites and information received is the responsibility of agency personnel operating the terminal, the TAC, and the agency head. Terminal locations must be secure from authorized access, and all employees authorized to use the system shall be instructed on the proper use of equipment and the dissemination of information received. Federal and state laws protect the information provided by ACCESS.

Violations of the rules, regulations, policies, or procedures developed by FBI and adopted by the WSP or any other misuse or abuse of the ACCESS system may result in agency disciplinary measures and/or criminal prosecution. Disciplinary measures imposed by the WSP may include revocation of individual certification, discontinuance of system access to the department, or purging the department's records.

Any misuse of the NCIC III system must be reported to the TAC (Data Center Manager) immediately. The TAC shall report the misuse to the Washington State Patrol and the FBI. The violator's chain of command will be notified of the misuse.

12. The Captain of the Compliance Section Will Assign Personnel to Conduct Regular Audits of the Department's Criminal History Records Inquiries

The Department audits will be completed biannually and the results of these audits will be reported to

the Chief Operating Officer.

The audit will look for any violations of the CJIS Security Policy, The WSP User Acknowledgement, and Department Policy. Violations include but are not limited to:

- Queries made for personal reasons
- Reason Field errors, such as using general terms such as investigation, arrest, warrant, criminal history
    - The Reason Field must contain a specific crime such as murder, assault, burglary.

Any users who are in violation of any or all of the above will have their access to the Criminal History system shut off. Access will be denied until they have attended a remedial class for making Criminal History inquiries.

- An e-mail will be sent to the employee and their immediate supervisor from the Compliance Section Captain that their access to the Criminal History system has been denied.
- The e-mail will contain information about the remedial classes that they must take in order to regain access.
- A copy of the e-mail will be sent to the Data Center Manager/TAC for implementation.

Site Disclaimer: The Seattle Police Department's website was developed to provide general information. Data contained at this location is generally not reviewed for legal sufficiency. SPD documents displayed are for reference purposes only. Their completeness or currency are not guaranteed. Links or references to other information or organizations are for reference only and do not constitute an endorsement.

ADA Notice

Notice of Nondiscrimination

Privacy

© Copyright 1995-2018 City of Seattle

Seattle Police Department Manual

Carmen Best, Chief of Police

12.055 - CRIMINAL JUSTICE RESEARCH

Effective Date: 8/15/2012

12.055–POL

This policy pertains to the Department's facilitation of research.

1. The Department Encourages Criminal Justice Research and will Facilitate Research as Allowed by Law and Available Resources

The Department may permit researchers to have direct access to police files and/or personnel under properly executed research and confidentiality agreements.

- The Chief of Staff will have final approval over outside research requests.
- A written Research Agreement is required for the release of any Department data for research, evaluative or statistical purposes.
- Research requests for criminal history shall comply with WAC 446-20-420.

2. Agencies, Institutions and Individuals Desiring the Use of Police Records for Research will Use the Seattle Police Department Research Request Instructions as a Guide to Complete a Request

Click here for instructions.

3. The Compliance Section will Receive and Vet all Outside Research Requests

See 12.055–PRO–1 Vetting Process for Outside Research Requests

The following questions will be considered when requests are analyzed:

- Is the information requested available?
- What is the estimated cost to complete the request?
- Personnel time
- File research
- Copying
- Can the additional workload required to complete the request be absorbed at the time it is requested?
- How will the completed research project be beneficial to the Department or to the criminal justice system?
- Are there privacy issues?
- Does the request comply with RCW 13.50.010?

4. Costs Shall be Forwarded to the Fiscal Section for Billing and Reimbursement

5. Department Employees are Encouraged to Submit Their Own Ideas for Research Topics

See 12.055–PRO–2 Receiving Internal Ideas for Research Topics

The Compliance Section Captain will maintain a list of research topics for assignment within the SPD-University of Washington Research Consortium.

6. The Compliance Section will Review Results of Completed Research and Determine if There is a Practical Application to Department Operations

12.055–PRO–1 Vetting Process for Outside Research Requests

Compliance Section Captain

1. **Receives** outside research request

Assigned Compliance Section Staff:

2. **Reviews** request
3. **Prepares** recommendation on how to proceed
4. **Shares** recommendation with work group (Compliance Section Sergeant, legal advisors, Records Manager, and Grants and Contracts Manager).

Work Group

5. **Reviews** the recommendation

Assigned Compliance Section Staff

6. **Schedules** a meeting with the work group and the Compliance Section Captain
   a. The chief or captain of the Bureau or Section which will benefit from, or be affected by, the research project may also be included.

Compliance Section Captain

7. **Determines** whether Compliance Section will endorse the request
   a. If Compliance Section will not endorse, then advises the work group
   b. If Compliance Section will endorse, then forwards the request to the Chief of Staff

Chief of Staff

8. **Determines** whether SPD will endorse the request
   a. If SPD will endorse, signs research agreement on behalf of the Department

Assigned Compliance Section Staff

9. **Advises** requester of the Department's decision via formal letter

12.055–PRO–2 Receiving Internal Ideas for Research Topics

Any SPD employee

1. **Develops** an idea for a research topic
2. **Submits** an e-mail to the Compliance Section, with the subject line: Research Topic

Assigned Compliance Section Staff

3. **Reviews** the memo
4. **Develops** a specific research topic
5. **Follows-up** with the employee
    a. **Verifies** that his research topic is consistent with the employee's intent
6. **Submits** research topic to Compliance Section Captain

Compliance Section Captain

7. **Maintains** file of research topics

Site Disclaimer: The Seattle Police Department's website was developed to provide general information. Data contained at this location is generally not reviewed for legal sufficiency. SPD documents displayed are for reference purposes only. Their completeness or currency are not guaranteed. Links or references to other information or organizations are for reference only and do not constitute an endorsement.

ADA Notice

Notice of Nondiscrimination

Privacy

© Copyright 1995-2018 City of Seattle

Seattle Police Department Manual

Carmen Best, Chief of Police

12.080 - DEPARTMENT RECORDS ACCESS, INSPECTION & DISSEMINATION

Effective Date: 11/20/2013

12.080-POL

This policy applies to access, inspection and dissemination of Department records.

1. All Records are Subject to Public Disclosure Unless a Specific Legal Exemption Exists

Per RCW 42.56.070, the Department must make all public records available to a requester, unless the record falls within the specific exemptions in the Public Records Act (PRA) or other statute which exempts or prohibits disclosure of specific information or records.

2. Public Records are Available for Release to the Maximum Extent Allowed by Law

A public record is any writing containing information relating to the conduct of the Department or the performance of any governmental or proprietary function prepared, owned, used, or retained by the Department, regardless of physical form or characteristics.

- Public records may include records received or created that relate to the conduct of the Department or the performance of any governmental or proprietary function and are prepared, owned, used, or retained by the Department.
- The Department frequently receives records from outside agencies. Any and all records that are in the Department's possession are Department records for the purposes of PRA.
- Writing means handwriting, typewriting, printing, photostating, photographing, and every other means of recording any form of communication or representation, including, but not limited to, letters, words, pictures, sounds, symbols, or combination thereof, and all papers, maps, magnetic or paper tapes, photographic films and prints, motion picture, film and video recordings, magnetic or punched cards, discs, drums, diskettes, sound recordings, and other documents including existing data compilations from which information may be obtained or translated.

Under RCW 42.56 Public Records Act (PRA) as interpreted by Washington courts, all Department records must be identified to the public, so long as the records are not part of an open and active investigation.

Exception: Department records that fall under a specific exemption within the PRA or other statute are not required to be identified to the public. Specific exemptions include, but are not limited to, public safety considerations and privacy concerns.

- The Department cannot withhold an entire record because portions of it fall under an exemption. The Department shall redact exempted information and release the record with an explanation for any redactions.

3. All Records That Relate to a Public Disclosure Request (PDR) Must Be Provided or Identified to the Public Disclosure Unit (PDU)

If an employee withholds known records that relate to a PDR, he or she may be subject to civil liability and/or Department discipline.

- Employees are advised to contact PDU (684-4848 or spdpdr@seattle.gov) when they are uncertain as to whether documents that they have constitute records that relate to a PDR.

4. Officers/Detectives Must Ask Victims, Witnesses and Complainants if They Want Their Identifying Information Disclosed or Not Disclosed

When gathering information at the time of reporting, officers and detectives must ask victims, witnesses and complainants if they want their identifying information disclosed or not disclosed. This decision supersedes any disclosure requests made by another person.

- When a victim, witness or complainant is unable to discuss disclosure due to incapacity, the reporting officer shall:
- Document the incapacity in the entity portion of the General Offense Report, and
- Document any specific evidence that disclosure of the identity of the victim, witness or complainant would threaten life, safety or property.

5. PDU Responds to PDRs

The Public Disclosure Unit (PDU) handles all public disclosure requests (PDRs) in accordance with the Public Records Act (PRA). See 12.080-PRO-1 Handling Public Disclosure Requests.

- Any Department employee who receives a PDR, or any request that appears to be a PDR, shall immediately forward it to spdpdr@seattle.gov.
- The request does not have to cite the PRA.

There are four options for member of the public to submit PDRs:

- E-mail: spdpdr@seattle.gov (preferred method)
- Mail: SPD PDU; PO Box 34986; 610 5th Ave; Seattle, WA 98124-4986
- Fax: (206) 684-5240
- In-person at the public counter at SPD Headquarters, 610 5th Ave.

6. Public Request Unit (PRU) Responds to Certain Requests

The PRU handles the following:

- Requests for police reports
- Requests for clearance letters
- Fingerprinting and criminal background checks on applicants for concealed pistol licenses
- Fingerprinting criminal justice applicants
- Fingerprinting citizens for general purposes
- Processing applications for transferring ownership of handguns
- Electronically redacting police reports for release to the SPD My Neighborhood Map website

7. Crime Records Unit (CRU) Responds to Certain Requests

The CRU receives and records all incoming requests for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies.

8. The Public Disclosure Request Steering Committee Resolves Complex PDR

The PDR Steering Committee, which meets each Monday, is comprised of the Chief Administrative Officer, PDU Manager and staff, Records Manager, SPD Legal Advisor, Compliance Section Captain or designee, and one or more representatives of the Seattle Law Department.

See 12.080-PRO-1 Handling Public Disclosure Requests.

12.080-PRO-1 Handling Public Disclosure Requests

PDU

1. **Receives** PDR
2. **Contacts** relevant units or specific employees to **request** records and **provides** a due date

Relevant Unit/Employee

3. **Gathers** all relevant records and **contacts** PDU with any questions

   a. If an employee believes that some or all of the information in the record(s) is protected from public disclosure, **provides** the record(s) to the PDU, with a memo stating what should be protected and why

   b. Whether the record(s) at issue is protected from public disclosure shall be discussed at the next meeting of the PDR Steering Committee

   - Absent conflicting advice from the Law Department and the SPD Legal Advisor, the Chief Administrative Officer shall determine whether record(s) will be disclosed wholly or in part, and whether any exemptions apply.
   - When there is conflicting advice from legal counsel, the issue shall be elevated to the Chief of Staff and the Law Department's Chief of the Civil Division for resolution.

4. **Provides** records to PDU by the due date

PDU

5. **Collects** records and **makes** any and all necessary redactions
6. **Provides** records to the requestor

Site Disclaimer: The Seattle Police Department's website was developed to provide general information. Data contained at this location is generally not reviewed for legal sufficiency. SPD documents displayed are for reference purposes only. Their completeness or currency are not guaranteed. Links or references to other information or organizations are for reference only and do not constitute an endorsement.

ADA Notice

Notice of Nondiscrimination

Privacy

© Copyright 1995-2018 City of Seattle

Seattle Police Department Manual
Carmen Best, Chief of Police

12.111 - USE OF CLOUD STORAGE SERVICES

Effective Date: 03/01/17

12.111-POL

The Seattle Police Department receives information from the FBI's Criminal Justice Information Service (CJIS) and must comply with the CJIS security policy and the rules governing the access, use, and dissemination of CJIS information found in Title 28, Part 20, CFR

SPD employees deal with CJIS data as part of daily Department business. This policy applies to employee use of cloud storage services as a whole and as it specifically relates to CJIS data.

1. Definitions

Cloud storage services are electronic, external storage locations where information can be deposited for shared use. Examples include OneDrive, DropBox, Google Drive, iCloud, etc.

Criminal Justice Information (CJI) is the term used to refer to all of the FBI provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

Personally Identifiable Information (PII) a subset of CJI, is information which can be used to distinguish or trace an individual's identity, such as name, social security number, biometric records, date and place of birth, or mother's maiden name.

Criminal History Record Information (CHRI), sometimes informally referred to as "restricted data", is also subset of CJI.

Restricted Files are hosted by the National Crime Information Center (NCIC) and are treated as CHRI. Restricted Files include the following:

- Gang Files
- Known or Appropriately Suspected Terrorist Files
- Supervised Release Files
- National Sex Offender Registry Files
- Historical Protection Order Files of the NCIC
- Identity Theft Files
- Protective Interest Files
- Person With Information (PWI) data in the Missing Person Files
- Violent Person File
- NICS Denied Transactions File

2. Employees May Only Store, Edit, and Share City Files on Cloud Storage Services Provided By the Department or the City

Employees may store, edit, and share files on city-provided cloud storage such as Microsoft Office 365's OneDrive.

Employees will not use personal cloud storage services, such as Drop Box Google Drive, and iCloud, for any city file.

Site Disclaimer: The Seattle Police Department's website was developed to provide general information. Data contained at this location is generally not reviewed for legal sufficiency. SPD documents displayed are for reference purposes only. Their completeness or currency are not guaranteed. Links or references to other information or organizations are for reference only and do not constitute an endorsement.

ADA Notice

Notice of Nondiscrimination

Privacy

© Copyright 1995-2018 City of Seattle

Seattle Police Department Manual

Carmen Best, Chief of Police

16.170 - AUTOMATIC LICENSE PLATE READERS

Effective Date: 8/15/2012

16.170-POL

This policy applies to the use of automatic license plate readers (ALPR) by Department employees.

1. Criminal Intelligence Section has Operational Control

The ALPR system administrator will be a member of the Technical and Electronic Support Unit (TESU).

2. Operators Must be Trained

Operators must be ACCESS certified and trained in the proper use of ALPR.

- Training will be administered by TESU and Parking Enforcement, as applicable.

3. ALPR Operation Shall be for Official Department Purposes

ALPR may be used during routine patrol or any criminal investigation.

4. Only Employees With ACCESS Level 1 Certification May Access ALPR Data

Employees are permitted to access ALPR data only when the data relates to a specific criminal investigation.

- A record of requests to review stored ALPR data will be maintained by TESU.

Site Disclaimer: The Seattle Police Department's website was developed to provide general information. Data contained at this location is generally not reviewed for legal sufficiency. SPD documents displayed are for reference purposes only. Their completeness or currency are not guaranteed. Links or references to other information or organizations are for reference only and do not constitute an endorsement.

ADA Notice

Notice of Nondiscrimination

Privacy

© Copyright 1995-2018 City of Seattle

Part 3 - ENFORCEMENT

Chapter 11.30 - IMPOUNDING

Sections:

11.30.010 - Impoundment defined.

"Impoundment" means removal of a vehicle to a storage facility either by an officer or authorized agent of the Seattle Police Department or by a contractor for towing and storage in response to a request from an officer or authorized agent of the Seattle Police Department or the Seattle Housing Authority.

(Ord. 117306 § 1, 1994: Ord. 108200 , § 2(11.30.010), 1979.)

11.30.020 - Vehicle defined.

The term "vehicle" as used in this chapter shall have the definition set forth in Section 11.14.710 and, in addition, shall include any vehicle hulk as the same is defined in Section 11.14.045.

(Ord. 108200 , § 2(11.30.020), 1979.)

11.30.030 - Applicable State law adopted by reference.

Applicable provisions of Chapter 46.55 RCW, as now or hereafter amended, are hereby incorporated into Seattle Municipal Code Chapter 11.30 by this reference.

(Ord. 117306 § 2, 1994.)

11.30.040 - When a vehicle may be impounded without prior notice.

A. A vehicle may be impounded with or without citation and without giving prior notice to its owner as required in Section 11.30.060 hereof only under the following circumstances:

1. When the vehicle is impeding or is likely to impede the normal flow of vehicular or pedestrian traffic; or
2. When the vehicle is illegally occupying a truck, commercial load zone, restricted parking zone, bus, loading, hooded-meter, taxi, street construction or maintenance, or other similar zone where, by order of the Director of Transportation or Chiefs of Police or Fire or their designees, parking is limited to designated classes of vehicles or is prohibited during certain hours, on designated days or at all times, if the zone has been established with signage for at least twenty-four (24) hours giving notice that a vehicle will be removed if illegally parked in the zone and where such vehicle is interfering with the proper and intended use of such zones; or
3. When a vehicle without a special license plate, card, or decal indicating that the vehicle is being used to transport a disabled person as defined under Chapter 46.16 RCW, as now or hereafter amended, is parked in a stall or space clearly and conspicuously marked as provided in Section 11.72.065 A, as now or hereafter amended, whether the space is provided on private property without charge or on public property; or
4. When the vehicle poses an immediate danger to the public safety; or
5. When a police officer has probable cause to believe that the vehicle is stolen; or

6. When a police officer has probable cause to believe that the vehicle constitutes evidence of a crime or contains evidence of a crime, if impoundment is reasonably necessary in such instance to obtain or preserve such evidence; or

7. When a vehicle is parked in a public right-of-way or on other publicly owned or controlled property and there are four or more parking infractions issued against the vehicle for each of which a person has failed to respond, failed to appear at a requested hearing, or failed to pay a parking infraction for at least 45 days from the date of the filing of the notice of infraction;

8. When the vehicle is a "junk motor vehicle" as defined in SMC 11.14.268, and is parked on a street, alley, or way open to the public, or on municipal or other public property.

9. When the vehicle is impounded pursuant to Section 11.30.105A, but if the vehicle is a commercial vehicle and the driver is not the registered owner of the vehicle, then the police officer shall attempt in a reasonable and timely manner to contact the registered owner before impounding the vehicle and may release the vehicle to the registered owner if the registered owner is reasonably available, was not in the vehicle at the time it was stopped and the driver arrested, and has not received a prior release under this Subsection 11.30.040 A9 or Subsection 11.30.120 C2.

10. When a vehicle with an expired registration of more than forty-five days is parked on a public street.

11. When the vehicle is impounded pursuant to Section 12A.10.115.

12. When the vehicle is impounded pursuant to Washington Laws of 2011, chapter 167, section 3.

B. Nothing in this section shall be construed to authorize seizure of a vehicle without a warrant where a warrant would otherwise be required.

(Ord. 123632, § 9, 2011; Ord. 123447, § 2, 2010; Ord. 123190, § 8, 2009; Ord. 123035, § 3, 2009; Ord. 121525 § 4, 2004; Ord. 120102 § 1, 2000; Ord. 119782 § 1, 1999; Ord. 119180 § 3, 1998; Ord. 117306 § 3, 1994; Ord. 114518 § 4, 1989; Ord. 111835 § 1, 1984; Ord. 108200 , § 2(11.30.040), 1979.)

11.30.060 - When a vehicle may be impounded after notice.

A vehicle not subject to impoundment under Section 11.30.040 may be impounded after notice of such proposed impoundment has been securely attached to and conspicuously displayed on the vehicle for a period of twenty-four (24) hours prior to such impoundment, for the following reasons:

A. When such vehicle is parked and/or used in violation of any law, ordinance or regulation; or

B. When such vehicle is abandoned, as that term is defined in SMC 11.14.015, as now or hereafter amended; or

C. When such vehicle is so mechanically defective as to be unsafe for operation; provided, however, that this section shall not be construed to prevent the operation of any such defective vehicle to a place for correction of equipment defect in the manner directed by any peace officer.

(Ord. 120102 § 2, 2000; Ord. 117306 § 4, 1994: Ord. 108200 , § 2(11.30.060), 1979.)

11.30.080 - How impoundment is to be effected.

When impoundment is authorized by this chapter, a vehicle may be impounded either by an officer or authorized agent of the Police Department or by a contractor for towing and storage acting at the request

of an officer or authorized agent of the Police Department or Seattle Housing Authority and in accordance with a contract authorized by Section 11.30.220.

(Ord. 117306 § 5, 1994: Ord. 108200 , § 2(11.30.080), 1979.)

11.30.100 - Owner of impounded vehicle to be notified.

A. Not more than twenty-four (24) hours after impoundment of any vehicle, the tow contractor shall mail a notice by first class mail to the last known and legal owners of the vehicles, as may be disclosed by the vehicle identification number, and as provided by the Washington State Department of Licenses. The notice shall contain the full particulars of the impoundment, redemption, and opportunity for hearing to contest the propriety of the impoundment as hereinafter provided.

B. Similar notice shall be given to each person who seeks to redeem an impounded vehicle, except that if a vehicle is redeemed prior to the mailing of notice, then notice need not be mailed.

C. The Seattle Police Department shall give written notification to the last registered and legal owner that the investigatory hold has been removed, except that if a vehicle is redeemed following notice by telephone and prior to the mailing of notice, then notice need not be mailed. In addition, the Police Department shall notify the towing contractor, by telephone or in writing, of the authorization to release such vehicle.

(Ord. 117306 § 6, 1994; Ord. 108200 , § 2(11.30.100), 1979.)

11.30.105 - Impoundment of vehicle where driver is arrested for a violation of Section 11.56.320 B or C or Section 11.56.020—Period of impoundment.

A. Whenever the driver of a vehicle who is also the registered owner of the vehicle is arrested for a violation of Section 11.56.020, 11.56.320 B or C, the vehicle is subject to impoundment at the direction of a police officer. For purposes of this subsection, "arrested" includes, but is not limited to, being temporarily detained under Section 12A.02.140 B and served with a citation and notice to appear pursuant to Section 12A.02.140 C and RCW 46.64.015.

B. Reserved.

C. Reserved.

D. If a vehicle is impounded because the driver is arrested for a violation of Section 11.56.320 B or C and the Washington Department of Licensing's records show that the driver has not been convicted of a violation of RCW 46.20.342(1)(a) or (b) or similar local ordinance within the past five (5) years, the vehicle shall be impounded for thirty (30) days.

E. If a vehicle is impounded because the driver is arrested for a violation of Section 11.56.320 B or C and the Washington Department of Licensing's records show that the driver has been convicted one (1) time of a violation of RCW 46.20.342(1)(a) or (b) or similar local ordinance once within the past five (5) years, the vehicle shall be impounded for sixty (60) days.

F. If a vehicle is impounded because the driver is arrested for a violation of Section 11.56.320 B or C and the Washington Department of Licensing's records show that the driver has been convicted of a violation of RCW 46.20.342(1)(a) or (b) or similar local ordinance two (2) or more times within the past five (5) years, the vehicle shall be impounded for ninety (90) days.

(Ord. 121483 § 1, 2004; Ord. 120006 § 1, 2000; Ord. 12005 § 1, 2000; Ord. 119180 § 4, 1998.)

11.30.120 - Redemption of impounded vehicles

Vehicles impounded by the City shall be redeemed only under the following circumstances:

A. The vehicle may be redeemed only by the following persons or entities: the legal owner; the registered owner; a person authorized in writing by the registered owner; the vehicle's insurer or a vendor working on behalf of the vehicle's insurer; a third-party insurer that has a duty to repair or replace the vehicle, has obtained consent from the registered owner or the owner's agent to move the vehicle, and has documented that consent in the insurer's claim file, or a vendor working on behalf of a third-party insurer that has received such consent; a person, who is known to the registered or legal owner of a motorcycle or moped, as each are defined in Chapter 11.14, that was towed from the scene of an accident, may redeem the motorcycle or moped as a bailment in accordance with chapter 46.55 RCW, as amended by Chapter 152, Section 4, Laws of 2017, while the registered or legal owner is admitted as a patient in a hospital due to the accident; provided, however, that at all times the registered owner must be granted access to and may reclaim possession of the vehicle. For the purposes of this subsection 11.30.120.A, "owner's agent" means the legal owner of the vehicle, a driver in possession of the vehicle with the registered owner's permission, or an adult member of the registered owner's family; a person who is determined and verified by the operator to have the permission of the registered owner of the vehicle; or a person who has purchased the vehicle from the registered owner, who produces proof of ownership or authorization and signs a receipt therefore. A person redeeming a vehicle impounded pursuant to Section 11.30.105 must prior to redemption establish that he or she has a valid driver's license and is in compliance with Section 11.20.340. A vehicle impounded pursuant to Section 11.30.105 can be released only pursuant to a written release authorization from the Seattle Police Department pursuant to subsection 11.30.120.C or a written release authorization or order from Municipal Court pursuant to subsection 11.30.120.B or 11.30.120.C.

B. Any person so redeeming a vehicle impounded by the City shall pay the towing contractor for costs of impoundment (removal, towing, and storage) and administrative fee prior to redeeming such vehicle. Such towing contractor shall accept payment as provided in RCW 46.55.120(1)(b), as now or hereafter amended. If the vehicle was impounded pursuant to Section 11.30.105 and was being operated by the registered owner when it was impounded, it may not be released to any person until all penalties, fines, or fees owed by the registered owner to the City of Seattle have been satisfied by payment in full, by establishment of a time payment agreement with the Municipal Court, or by other means acceptable to the Municipal Court. If the vehicle was impounded pursuant to Section 11.30.040.A.7, it may not be released to any person until all penalties, fines, or fees on all parking infractions described in that section, and all booting, removal, towing, storage, lost boot, and administrative fees charged against the vehicle and owed by the registered owner to the City of Seattle have been satisfied by payment in full or through a time payment plan. Upon payment in full or time payment arrangement of such obligations, the court may issue a written release authorization allowing the vehicle to be released from impoundment.

C. The Chief of Police or Municipal Court shall release a vehicle impounded pursuant to Section 11.30.105 prior to the expiration of any period of impoundment:

1. Upon petition of the spouse of the driver, or the person registered pursuant to Ordinance 117244 as the domestic partner of the driver, based on economic or personal hardship to such spouse or domestic partner resulting from the unavailability of the vehicle and after consideration of the threat to public safety that may result from release of the vehicle, including, but not limited to, the driver's criminal history, driving record, license status, and access to the vehicle; or

2. If the registered owner of the vehicle was not the driver, did not know that the driver's license was suspended or revoked and has not received a prior release under this Subsection 11.30.120 C2 or Subsection 11.30.040 A9.

In order to avoid discriminatory application, the Chief of Police and Municipal Court shall deny release without discretion in all circumstances other than for the reasons set forth in this Subsection

11.30.120 C. If such release is authorized, the person redeeming the vehicle still must satisfy the requirements of Section 11.30.120 A and B.

D. Any person seeking to redeem a vehicle impounded as a result of a parking or traffic citation or under Section 12A.10.115 has a right to a hearing before a Municipal Court judicial officer to contest the validity of an impoundment or the amount of removal, towing, and storage charges or administrative fee if such request for hearing is in writing, in a form approved by the Municipal Court and signed by such person, and is received by the Municipal Court within ten (10) days (including Saturdays, Sundays, and holidays) of the latter of the date the notice was mailed to such person pursuant to Section 11.30.100 A or B, or the date the notice was given to such person by the registered tow truck operator pursuant to RCW 46.55.120(2)(a). Such hearing shall be provided as follows:

1. If all of the requirements to redeem the vehicle, including expiration of any period of impoundment under Section 11.30.105, have been satisfied, then the impounded vehicle shall be released immediately, and a hearing as provided for in Section 11.30.160 shall be held within ninety (90) days of the written request for hearing.

2. If not all of the requirements to redeem the vehicle, including expiration of any period of impoundment under Section 11.30.105, have been satisfied, then the impounded vehicle shall not be released until after the hearing provided pursuant to Section 11.30.160, which shall be held within two (2) business days (excluding Saturdays, Sundays and holidays) of the written request for hearing.

3. Any person seeking a hearing who has failed to request such hearing within the time specified in Section 11.30.120 D may petition the Municipal Court for an extension to file a request for hearing. Such extension shall only be granted upon the demonstration of good cause as to the reason(s) the request for hearing was not timely filed. For the purposes of this section, "good cause" shall be defined as circumstances beyond the control of the person seeking the hearing that prevented such person from filing a timely request for hearing. In the event such extension is granted, the person receiving such extension shall be granted a hearing in accordance with this chapter.

4. If a person fails to file a timely request for hearing and no extension to file such a request has been granted, the right to a hearing is waived, the impoundment and the associated costs of impoundment and administrative fee are deemed to be proper, and the City shall not be liable for removal, towing, and storage charges arising from the impoundment.

5. In accordance with RCW 46.55.240 (1)(d), a decision made by a Municipal Court judicial officer may be appealed to Municipal Court for final judgment. The hearing on the appeal under this subsection shall be de novo. A person appealing such a decision must file a request for an appeal in Municipal Court within fifteen (15) days after the decision of the Municipal Court judicial officer and must pay a filing fee in the same amount required for the filing of a suit in district court. If a person fails to file a request for an appeal within the time specified by this section or does not pay the filing fee, the right to an appeal is waived and the Municipal Court judicial officer's decision is final.

(Ord. 125344 , § 1, 2017; Ord. 124302, § 6, 2013; Ord. 123447, § 3, 2010; Ord. 123190, § 9, 2009; Ord. 121525 § 5, 2004; Ord. 121483 § 2, 2004; Ord. 120007 § 1, 2000; Ord. 120006 § 2, 2000; Ord. 119180 § 5, 1998: Ord. 117306 § 7, 1994: Ord. 115634 § 1, 1991: Ord. 110106 § 1, 1981: (Ord. 108200 , § 2(11.30.120), 1979.)

11.30.160 - Post-impoundment hearing procedure.

Hearings requested pursuant to Section 11.30.120 shall be held by a Municipal Court judicial officer, who shall determine whether the impoundment was proper and whether the associated removal, towing, storage, and administrative fees were proper. The Municipal Court judicial officer shall not have the

authority to determine the commission or mitigation of any parking infraction unless a timely response under Section 11.31.050 A was filed to that notice of infraction requesting a hearing and the hearing date for that infraction has not passed, in which case the Municipal Court judicial officer has discretion to consolidate the impoundment hearing and the notice of infraction hearing.

A. At the hearing, an abstract of the driver's driving record is admissible without further evidentiary foundation and is prima facie evidence of the status of the driver's license, permit, or privilege to drive and that the driver was convicted of each offense shown on the abstract. In addition, a certified vehicle registration of the impounded vehicle is admissible without further evidentiary foundation and is prima facie evidence of the identity of the registered owner of the vehicle.

B. If the impoundment is found to be proper, the Municipal Court judicial officer shall enter an order so stating. In the event that the costs of impoundment (removal, towing, and storage) and administrative fee have not been paid or any other applicable requirements of Section 11.30.120 B have not been satisfied or any period of impoundment under Section 11.30.105 has not expired, the Municipal Court judicial officer's order shall also provide that the impounded vehicle shall be released only after payment to the City of any fines imposed on any underlying traffic or parking infraction and satisfaction of any other applicable requirements of Section 11.30.120 B and payment of the costs of impoundment and administrative fee to the towing company and after expiration of any period of impoundment under Section 11.30.105. In the event that the Municipal Court judicial officer grants time payments for the costs of impoundment and administrative fee, the City shall be responsible for paying the costs of impoundment to the towing company. The Municipal Court judicial officer shall grant such time payments only in cases of extreme financial need, and where there is an effective guarantee of payment.

C. If the impoundment is found to be improper, the Municipal Court judicial officer shall enter an order so stating and order the immediate release of the vehicle. If the costs of impoundment and administrative fee have already been paid, the Municipal Court judicial officer shall enter judgment against the City and in favor of the person who has paid the costs of impoundment and administrative fee in the amount of the costs of the impoundment and administrative fee.

D. In the event that the Municipal Court judicial officer finds that the impound was proper, but that the removal, towing, storage, or administrative fees charged for the impoundment were improper, the Municipal Court judicial officer shall determine the correct fees to be charged. If the costs of impoundment and administrative fee have been paid, the Municipal Court judicial officer shall enter a judgment against the City and in favor of the person who has paid the costs of impoundment and administrative fee for the amount of the overpayment.

E. No determination of facts made at a hearing under this section shall have any collateral estoppel effect on a subsequent criminal prosecution and such determination shall not preclude litigation of those same facts in a subsequent criminal prosecution.

F. An appeal of the Municipal Court judicial officer's decision in Municipal Court shall be conducted according to, and is subject to, the procedures of this section. If the court finds that the impoundment or the removal, towing, storage, or administrative fees are improper, any judgment entered against the City shall include the amount of the filing fee.

(Ord. 120006 § 3, 2000: Ord. 119180 § 6, 1998: Ord. 115634 § 3, 1991: Ord. 110106 § 2, 1981: Ord. 108200 , § 2(11.30.160), 1979.)

11.30.180 - Responsibility for fees as to standby time or vehicles held for investigatory purposes.

A. No fee shall be assessed against the owner of a vehicle for time elapsed after the towing equipment has arrived at the location of the vehicle to be towed and prior to the operation of the towing equipment or performance of the impound service.

B. No impoundment fee and/or towing or storage charges shall be assessed against the owner of a vehicle which is being held for investigatory purposes pursuant to Section 11.30.040 A6 and which is redeemed within forty-eight (48) hours after the Police Department shall have notified the owner of the release of such vehicle in writing in the manner provided in Section 11.30.100 C; provided that such owner or person authorized to obtain possession of such impounded vehicle shall pay any charges assessed for storage after such forty-eight (48) hour period; provided further, that if the registered owner or the driver authorized by the registered owner is arrested or charged with a crime in connection with the incident leading to impoundment, the City shall not pay the towing or storage charges.

(Ord. 117306 § 8, 1994: Ord. 115634 § 4, 1991: Ord. 112421 § 6, 1985; Ord. 109031 § 1, 1980: Ord. 108200 , § 2 (11.30.180), 1979.)

11.30.200 - Abandoned vehicles.

A. Any impounded vehicle not redeemed within fifteen (15) days of mailing of the notice required by Section 11.30.100 shall be deemed abandoned.

B. No tow truck operator shall sell or otherwise dispose of an abandoned vehicle unless all applicable provisions of State law have been complied with.

(Ord. 117306 § 9, 1994: Ord. 108200 , § 2(11.30.200), 1979.)

11.30.220 - Contract for towing and storage.

A. The Director of Finance and Administrative Services is authorized and directed to prepare specifications for towing and storage of vehicles, including instructions to bidders, containing such provisions as the Director shall deem advisable and not in conflict with this chapter.

B. A call for bids responsive to such specifications shall then be made, and the contract shall be awarded to the lowest and best bidder whose proposal is deemed by the Director of Finance and Administrative Services to be the most advantageous for the public and the City; provided that, in the event all bids are deemed by the Director to be too high or irregular, he or she may reject all such bids and make another call for bids or proceed alternatively pursuant to ordinance passed for such purpose.

The Director shall consider, among other relevant factors, the following:

1. Integrity, skill, and business judgment of the bidder;
2. General experience in providing towing and storage services;
3. Conduct and performance under a previous City towing impound contract demonstrating honesty, promptness, skill, efficiency, and a satisfactory relationship with vehicle owners;
4. Existing availability of equipment, facilities, and personnel; and
5. The bidder's financial ability and willingness to expand or improve available equipment, facilities, and services.

The contract award shall be in accordance with the specifications so approved for towing and storage service necessary for carrying out the provisions of this chapter.

C. Subsequent to the award of the contract, the Director of Finance and Administrative Services shall file a written statement with the City Clerk giving the name and address of the contractor for towing and storage of vehicles and, if more than one place of storage has been provided, the name and address or location of each storage place. The Director shall administer and enforce contracts made pursuant to this section.

(Ord. 123361, § 251, 2010; Ord. 122589 , § 1, 2007; Ord. 120794 § 199, 2002: Ord. 117169 § 128, 1994: Ord. 116368 § 214, 1992; Ord. 108200 , § 2(11.30.220), 1979.)

11.30.240 - Contract for towing and storage—Financial responsibility.

Any contract for towing and storage under the provisions of this chapter shall require the contractor to demonstrate proof of financial responsibility for any liability which the City may have as a result of any negligence, willful conduct or breach of contract by the contractor and for any damages which the owner of an impounded vehicle may sustain as a result of damage to or loss of the vehicle, or the contents of a vehicle in the custody of the contractor. Proof of financial responsibility shall be furnished either by proof of insurance, by filing a surety bond and/or by depositing cash in such amounts as the Director of Finance and Administrative Services shall determine necessary.

(Ord. 123361, § 252, 2010; Ord. 117306 § 10, 1994: Ord. 117169 § 129, 1994: Ord. 108200 , § 2(11.30.240), 1979.)

11.30.260 - Contract for towing and storage—Notice to owners of impounded vehicles.

Any contract for towing and storage under provisions of this chapter shall require the contractor, at any location where vehicles are impounded, to post conspicuous notice of the rights of the owners of such vehicles under Section 11.30.220.

(Ord. 108200 , § 2(11.30.260), 1979.)

11.30.280 - Contractor to file monthly claim for services.

The contractor shall, on or before the tenth day of each month, file his or her claim with the Department of Finance and Administrative Services for towing and storage charges accruing to him or her upon vehicles redeemed as provided in this chapter during the preceding month, in accordance with this chapter and with the specifications for the contract authorized in Section 11.30.220, and such claim shall be sworn to by him or her under oath. The Director of Finance and Administrative Services shall audit such claim and any payment thereof at least once annually. A warrant or warrants for payment of such claim shall be drawn and paid by the Director from such expenditure allowances as may be provided therefor in the annual budget or from such moneys as may otherwise be appropriated for such purpose. If the appropriate fund is solvent at the time payment is ordered, the Director may elect to make payment by check.

(Ord. 123361, § 253, 2010; Ord. 120794 § 200, 2002; Ord. 120181 § 115, 2000; Ord. 120114 § 34, 2000; Ord. 118397 § 100, 1996; Ord. 117169 § 130, 1994; Ord. 116368 § 215, 1992; Ord. 108200 , § 2(11.30.280), 1979.)

11.30.290 - Contract for towing and storage—Administrative fee.

A. If a vehicle is impounded pursuant to Section 11.30.105, an administrative fee shall be levied when the vehicle is redeemed under the specifications of the contract provided for by Section 11.30.220.

B. If a vehicle is impounded pursuant to subsection 11.30.040.A7, an administrative fee shall be levied when the vehicle is redeemed under the specifications of the contract provided for by Section 11.30.220.

C. If a vehicle is impounded other than pursuant to subsection 11.30.040.A7 or Section 11.30.105, an administrative fee shall be levied when the vehicle is redeemed under the specifications of the contract provided for by Section 11.30.220.

D. The administrative fee shall be collected by the contractor performing the impound, and shall be remitted to the Department of Finance and Administrative Services in the manner directed by the Director of Finance and Administrative Services and as specified in the contract provided by subsection 11.30.220.A. The administrative fee shall be for the purpose of offsetting, to the extent practicable, the cost to the City of implementing, enforcing, and administering the provisions of this chapter and shall be deposited in an appropriate account. The administrative fee shall be set by rule by the Director in an amount not to exceed $100.

(Ord. 123361, § 254, 2010; Ord. 120794 § 201, 2002; Ord. 120181 § 116, 2000; Ord. 119180 § 7, 1998; Ord. 118397 § 101, 1996; Ord. 117306 § 11, 1994.)

11.30.300 - Record of impounded vehicles.

A. The Police Department shall keep, and make available for public inspection, a record of all vehicles impounded under the provisions of this chapter. The record shall include at least the following information:

1. Manufacturer's trade name or make;
2. Vehicle license number and state of registration;
3. Vehicle identification number;
4. Such other descriptive information as the Chief of Police deems useful for purposes of vehicle identification;
5. Basis for impoundment, including reference to the appropriate section or sections of this subtitle; and
6. Disposition of the vehicle and date of disposition.

B. The Police Department shall furnish to the towing contractor, upon request, the name of the registered owner of any vehicle impounded by such contractor pursuant to this chapter.

(Ord. 108200 , § 2(11.30.300), 1979.)

11.30.320 - Rules and regulations.

The Director of Finance and Administrative Services and the Chief of Police are authorized and directed to promulgate rules and regulations consistent with this chapter, the Charter of the City, and Chapter 3.02 to provide for the fair and efficient administration of any contract or contracts awarded pursuant to Section 11.30.220 and to provide for the fair and efficient administration of any vehicle impoundment, redemption, or release or any impoundment hearing under this chapter.

(Ord. 123361, § 255, 2010; Ord. 120794 § 202, 2002; Ord. 119180 § 8, 1998; Ord. 117169 § 131, 1994; Ord. 108200 , § 2(11.30.320), 1979.)

11.30.340 - Vehicle immobilization prohibited.

A. A property owner, other than the State of Washington or any unit of local government, shall not immobilize any vehicle owned by a person other than the property owner. "Immobilize" means the use of a locking wheel boot that, when attached to the wheel of a vehicle, prevents the vehicle from moving without damage to the tire to which the locking wheel boot is attached.

B. A violation of this section is a gross misdemeanor. (RCW 46.55.300)

(Ord. 122742, § 6, 2008.)

11.30.360 - Violations constituting abandoning—Evidence—Penalty.

A. No person shall wilfully leave an abandoned vehicle on private property for more than twenty-four (24) hours without the permission of the person having the right to possession of the property, or a wrecked, dismantled, or inoperative vehicle or automobile hulk on a street, alley or way open to the public for twenty-four (24) hours or longer without notification to the Chief of Police of the reasons for leaving the motor vehicle in such a place. Any such vehicle or hulk shall be abated and removed in accordance with the provisions of Ordinance 98223, [13] as amended, and enforcement shall be by the Director of Transportation in accordance with said ordinance as amended. For the purposes of this section, the fact that a motor vehicle has been so left without permission or notification is prima facie evidence of abandonment.

B. Any person found to have abandoned a vehicle or hulk shall, in addition to any penalty imposed, also be assessed any costs incurred by the City in the removal of such abandoned vehicle or hulk less any moneys received by the City from such removal.

(Ord. 121420 § 6, 2004; Ord. 117306 § 13, 1994; Ord. 109476 § 3(part), 1980; Ord. 108200 , § 2(11.30.360), 1979.)

Footnotes:

--- (13) ---

Editor's note— Ord. 98223 is codified in Chapter 11.92 of this Code.

Chapter 11.31 - DISPOSITION OF TRAFFIC OFFENSES

Sections:

11.31.010 - Violations as traffic infractions.

Except as otherwise provided in Section 11.34.020 or elsewhere in this title, failure to perform any act required or the performance of any act prohibited by this title is designated as a traffic infraction and may not be classified as a criminal offense.

(Ord. 123632, § 10, 2011; Ord. 122003 , § 2, 2005; Ord. 115040, § 6, 1990; Ord. 112975 , § 1, 1986; Ord. 112466 , § 2, 1985; Ord. 110967 , § 5, 1983; Ord. 109476 , § 1, 1980; Ord. 108200 , § 2(11.31.010), 1979.)

11.31.020 - Notice of traffic infraction—Issuance.

A. A peace officer has the authority to issue a notice of traffic infraction:

1. when the infraction is committed in the officer's presence;
2. if an officer investigating at the scene of a motor vehicle accident has reasonable cause to believe that the driver of a motor vehicle involved in the accident has committed a traffic infraction; or
3. when a violation of Section 11.50.140, 11.50.150, 11.52.040, or 11.52.100 is detected through the use of an automated traffic safety camera as authorized pursuant to RCW 46.63.170 and Section 11.50.570.

B. A court may issue a notice of traffic infraction upon receipt of a written statement of the officer that there is reasonable cause to believe that an infraction was committed. (RCW 46.63.030)

(Ord. 124950 , § 5, 2015; Ord. 123632, § 8, 2011; Ord. 123420, § 6, 2010; Ord. 123035, § 2, 2009; Ord. 119011 , § 7, 1998; Ord. 118105, § 2, 1996; Ord. 112421 , § 12, 1985; Ord. 109476 , § 3(part), 1984; Ord. 108200 , § 2(11.23.400), 1979.) Ord. 123946, § 4, 2012; Ord. 123170, § 1, 2009; Ord. 121944 , § 2, 2005; Ord. 109476 , § 1(part), 1980; Ord. 108200 , § 2(11.31.020), 1979.)

11.31.030 - Parking notices.

Whenever any motor vehicle without an operator is found parked, standing or stopped in violation of this subtitle, the officer finding it may take its registration number and any other information displayed on the vehicle which may identify its user, and shall fix conspicuously to such vehicle a notice of traffic infraction. (RCW 46.63.030(3))

(Ord. 109476 § 2(part), 1980; Ord. 108200 , § 2(11.31.030), 1979.)

11.31.040 - Notice of traffic infraction—Determination—Response.

A notice of traffic infraction represents a determination that an infraction has been committed. The determination will be final unless contested as provided in this chapter. (RCW 46.63.060)

(Ord. 109476 § 1(part), 1980: Ord. 108200 , § 2(11.31.020), 1979.)

11.31.050 - Response to notice of traffic infraction—Contesting determination—Hearing—Failure to appear.

A. Any person who receives a notice of traffic infraction shall respond to such notice as provided in this section within fifteen (15) days of the date of the notice.

B. If the person determined to have committed the infraction does not contest the determination the person shall respond by completing the appropriate portion of the notice of infraction and submitting it, either by mail or in person, to the Municipal Court of Seattle. A check or money order in the amount of the penalty prescribed for the infraction must be submitted with the response. When a response which does not contest the determination is received, an appropriate order shall be entered in the court's records, and a record of the response and order shall be furnished to the Department of Licensing in accordance with RCW 46.20.270.

C. If the person determined to have committed the infraction wishes to contest the determination the person shall respond by completing the portion of the notice of infraction requesting a hearing and submitting it, either by mail or in person, to the Municipal Court of Seattle. The court shall notify the person in writing of the time, place, and date of the hearing, and that date shall not be sooner than seven (7) days from the date of the notice, except by agreement.

D. If the person determined to have committed the infraction does not contest the determination but wishes to explain mitigating circumstances surrounding the infraction, the person shall respond by completing the portion of the notice of infraction requesting a hearing for that purpose and submitting it, either by mail or in person, to the Municipal Court of Seattle. The court shall notify the person in writing of the time, place, and date of the hearing.

E. In any hearing conducted pursuant to subsections C or D of this section, the court may defer findings, or in a hearing to explain mitigating circumstances may defer entry of its order, for up to one (1) year and impose conditions upon the defendant the court deems appropriate. Upon deferring

findings, the court may assess costs as the court deems appropriate for administrative processing. If at the end of the deferral period the defendant has met all conditions and has not been determined to have committed another traffic infraction, the court may dismiss the infraction. A person may not receive more than one (1) deferral within a seven (7) year period for traffic infractions for moving violations and more than one (1) deferral within a seven (7) year period for traffic infractions for nonmoving violations. A person who commits negligent driving in the second degree with a vulnerable user victim may not receive a deferral for this infraction under this section.

F. If any person issued a notice of traffic infraction:

1. Fails to respond to the notice of traffic infraction as provided in subsection B of this section; or

2. Fails to appear at a hearing requested pursuant to subsections C or D; the court shall enter an appropriate order assessing the monetary penalty prescribed for the traffic infraction and any other penalty authorized by this chapter and shall notify the Department of Licensing in accordance with RCW 46.20.270 of the failure to respond to the notice of infraction or to appear at a requested hearing. (RCW 46.63.070)

(Ord. 123946, § 5, 2012; Ord. 120060 , § 1, 2000; Ord. 111859 , § 2, 1984; Ord. 109476 , § 1(part), 1980; Ord. 108200 , § 2(11.31.050), 1979.)

11.31.060 - Hearing—Contesting determination that infraction committed—Appeal.

A. A hearing held for the purpose of contesting the determination that an infraction has been committed shall be without a jury.

B. The court may consider the notice of traffic infraction and any other written report made under oath submitted by the officer who issued the notice or whose written statement was the basis for the issuance of the notice in lieu of the officer's personal appearance at the hearing. The person named in the notice may subpoena witnesses, including the officer, and has the right to present evidence and examine witnesses present in court.

C. The burden of proof is upon the City to establish the commission of the infraction by a preponderance of the evidence.

D. After consideration of the evidence and argument, the court shall determine whether the infraction was committed. Where it has not been established that the infraction was committed, an order dismissing the notice shall be entered in the court's records. Where it has been established that the infraction was committed an appropriate order shall be entered in the court's records. A record of the court's determination and order shall be furnished to the Department of Licensing in accordance with RCW 46.20.270 as now or hereafter amended.

E. An appeal from the court's determination or order shall be to the Superior Court. The decision of the Superior Court is subject only to discretionary review pursuant to Rule 2.3 of the Rules of Appellate Procedure. (RCW 46.63.090)

(Ord. 109476 § 1(part), 1980: Ord. 108200 , § 2(11.31.060), 1979.)

11.31.070 - Hearings—Explanation of mitigating circumstances.

A. A hearing held for the purpose of allowing a person to explain mitigating circumstances surrounding the commission of an infraction shall be an informal proceeding. The person may not subpoena witnesses. The determination that an infraction has been committed may not be contested at a hearing held for the purpose of explaining mitigating circumstances.

B. After the court has heard the explanation of the circumstances surrounding the commission of the infraction an appropriate order shall be entered in the court's records. A record of the court's

determination and order shall be furnished to the Department of Licensing in accordance with RCW 46.20.270 as now or hereafter amended.

C. There may be no appeal from the court's determination or order. (RCW 46.63.100)

(Ord. 109476 § 1(part), 1980: Ord. 108200 , § 2(11.31.070), 1979.)

11.31.080 - Owner responsible for stopping, standing, parking, or alarm violation.

A. In any traffic infraction case involving a violation of this title relating to the stopping, standing or parking of a vehicle, or the sounding of an audible alarm, proof that the particular vehicle described in the notice of traffic infraction was stopping, standing or parking or emitting an audible alarm in violation of any such provision in this title together with proof of registered ownership of the vehicle at the time of the violation, shall constitute in evidence a prima facie presumption that the registered owner of the vehicle was the person who parked or placed the vehicle at the point where, and for the time during which, the violation occurred or was responsible for the failure to turn off the audible alarm as required.

B. The foregoing stated presumption shall apply only when the procedure prescribed in Section 11.31.030 has been followed. (RCW 46.63)

C. If a car rental agency declares that the vehicle was under lease at the time of the violation, and supplies the name and address of the lessee, there shall be a prima facie presumption that the lessee so identified parked or placed the vehicle at the point where the violation occurred, or was responsible for the failure to turn off the audible alarm as required.

(Ord. 116701 § 2, 1993: Ord. 109476 § 2(part), 1980: Ord. 108200 , § 2(11.31.080), 1979.)

11.31.090 - Traffic infractions detected through the use of an automated traffic safety camera

A. A notice of infraction based on evidence detected through the use of an automated traffic safety camera must be mailed to the registered owner of the vehicle within 14 days of the violation, or to the renter of a vehicle within 14 days of establishing the renter's name and address under subsection C1 of this section, SMC 11.31.090. The peace officer issuing the notice of infraction shall include with it a certificate or facsimile thereof, based upon inspection of photographs, microphotographs, or electronic images produced by an automated traffic safety camera, stating the facts supporting the notice of infraction. This certificate or facsimile is prima facie evidence of the facts contained in it and is admissible in a proceeding charging a violation of Section 11.50.140, Section 11.50.150, Section 11.52.040, or Section 11.52.100. The photographs, microphotographs, or electronic images evidencing the violation must be available for inspection and admission into evidence in a proceeding to adjudicate the liability for the infraction.

B. A person receiving such a notice of infraction may respond to the notice by mail. The registered owner of a vehicle is responsible for such an infraction unless the registered owner overcomes the presumption in SMC subsection 11.31.090.E, or, in the case of a rental car business, satisfies the conditions under SMC subsection 11.31.090.C. If appropriate under the circumstances, a renter identified under SMC subsection 11.31.090.C1 is responsible for such an infraction.

C. If the registered owner of the vehicle is a rental car business, the peace officer shall, before such a notice of infraction is issued, provide a written notice to the rental car business that a notice of infraction may be issued to the rental car business if the rental car business does not, within 18 days of receiving the written notice, provide to the peace officer by return mail:

1. A statement under oath stating the name and known mailing address of the individual driving or renting the vehicle when the infraction occurred; or

2. A statement under oath that the business is unable to determine who was driving or renting the vehicle at the time the infraction occurred; or

3. In lieu of identifying the vehicle operator, the rental car business may pay the applicable penalty.

Timely mailing of this statement to the peace officer relieves a rental car business of any liability under Chapter 11.31 for the notice of infraction.

D. The term "automated traffic safety camera" means a device that uses a vehicle sensor installed to work in conjunction with an intersection traffic control system, a railroad grade crossing system or speed measuring device, and a camera synchronized to automatically record one or more sequenced photographs, microphotographs, or electronic images of the rear of a motor vehicle at the time the vehicle fails to stop when facing a steady red traffic control signal or an activated railroad grade crossing control signal or exceeds a speed limit in a school speed zone as detected by a speed measuring device. An automated traffic safety camera includes a camera used to detect violations other than stoplight, railroad crossing and school speed zone violations as authorized by and subject to the restrictions imposed by the Washington Legislature.

E. In a traffic infraction case involving an infraction detected through the use of an automated traffic safety camera, proof that the particular vehicle described in the notice of traffic infraction was in violation of Section 11.50.140, Section 11.50.150, 11.52.040, or Section 11.52.100, together with proof that the person named in the notice of traffic infraction was at the time of the violation the registered owner of the vehicle, constitutes in evidence a prima facie presumption that the registered owner of the vehicle was the person in control of the vehicle at the point where, and for the time during which, the violation occurred. This presumption may be overcome only if the registered owner states, under oath, in a written statement to the court or in testimony before the court that the vehicle involved was, at the time, stolen or in the care, custody, or control of some person other than the registered owner.

(Ord. 124686 , § 2, 2015; Ord. 123946, § 6, 2012; Ord. 123170, § 2, 2009; Ord. 122725 , § 1, 2008; Ord. 122554 , § 1, 2007; Ord. 121944 § 3, 2005.)

11.31.115 - Monetary penalty doubled for certain traffic infractions.

A person found to have committed a traffic infraction relating to right of way, speed restrictions, overtaking and passing or regard for pedestrians in a school or playground crosswalk zone under Sections 11.40.040, 11.44.120, 11.52.100, 11.53.400, 11.58.230 or 11.58.310, speed restrictions in a roadway construction zone under Section 11.52.110 or an emergency zone under Section 11.58.272 or overtaking and passing a school bus under Section 11.53.440 A shall be assessed a monetary penalty equal to twice the penalty assessed under Section 11.31.120. This penalty may not be waived, reduced or suspended. (RCW 46.61.212(3); RCW 46.61.235(5); RCW 46.61.245(2); RCW 46.61.261(2); RCW 46.61.440(3); RCW 46.61.527(3); RCW 46.61.370(6))

(Ord. 123420, § 8, 2010; Ord. 123420, § 7, 2010; Ord. 119011 § 9, 1998.)

11.31.120 - Monetary penalties.

A. A person found to have committed a traffic infraction shall be assessed a monetary penalty. No penalty may exceed $250.00 for each offense unless a higher penalty is specifically provided for in this title or by statute.

B. There shall be a penalty of $25.00 for failure to respond to a notice of traffic infraction, to appear at a requested hearing or to pay a monetary penalty imposed pursuant to this chapter.

C. A traffic infraction for violation of Section 11.50.140, Section 11.50.150, Section 11.52.040, or Section 11.52.100 detected through the use of an automated traffic safety camera shall be processed in the same manner as a parking infraction, with a monetary penalty equal to the total penalty, including the base penalty plus any statutory assessments authorized under state law, for violations of such Sections otherwise detected by a police officer. However, the monetary penalty for

a violation of Section 11.50.140 or Section 11.50.150 detected through the use of an automated traffic safety camera shall not exceed the monetary penalty for a violation of Section 11.50.380 as provided under subsection A of this Section, including all applicable statutory assessments.

(Ord. 123946, § 7, 2012; Ord. 123445, § 1, 2010; Ord. 123170, § 4, 2009; Ord. 122725 , § 2, 2008; Ord. 122554 , §§ 1, 2, 2007; Ord. 121944 , § 4, 2005; Ord. 120481 , § 3, 2001; Ord. 115927, § 1, 1991; Ord. 114839, § 1, 1989; Ord. 113186 , § 1, 1986; Ord. 110013 , § 1, 1981; Ord. 109476 , § 1(part), 1980; Ord. 108200 , § 2(11.31.120), 1979.)

11.31.121 - Monetary penalties—Parking infractions

The base monetary penalty for violation of each of the numbered provisions of the Seattle Municipal Code listed in the following table is as shown, unless and until the penalty shown below for a particular parking infraction is modified by Local Rule of the Seattle Municipal Court adopted pursuant to the Infraction Rules for Courts of Limited Jurisdiction ("IRLJ") or successor rules to the IRLJ:

Municipal Code reference	Parking infraction short description	Base penalty amount
11.23.400	UNAUTHORIZED USE - DISABLED	$250
11.23.410	CARPOOL, FREE & PREFERENTIAL	$47
11.23.415	CARPOOL PERMIT	$47
11.26.060	SERVICE CONTROLLED PARKING AREA	$47
11.26.080	HOOD, CONTROLLED PARKING AREA	$47
11.26.100	HOOD, FREE PARKING AREA	$47
11.26.120	HOOD, WORK LOCATION	$47
11.26.140	HOOD ON OCCUPIED METER	$47
11.26.160	HOODED METER, UNOCCUPIED	$47
11.26.180	HOOD ON METER OVER 2 DAYS	$47
11.26.200	HOOD, PROH. HOURS	$47
11.26.220	HOOD, PASSENGER VEH.	$47

11.26.240	HOOD, REVOKED	$47
11.26.280	HOOD, VIOLATION	$47
11.70.020	ANGLE, GEN.	$47
11.70.040	PARALLEL R. SIDE	$47
11.70.060	PARALLEL 1 WAY ST.	$47
11.70.080	SHOULDER	$47
11.70.100	STALLS/SPACES	$47
11.70.120	PARK, R/W	$47
11.70.140	SECURE VEH.	$44
11.70.160	KEYS IGNITION	$47
11.70.180	REMOVE KEY, LOCK DOOR	$47
11.70.200	ILLEGAL ON STREET/ALLEY	$47
11.72.010	ADVERTISING	$47
11.72.020	ALLEY	$47
11.72.025	ALLEY/DRIVEWAY	$47
11.72.030	ANGLE/ARTERIAL OR BUS ROUTE	$47
11.72.035	BLOCK TRAF OR WALK UNOCCUPIED	$47
11.72.045	BUS SHELTER	$47
11.72.050	BUS ZONE	$47
11.72.051	CURB BULBS	$47

11.72.053	UNAUTHOR. VEH/CARPOOL	$47
11.72.054	CAR SHARING VEH ZONE	$47
11.72.055	CLASS OF VEH.	$47
11.72.060	CLEAR ROADWAY	$47
11.72.065	IN MARKED DISABLED, INVALID PLACARD	$250
11.72.070	COMMERCIAL VEH.	$47
11.72.075	RESTRICTIONS - COMM LOAD ZONE	$53
11.72.080	CROSSWALK	$47
11.72.090	XWALK APPROACH	$47
11.72.100	DOUBLE PARKED	$47
11.72.110	DRIVEWAY OR ALLEY ENTRANCE	$47
11.72.125	ELECTRIC VEHICLE CHARGING STATION	$124
11.72.130	ELEVATED STRUCTURE	$47
11.72.140	EXCAVATION OR OBSTRUCTION	$47
11.72.145	EXPIRED/IMPROPER PLATES	$47
11.72.150	FIRE APPARATUS	$47
11.72.155	FIRE EXIT DOOR	$47
11.72.160	FIRE HYDRANT	$47
11.72.170	FIRE STATION DRIVEWAY	$47
11.72.180	FIRE AREA	$47

11.72.185	FIRE LANE	$47
11.72.190	FLASHING SIGNAL	$47
11.72.195	FOOD-VEHICLE ZONE	$47
11.72.200	FUEL LOSS	$47
11.72.205	DROPPING OIL OR GREASE	$47
11.72.210	INTERSECTION	$47
11.72.215	LOAD/UNLOAD ZONE	$47
11.72.220	HOODED METERS, SIGNS	$47
11.72.230	MOVING VEHICLE OF ANOTHER	$47
11.72.240	MOVE VEH. AVOID TIME LIMIT	$47
11.72.250	PARK, MUNICIPAL PROPERTY	$44
11.72.260	OVERTIME	$44
11.72.270	REPEATED OVERTIME	$47
11.72.280	IN PARK	$47
11.72.285	PASS. LOAD ZONE	$47
11.72.290	PAVEMENT MARKINGS	$47
11.72.300	PEAK HOUR	$47
11.72.310	PLANTED AREA	$44
11.72.320	PLANTING STRIP	$44
11.72.330	SIGN POSTED LOCATIONS	$47

11.72.350	TOO CLOSE TO R.R.	$47
11.72.351.A	RESTRICTED PARKING ZONE	$53
11.72.351.B	RPZ PERMIT DISPLAY IN IMPROPER LOCATION ON VEHICLE	$29
11.72.351.C	ILLEGAL SALE, PURCHASE OR POSSESSION OF RPZ PERMIT	$250
11.72.352	HUSKY STADIUM EVENT RESTRICTED PARKING	$53
11.72.353	SCHOOL LOAD ZONE	$47
11.72.355	SERVICE VEH. IN ST.	$47
11.72.357	SHUTTLE BUS LOAD ZONE	$47
11.72.360	SIDEWALK	$47
11.72.370	STOP SIGN APPROACH (30')	$47
11.72.390	LIMITED ACCESS, STREET	$47
11.72.400	TAXI CAB ZONE	$47
11.72.410	TOW AWAY ZONE	$47
11.72.415	TRAIL OR PATH (VEH/BIKE)	$47
11.72.420	TRF. CONTROL SIGNAL APPROACH	$47
11.72.430	TRL./CAMPER DETACHED	$47
11.72.435	PASS. VEH. IN TRUCK ZONE	$47
11.72.440	OVER 72 HOURS	$44
11.72.450	TYPE OF VEH.	$47
11.72.460	WALL OR FENCE	$47

11.72.465	CURB RAMP	$47
11.72.470	WRONG SIDE	$47
11.72.480	W/IN 30 FT. OF YIELD SIGN	$47
11.72.500	PARKING JUNK VEHICLE ON STREET (IMPOUND)	$250
11.74.010	STAND/ALLEY/COMM. VEH.	$47
11.74.020	TRUCK LOAD ZONE - CMCRL VEH.	$47
11.74.030	LOAD ZONE - TIME RESTRICTIONS	$53
11.74.060	LOAD/UNLOAD PROH.	$47
11.74.120	RESTRICTED AREA	$47
11.76.005	IMPROPER PARKING RECEIPT DISPLAY	$29
11.76.015	PAY-TO-PARK VIOLATIONS	$44
11.76.020	PARKING TIME LIMIT	$47
11.76.030	METER RESTRICTION	$44
11.76.040	ILLEGAL USE, PARKING PAYMENT, TAMPERING	$47
11.82.300	LIGHTS, PARKED VEHICLE	$47
11.82.320	LIGHTS, PARKED, HIGHBEAM	$47
11.84.345	FALSE ALARM - PARKED AUTO	$47
18.12.235	RESTRICTIONS IN CERTAIN PARKS (REQ)	$47

(Ord. 125609 , § 5, 2018; Ord. 124302, § 7, 2013; Ord. 123712, § 2, 2011; Ord. 123705, § 1, 2011; Ord. 123659, § 8, 2011; Ord. 123161, § 1, 2009; Ord. 123035, § 4, 2009; Ord. 123001, §

10, 2009; Ord. 122779, § 6, 2008; Ord. 122761, § 2, 2008; Ord. 121954, § 2, 2005; Ord. 121917, § 5, 2005; Ord. 121388, § 11, 2004; Ord. 121005, § 1, 2002.)

11.31.125 - Civil infraction — Automobile alarm — Failure to respond.

A. The violation of or failure to comply with Section 11.84.345 is a civil infraction as contemplated by RCW Chapter 7.80, and subject as a Class 4 civil infraction to a maximum penalty and a default amount of Twenty-three Dollars ($23).

B. There shall be a maximum penalty and default amount of Twenty-five Dollars ($25) for failure to respond to a notice of violation under Section 11.84.345 within fifteen (15) days from the date of notice as contemplated by RCW 7.80.030(1) and 7.80.076(2)(K), a failure to appear at a hearing requested by the recipient of the notice as contemplated by RCW 7.80.160(2) and RCW 7.80.070(2)(K), and a failure to pay a penalty imposed under subsection A of this section, as contemplated by RCW 7.80.160(3).

C. If the court determines that a person has insufficient funds to pay the monetary penalty, the court may order performance of a number of hours of community service instead.

(Ord. 116701 § 3, 1993.)

11.31.130 - Order of court—Civil in nature.

An order entered after the receipt of a response which does not contest the determination, or after it has been established at a hearing that the infraction was committed, or after a hearing for the purpose of explaining mitigating circumstances is civil in nature. (RCW 46.63.120)

(Ord. 109476 § 1(part), 1980: Ord. 108200, § 2(11.31.130), 1979.)

Chapter 11.32 - CITATIONS

Sections:

11.32.020 - Service of citation.

Whenever any person is charged with any violation of this subtitle, other than a traffic infraction, the officer may serve upon him or her a traffic citation and notice to appear in court. Such citation and notice shall be handled and disposed of as set forth in RCW 46.64.010 and also shall conform with the requirements of RCW 46.64.010 and be in the form prescribed in RCW 46.64.015. (RCW 46.64.010, 46.64.015)

(Ord. 123946, § 8, 2012; Ord. 109476 § 3(part), 1980: Ord. 108200, § 2(11.32.020), 1979.)

11.32.080 - Return of citation.

The original or a copy of every citation issued by an enforcement officer shall be transmitted to the Municipal Court of Seattle as soon as is practicable. (RCW 46.64.010)

(Ord. 108200, § 2(11.32.080), 1979.)

11.32.160 - Cancellation.

No person shall cancel or solicit the cancellation of any citation in any manner other than as provided in this chapter.

(Ord. 108200 , § 2(11.32.160), 1979.)

Chapter 11.34 - PENALTIES

Sections:

11.34.020 - Penalties for criminal offenses

A. Any person convicted of any of the following offenses may be punished by a fine in any sum not to exceed $5,000 or by imprisonment for a term not to exceed 364 days, or by both such fine and imprisonment:

1. Subsection 11.22.070.B, Licenses and plates required—Penalties—Exceptions;
2. Section 11.22.090, Vehicle trip permits—Restrictions and requirements—Penalty;
3. Section 11.22.200, Special license plates—Hulk hauler;
4. Section 11.23.400, Disabled parking—Enforcement;
5. Section 11.30.340, Vehicle immobilization prohibited;
6. Section 11.55.340, Vehicles carrying explosives, flammable liquids, poison gas, liquefied petroleum gas (LPG) and cryogenics must stop at all railroad grade crossings;
7. Section 11.56.120, Reckless driving;
8. Section 11.56.130, Reckless endangerment of roadway workers;
9. Section 11.56.140, Reckless endangerment of emergency zone workers;
10. Subsection 11.56.320.B, Driving while license is suspended or revoked in the first degree;
11. Subsection 11.56.320.C, Driving while license is suspended or revoked in the second degree;
12. Section 11.56.330, Violation of an occupational, temporary restricted or ignition interlock driver's license;
13. Section 11.56.340, Operation of motor vehicle prohibited while license is suspended or revoked;
14. Section 11.56.350, Operation of a motor vehicle without required ignition interlock or other biological or technical device;
15. Section 11.56.355, Tampering with or assisting another in circumventing an ignition interlock device;
16. Section 11.56.420, Hit and run (attended);
17. Section 11.56.445, Hit and run (by unattended vehicle);
18. Section 11.56.450, Hit and run (pedestrian or person on a device propelled by human power);
19. Section 11.60.690, Transportation of liquified petroleum gas;
20. Section 11.62.020, Flammable liquids, combustible liquids and hazardous chemicals;
21. Section 11.62.040, Explosives;
22. Subsection 11.74.160.B, Failure to secure load in the first degree;
23. Subsection 11.80.140.B, Certain vehicles to carry flares or other warning devices (subsection B only);

24. Subsection 11.80.160.E, Display of warning devices when vehicle disabled (subsection E only);

25. Subsection 11.84.370.D, Using, selling or purchasing a signal preemption device except as authorized;

26. Section 11.84.380, Fire extinguishers;

27. Section 11.86.080, Flammable or combustible labeling;

28. Section 11.86.100, Explosive cargo labeling;

29. Section 11.34.040, with respect to aiding and abetting the foregoing criminal offenses.

B. Any person convicted of any of the following offenses may be punished by a fine in any sum not to exceed $1,000 or by imprisonment for a term not to exceed 90 days, or by both such fine and imprisonment:

1. Section 11.20.010, Driver's license required—Exception—Penalty, unless the person cited for the violation provided the citing officer with an expired driver's license or other valid identifying documentation under RCW 46.20.035 at the time of the stop and was not in violation of Section 11.56.320 or Section 11.56.340, in which case the violation is an infraction;

2. Section 11.20.100, Display of nonvalid driver's license;

3. Section 11.20.120, Loaning driver's license;

4. Section 11.20.140, Displaying the driver's license of another;

5. Section 11.20.160, Unlawful use of driver's license;

6. Section 11.20.200, Unlawful to allow unauthorized person to drive;

7. Subsection 11.20.350.C, Providing false evidence of financial responsibility;

8. Section 11.22.025, Transfer of ownership;

9. Subsection 11.23.400.B, Unlawfully obtaining placard or special license plate;

10. Subsection 11.23.400.C, Unlawful sale of placard or special license plate;

11. Section 11.32.160, Cancellation of citation;

12. Section 11.40.180, Standard of care for drivers of motor vehicles - blind pedestrians carrying white cane or using guide dog;

13. Section 11.40.430, Prohibited entry to no admittance area;

14. Subsection 11.56.320.D, Driving while license is suspended or revoked in the third degree;

15. Section 11.56.430, Hit and run (unattended vehicle)—Duty in case of accident with unattended vehicle;

16. Section 11.56.440, Hit and run (property damage)—Duty in case of accident with property;

17. Subsection 11.58.005.A, Negligent driving in the first degree;

18. Section 11.58.190, Leaving minor children in unattended vehicle;

19. Section 11.59.010, Obedience to peace officers, flaggers, and firefighters;

20. Section 11.59.040, Refusal to give information to or cooperate with officer;

21. Section 11.59.060, Refusal to stop;

22. Section 11.59.080, Examination of equipment;

23. Section 11.59.090, Duty to obey peace officer—Traffic infraction;

24. Section 11.66.240, Obstructing or delaying train;

25. Subsection 11.74.160.C, Failure to secure load in the second degree;

26. Subsection 11.84.370.C, Possessing signal preemption device except as authorized;

27. Section 11.34.040, Aiding and abetting with respect to the criminal offenses in this subsection 11.34.020.B.

(Ord. 124950 , § 6, 2015; Ord. 124686 , § 3, 2015; Ord. 123632, § 11, 2011; Ord. 123420, § 10, 2010; Ord. 123420, § 9, 2010; Ord. 122742, § 7, 2008; Ord. 120885, § 3, 2002; Ord. 119189 , § 5, 1998; Ord. 119011 , § 10, 1998; Ord. 118105, § 3, 1996; Ord. 116872, § 3, 1993; Ord. 116538, § 2, 1993; Ord. 115757, § 1, 1991; Ord. 115040, § 5, 1990; Ord. 112975 , § 2, 1986; Ord. 112466 , § 3, 1985; Ord. 111859 , § 4, 1984: Ord. 109476 , § 3(part), 1980: Ord. 108200 , § 2(11.34.020), 1979.)

11.34.040 - Aiding and abetting violation.

It is unlawful to counsel, aid, or abet the violation of or failure to comply with any of the provisions of this subtitle.

(Ord. 108200 , § 2(11.34.040), 1979.)

Chapter 11.35 - IMMOBILIZATION

Sections:

11.35.010 - Scofflaw list

A. When there are four or more parking citations issued against a vehicle for each of which a person has failed to respond, failed to appear at a requested hearing, or failed to pay amounts due for at least 45 days from the date of the filing of each of those citations, the Seattle Municipal Court shall place the vehicle on a list of scofflaws, and shall mail, by first class mail, a notice to the last known registered owner of the vehicle, as disclosed by the vehicle license number as provided by the Washington State Department of Licensing or equivalent vehicle licensing agency of the state in which the vehicle is registered. If there is no last known address that can be ascertained from the Washington Department of Licensing, or if the vehicle has no Washington vehicle license number or is not registered in the State of Washington, the notice, in the form of a readily visible notification sticker, may be affixed to the vehicle while left within a public right-of-way or other publicly owned or controlled property. A notification sticker may be used in lieu of mailing even if the last known address is ascertainable for vehicles registered in the State of Washington.

B. The registered vehicle owner may request an administrative review at the Seattle Municipal Court at any time that the vehicle is on the scofflaw list until the vehicle has been immobilized or impounded. The review should only examine whether the vehicle is properly on the scofflaw list and shall not review the underlying citations that caused the vehicle to be included on the scofflaw list. The vehicle shall be removed from the list only upon a showing by the registered owner that either:

1. fewer than four of the citations that caused the vehicle to be included on the scofflaw list were committed while the current registered owner was the legal owner of the vehicle; or

2. all amounts due pertaining to the citations that met the criteria for scofflaw under Section 11.35.010 A have been satisfied in full.

C. A vehicle shall remain on the scofflaw list until all outstanding parking infraction penalties, court costs (including but not limited to collection agency remuneration authorized under RCW 3.02.045), default penalties on parking traffic infractions imposed under Section 11.31.120, immobilization release fees imposed under subsection 11.35.020.H, costs of impoundment (including removal,

towing and storage fees) imposed under Section 11.30.120, towing administrative fees imposed under Section 11.30.290 and immobilization administrative fees under subsection 11.35.020.H, and interest, have been paid, or a time payment plan has been arranged with the Seattle Municipal Court or their authorized agent.

D. When a time payment plan is created, the subject vehicle shall be temporarily removed from the scofflaw list and the payment amounts shall be applied on a pro rata basis until all penalties, fines or fees owed relating to all parking citations are satisfied. A vehicle that has been temporarily removed from the scofflaw list shall be returned to the list if the owner defaults on the time payment agreement, in accordance with guidelines adopted by the Seattle Municipal Court.

(Ord. 124558, § 1, 2014; Ord. 123563, § 1, 2011; Ord. 123447, § 1, 2010)

11.35.020 - Immobilization

A. Effective July 1, 2011 and thereafter, if the notice requirements under Section 11.35.010 A have been met, and if parked in public right-of-way or on other publicly owned or controlled property, a vehicle on the scofflaw list may be immobilized by installing on such vehicle a device known as a "boot," which clamps and locks onto the vehicle wheel and impedes vehicle movement. If a vehicle is immobilized, it shall not be released until full payment has been made, or a time payment agreement has been entered into for all outstanding penalties, fines, or fees owed for all parking citations, plus all immobilization, towing, and storage charges and administrative fees.

B. Any vehicle that remains booted for 48 hours or more, not including any of the 48 hours from the beginning of Saturday until the end of Sunday, or which becomes illegally parked while booted, shall be subject to towing and impoundment pursuant to Section 11.30.040. The Seattle Department of Transportation and Seattle Police Department shall issue joint guidelines for vehicle towing related to immobilization, based on Sections 11.30.040 and 11.16.320.

C. The person installing the boot shall leave under the windshield wiper or otherwise attach to the vehicle a notice advising the owner that the vehicle has been booted by the City of Seattle for failure to respond, failure to appear at a requested hearing, and failure to pay amounts due for four or more adjudicated parking infractions for at least 45 days from the date of the last such adjudication issued against the vehicle; that release of the boot may be obtained by paying all outstanding penalties, fines, or forfeitures owed relating to all adjudicated violations, plus all booting, removal, towing, and storage charges and administrative fees; that unless such payment is made within two business days of the date of the notice, the vehicle will be impounded; that it is unlawful for any person to remove or attempt to remove the boot, to damage the boot, or to move the vehicle with the boot attached, unless authorized by the Seattle Police Department or an authorized agent of the City; and that the owner may seek an administrative review of the booting by submitting a request to the Seattle Municipal Court within ten days of the release of the boot. The notice shall further state that the vehicle remains subject to impoundment regardless of whether the owner requests an appeal.

D. The vehicle may be released from immobilization when the vehicle owner or an agent of the owner pays all outstanding parking infraction penalties, court costs (including but not limited to collection agency remuneration authorized under RCW 3.02.045), default penalties on parking traffic infractions imposed under Section 11.31.120, immobilization release fees imposed under subsection 11.35.020.H, costs of impoundment (including removal, towing and storage fees) imposed under Section 11.30.120, towing administrative fees imposed under Section 11.30.290 and immobilization administrative fees under subsection 11.35.020.H, and interest, or enters into a time payment agreement for the payment thereof. Upon full payment or upon entry into a time payment agreement, the Seattle Police Department or other authorized agent of the City shall promptly remove or enable the removal of the boot from the vehicle. If payment is made in full, the vehicle shall be removed from the scofflaw list and shall not be subject to immobilization or impoundment for the paid citations. Upon entry into a time payment agreement, the vehicle shall be temporarily removed from the scofflaw list and shall not be subject to immobilization, provided, however, that the vehicle shall be returned to the scofflaw list and be subject to immobilization if the owner defaults on the time

payment agreement. A registered owner who defaults on a time payment agreement shall not be given another opportunity to make a time payment arrangement and therefore, payment for all outstanding amounts above shall be made in full before the vehicle may be removed from the scofflaw list or released from immobilization or impound. Any person who has previously removed or enabled removal of a booting device in violation of subsection E while on the scofflaw list for any four or more parking infractions, and subsequently is booted a second time while on the scofflaw list for the same parking infractions, shall not be eligible for a time payment plan.

E. No person other than an authorized employee of the Seattle Police Department or an authorized agent of the City shall remove or enable the removal of the boot described in subsection A of this Section from any vehicle on which it has been installed unless the requirements of subsection D have been met.

F. If the Seattle Police Department or an authorized agent of the City enables the vehicle owner to remove the boot, the owner shall return the boot to a location designated by the Department within two calendar days of the removal.

G. No person, other than an authorized employee of the Seattle Police Department or other authorized agent of the City, shall move, by towing or other means, any vehicle after it has been immobilized but before the boot has been removed.

H. The Director of Finance and Administrative Services shall determine and set an immobilization fee and an administrative fee in amounts such that the sum of such fees do not exceed the sum of the lowest impound fee, minimum storage fee, and administrative fee for vehicle impoundment under Section 11.30.120. An administrative fee, if any, shall be levied when the boot is removed. The administrative fee shall be collected by the contractor releasing the vehicle from immobilization, shall be remitted to the Department of Finance and Administrative Services, and shall be deposited in an appropriate account.

I. A person who fails to return the booting device within the time frame required by subsection F of this section may be charged a late fee as determined by the Director of Finance and Administrative Services.

J. A person who intentionally damages the booting device may be charged a replacement fee as determined by the Director of Finance and Administrative Services and also may be prosecuted for the crime of property destruction under section 12A.08.020.

K. The Director of Finance and Administrative Services shall adopt rules governing the imposition of fees under this Section 11.35.020.

(Ord. 124558, § 2, 2014; Ord. 123563, § 2, 2011; Ord. 123447, § 1, 2010)

11.35.030 - Post-immobilization review

The registered vehicle owner may seek a post-deprivation review of the immobilization by submitting a written request to the Seattle Municipal Court within ten days of the placement of the notice on the vehicle, as established by the notice date. Upon timely receipt of such written request, the Seattle Municipal Court shall, within a reasonable time as established by the Court, conduct a review on the issue of whether the immobilization was proper and shall issue a written decision setting forth the reasons on which the decision is based, provided, however, that any previously adjudicated parking infractions that formed the basis of the vehicle's scofflaw status shall not be subject to the review. The person seeking review shall have an opportunity to present evidence on his or her behalf in accordance with requirements established by the Court.

(Ord. 123447, § 1, 2010)

WAC 446-20-260

Auditing of criminal history record information systems.

(1) Every criminal justice agency, including contractors authorized to collect, retrieve, maintain, and disseminate criminal history record information pursuant to WAC 446-20-180, must make its records available under RCW 10.97.090(3) to determine the extent of compliance with the following:

(a) Dissemination records as required under RCW 10.97.050(7);

(b) Security procedures as required by RCW 10.97.090(1); and

(c) Personnel standards as required by RCW 10.97.090(2).

(2) Personnel engaged in the auditing function will be subject to the same personnel security requirement as required under WAC 446-20-230, 446-20-240, and 446-20-250, as employees who are responsible for the management and operation of criminal history record information systems.

[Statutory Authority: Chapters 10.97 and 43.43 RCW. WSR 10-01-109, § 446-20-260, filed 12/17/09, effective 1/17/10. Statutory Authority: RCW 10.97.080 and 10.97.090. WSR 80-08-057 (Order 80-2), § 446-20-260, filed 7/1/80.]

JAY INSLEE
Governor

JOHN R. BATISTE
Chief

STATE OF WASHINGTON
WASHINGTON STATE PATROL
General Administration Building • PO BOX 42602 • Olympia, WA 98504-2602 • (360) 596-4043 • www.wsp.wa.gov

March 11, 2014

Mr. Mark Knutson
Seattle Police Department
610 5th Ave
PO Box 34986
Seattle WA 98104

Dear Mr. Knutson:

Subject: WSP Memorandum of Understanding No. C141174GSC

Enclosed with this letter is one fully executed original of the referenced agreement between the Washington State Patrol and your organization. Please keep this original for your records.

The Washington State Patrol agreement tracking number is the agreement number referenced above; please use this number on all correspondence regarding this agreement. If you need further assistance, please contact Terri Johnson at (360) 596-4063 or terri.johnson@wsp.wa.gov.

Sincerely,

Terri L. Johnson

for Mr. Robert L. Maki, CFE, CGFM
Budget and Fiscal Services

RLM: tlj

Enclosure

WSP No. C141174GSC

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE WASHINGTON STATE PATROL
AND
THE SEATTLE POLICE DEPARTMENT

1. PURPOSE: The purpose of this Memorandum of Understanding (MOU) between the Washington State Patrol (WSP) and the Police Department for the City of the Seattle hereinafter referred to as the "parties", is to memorialize the parties' understanding regarding transmitting, receiving, and storage of information contained in the National Crime Information Center (NCIC) and Washington Crime Information Center (WACIC) systems of records made available through a data transfer program. The data provided by WSP will be used by Seattle Police Department as input to a law enforcement application.

WSP provides NCIC/WACIC data to the Seattle Police Department through WSP's A Central Computerized Enforcement Service System (ACCESS). Department has a separate agreement with WSP regarding access to, use of, and subsequent dissemination of information obtained through ACCESS, including NCIC/WACIC data. This MOU has no affect on that agreement.

2. BACKGROUND: The Federal Bureau of Investigation (FBI) maintains the NCIC system of records containing multiple files. WSP maintains the WACIC system of records containing multiple files. Information included may be stolen vehicles, vehicles wanted in conjunction with felonies, wanted persons, and vehicles subject to seizure based on federal court orders.

The Seattle Police Department has instituted state-of-the-art license plate screening technology from mobile and fixed sites. The Seattle Police Department's vendors provide software and screening devices that have the capability of scanning license plates and searching a local database loaded into a patrol vehicle computer or other locations controlled by the agency. The Seattle Police Department has requested to obtain relatively current information from the NCIC and WACIC files in order to compare scanned numbers against stolen license plates. The Seattle Police Department certifies its vendors providing license plate screening technology do not have access to NCIC/WACIC data provided to the Seattle Police Department by WSP.

3. SCOPE: This MOU applies to WSP making information from the NCIC and WACIC Vehicle File, License Plate File and Wanted Person File available to Seattle Police Department via a secure FTP Server environment.

A. WSP will:

1) Provide the Seattle Police Department with the data elements and disqualifying items are described in Attachment 1, Data Elements and Handling Instructions, which is attached hereto and incorporated herein.

2) Provide updated extract information on a mutually agreed to frequency;

3) Respond to specific inquiries from the Seattle Police Department; and

4) Provide the Seattle Police Department with the name and telephone number of a technical and an administrative point of contact.

B. the Seattle Police Department will:

1) Use the NCIC and WACIC extracts for law enforcement purposes;

2) Update its local database as FBI and WACIC updates become available via WSP, ensuring that those numbers deleted from the NCIC/WACIC system are also deleted from all local databases;

3) Confirm extract hits are still active in NCIC and WACIC, at the earliest reasonable opportunity, in accordance with current hit confirmation policy;

4) Provide the WSP with the name and telephone number of a technical and an administrative point of contact; and

5) Ensure that the Seattle Police Department's use and dissemination of data provided by WSP under this MOU is in accordance with federal and state laws and regulations, including but not limited to the FBI's Criminal Justice Systems Information (CJIS) regulations.

4. FUNDING: Each party will fund its own activities unless otherwise agreed in writing. PCSO has a separate agreement with WSP for use of ACCESS. This MOU has no affect on that agreement, or the rates and fees WSP charges for the services provided thereunder.

5. LIAISON REPRESENTATIVES

For the Washington State Patrol:	For the City of Seattle Police Department:
Mr. Jim Anderson, Administrator	Mr. Mark Knutson, IT Manager
Criminal Records Division	Information Technology Section
PO Box 42619	610 5th Ave , PO Box 34986
Olympia WA 98504-2619	Seattle WA 98104
Phone: (360) -534-2101	Phone: (206) - 684-0970
Fax: (360) – 534-2070	Fax: (206) – 684-5109
E-mail: jim.anderson@wsp.wa.gov	Email: Mark.Knutson@seattle.gov

5. CONFIDENTIAL INFORMATION: The Seattle Police Department acknowledges that some of the material and information that may come into its possession or knowledge in connection with this MOU or its performance may consist of information that is exempt from disclosure to the public or other unauthorized persons under either chapter 42.56 RCW or other state or federal statutes ("Confidential Information"). Confidential Information includes, but is not limited to, names, addresses, Social Security numbers, e-mail addresses, telephone numbers, financial profiles, credit card information, driver's license numbers, medical data, law enforcement records, agency source code or object code, agency security data, or information identifiable to an individual that relates to any of these types of information. The Seattle Police Department agrees to hold Confidential Information in strictest confidence and not to make use of Confidential Information for any purpose other than the performance of this MOU, to release it only to authorized employees requiring such information for the purposes of carrying out this MOU, and not to release, divulge, publish, transfer, sell, disclose, or otherwise make it known to any other party without WSP's

express written consent or as provided by law. Furthermore, the Seattle Police Department's use and dissemination of NCIC data provided by WSP under this MOU is governed by the Seattle Police Department's agreement with WSP regarding access to, use of, and subsequent dissemination of NCIC data and other information obtained through ACCESS.

6. SETTLEMENT OF DISPUTES: Disagreements between the parties arising under or relating to this MOU will be resolved only by consultation between the parties and will not be referred to any other person or entity for settlement.

7. AMENDMENT, TERMINATION, ENTRY INTO FORCE, AND DURATION:

A. All activities of the parties under this MOU will be carried out in accordance to the above-described provisions.

B. This MOU may be amended or terminated by the mutual written consent of the parties' authorized representatives.

c. Either party may terminate this MOU upon 30 days written notification to the other party. The parties will continue participation up to the effective date of termination.

8. This MOU, which consists of eight Sections, will enter into effect upon signature of both parties, will be reviewed annually to determine whether amendments are needed, and will remain in effect until terminated. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

The foregoing represents the understandings reached between the WSP and the Seattle Police Department.

State of Washington Washington State Patrol	Seattle Police Department
John R. Batiste, Chief	Signature
3/10/14	3 DEC 13
Date	Date

Attachment 1

NCIC/WACIC Data Elements and Handling Instructions

1) Data Elements: WSP will transmit to the Seattle Police Department information from the Vehicle File, License Plate File, and vehicle information from the Wanted Person Files.

2) Data Handling

   a) If the Seattle Police Department has no need for a particular class of data, they will delete that data immediately on receipt.

   b) Record updates are accomplished by record replacement. The Seattle Police Department may have to compare a new data file with former files provided by WSP in order to determine any changes.

   c) If a record is present within the Seattle Police Department's application and not present in the transferred file from WSP, the record has been removed for operational reasons by local law enforcement. Reasons for that removal include cancellation of the subject plate, or the vehicle has been located.

   d) The Seattle Police Department will not retain any data file provided by WSP longer than 30 calendar days.

e) The Seattle Police Department will not enter or modify NCIC/WACIC data directly.

3) Schedule: WSP shall refresh the data files provided to the Seattle Police Department in a mutually agreed upon process and at agreed upon intervals. WSP shall notify the Seattle Police Department if files will not be available due to problems or of updated code tables.

4) Problem Reporting: Problem reporting by WASPC under this MOU is governed by Attachment 2, WSP Secure FTP Problem Notification Procedures, which is attached hereto and incorporated into this MOU herein.

Attachment 2

WSP Secure FTP Problem Notification Procedures

- When a problem with acquiring data occurs with the WSP Secure FTP Server, the Seattle Police Department will call WSP ITD Customer Services at (360) 705-5999 or send an e-mail to ITDcustomerservicesg@wsp.wa.gov explaining the issue and having a work order opened. The Seattle Police Department will include identifying information about the Seattle Police Department staff that identified the problem in the explanation with e-mail address and phone number(s).
- The WSP Information Technology Division (ITD) Customer Services group will escalate the work order to the appropriate ITD group.
- That group will notify the Seattle Police Department that the issue is being worked on or has been completed.
- If there is no contact within four business hours, the Seattle Police Department should do a follow-up contact.
- The ITD Customer Services group working the problem may call or send e-mail to the Seattle Police Department in order to determine problem particulars or to request testing. The Seattle Police Department will only call or e-mail that person or group in the context of an existing, open problem, and not for new problems.
- Once the Seattle Police Department is satisfied with the results, the work order will be closed. Another work order should be opened for any new problem with receiving data from the WSP Secure FTP Server. The prior work order can be cited by the Seattle Police Department in any subsequent work orders if it seems relevant.

APPENDIX J: CTO NOTICE OF SURVEILLANCE TECHNOLOGY

Thank you for your department's efforts to comply with the new Surveillance Ordinance, including a review of your existing technologies to determine which may be subject to the Ordinance. I recognize this was a significant investment of time by your staff; their efforts are helping to build Council and public trust in how the City collects and uses data.

As required by the Ordinance (SMC 14.18.020.D), this is formal notice that the technologies listed below will require review and approval by City Council to remain in use. This list was determined through a process outlined in the Ordinance and was submitted at the end of last year for review to the Mayor's Office and City Council.

The first technology on the list below must be submitted for review by March 31, 2018, with one additional technology submitted for review at the end of each month after that. The City's Privacy Team has been tasked with assisting you and your staff with the completion of this process and has already begun working with your designated department team members to provide direction about the Surveillance Impact Report completion process.

Please let me know if you have any questions.

Thank you,

Michael Mattmiller

Chief Technology Officer

Technology	Description	Proposed Review Order
Automated License Plate Recognition (ALPR)	ALPRs are computer-controlled, high-speed camera systems mounted on parking enforcement or police vehicles that automatically capture an image of license plates that come into view and converts the image of the license plate into alphanumeric data that can be used to locate vehicles reported stolen or otherwise sought for public safety purposes and to enforce parking restrictions.	1
Booking Photo Comparison Software (BPCS)	BCPS is used in situations where a picture of a suspected criminal, such as a burglar or convenience store robber, is taken by a camera. The still screenshot is entered into BPCS, which runs an algorithm to compare it to King County Jail booking photos to identify the person in the picture to further investigate his or her involvement in the crime. Use of BPCS is governed by SPD Manual §12.045.	2

Technology	Description	Proposed Review Order
Forward Looking Infrared Real-time video (FLIR)	Two King County Sheriff's Office helicopters with Forward Looking Infrared (FLIR) send a real-time microwave video downlink of ongoing events to commanders and other decision-makers on the ground, facilitating specialized radio tracking equipment to locate bank robbery suspects and provides a platform for aerial photography and digital video of large outdoor locations (e.g., crime scenes and disaster damage, etc.).	3
Undercover/ Technologies	The following groups of technologies are used to conduct sensitive investigations and should be reviewed together. • **Audio recording devices**: A hidden microphone to audio record individuals without their knowledge. The microphone is either not visible to the subject being recorded or is disguised as another object. Used with search warrant or signed Authorization to Intercept (RCW 9A.73.200). • **Camera systems**: A hidden camera used to record people without their knowledge. The camera is either not visible to the subject being filmed or is disguised as another object. Used with consent, a search warrant (when the area captured by the camera is not in plain view of the public), or with specific and articulable facts that a person has or is about to be engaged in a criminal activity and the camera captures only areas in plain view of the public. • **Tracking devices**: A hidden tracking device carried by a moving vehicle or person that uses the Global Positioning System to determine and track the precise location. U.S. Supreme Court v. Jones mandated that these must have consent or a search warrant to be used.	4
Computer-Aided Dispatch (CAD)	CAD is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field.	5

Technology	Description	Proposed Review Order
CopLogic	System allowing individuals to submit police reports on-line for certain low-level crimes in non-emergency situations where there are no known suspects or information about the crime that can be followed up on. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.	6
Hostage Negotiation Throw Phone	A set of recording and tracking technologies contained in a phone that is used in hostage negotiation situations to facilitate communications.	7
Remotely Operated Vehicles (ROVs)	These are SPD non-recording ROVs/robots used by Arson/Bomb Unit to safely approach suspected explosives, by Harbor Unit to detect drowning victims, vehicles, or other submerged items, and by SWAT in tactical situations to assess dangerous situations from a safe, remote location.	8
911 Logging Recorder	System providing networked access to the logged telephony and radio voice recordings of the 911 center.	9
Computer, cellphone and mobile device extraction tools	Forensics tool used with consent of phone/device owner or pursuant to a warrant to acquire, decode, and analyze data from smartphones, tablets, portable GPS device, desktop and laptop computers.	10
Video Recording Systems	These systems are to record events that take place in a Blood Alcohol Concentration (BAC) Room, holding cells, interview, lineup, and polygraph rooms recording systems.	11
Washington State Patrol (WSP) Aircraft	Provides statewide aerial enforcement, rapid response, airborne assessments of incidents, and transportation services in support of the Patrol's public safety mission. WSP Aviation currently manages seven aircraft equipped with FLIR cameras. SPD requests support as needed from WSP aircraft.	12
Washington State Patrol (WSP) Drones	WSP has begun using drones for surveying traffic collision sites to expedite incident investigation and facilitate a return to normal traffic flow. SPD may then request assistance documenting crash sites from WSP.	13
Callyo	This software may be installed on an officer's cell phone to allow them to record the audio from phone communications between law enforcement and suspects. Callyo may be used with consent or search warrant.	14

Technology	Description	Proposed Review Order
I2 iBase	The I2 iBase crime analysis tool allows for configuring, capturing, controlling, analyzing and displaying complex information and relationships in link and entity data. iBase is both a database application, as well as a modeling and analysis tool. It uses data pulled from SPD's existing systems for modeling and analysis.	15
Parking Enforcement Systems	Several applications are linked together to comprise the enforcement system and used with ALPR for issuing parking citations. This is in support of enforcing the Scofflaw Ordinance SMC 11.35.	16
Situational Awareness Cameras Without Recording	Non-recording cameras that allow officers to observe around corners or other areas during tactical operations where officers need to see the situation before entering a building, floor or room. These may be rolled, tossed, lowered or throw into an area, attached to a hand-held pole and extended around a corner or into an area. Smaller cameras may be rolled under a doorway. The cameras contain wireless transmitters that convey images to officers.	17
Crash Data Retrieval	Tool that allows a Collision Reconstructionist investigating vehicle crashes the opportunity to image data stored in the vehicle's airbag control module. This is done for a vehicle that has been in a crash and is used with consent or search warrant.	18
Maltego	An interactive data mining tool that renders graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the internet.	19

Please let me know if you have any questions.

Thank you,

Michael

POWERFUL TECHNOLOGY SOLUTIONS
FOR THE CITY AND PUBLIC WE SERVE

2018 Surveillance Impact Report

AUTOMATED LICENSE PLATE READERS (ALPR) (PATROL)

SEATTLE POLICE DEPARTMENT

January 31, 2019

Seattle
Information Technolog

CONTENTS

SUBMITTING DEPARTMENT SIR RESPONSE 4

2019 POLICY UPDATE 7

SURVEILLANCE IMPACT REPORT OVERVIEW 8

PRIVACY IMPACT ASSESSMENT 9

FINANCIAL INFORMATION 28

EXPERTISE AND REFERENCES 30

RACIAL EQUITY TOOLKIT AND ENGAGEMENT FOR PUBLIC COMMENT WORKSHEET 32

PRIVACY AND CIVIL LIBERTIES ASSESSMENT 42

CTO RESPONSE 49

APPENDIX A: GLOSSARY 58

APPENDIX B: PUBLIC COMMENT DEMOGRAPHICS AND ANALYSIS 60

APPENDIX C: PUBLIC MEETING NOTICE(S) 65

APPENDIX D: MEETING SIGN-IN SHEET(S) 73

APPENDIX E: ALL INDIVIDUAL COMMENTS RECEIVED 101

APPENDIX F: LETTERS FROM ORGANIZATIONS 181

APPENDIX G: EMAILS & LETTERS FROM THE PUBLIC 193

APPENDIX H: PUBLIC COMMENT ANALYSIS METHODOLOGY 199

APPENDIX I: POLICIES AND PROCEDURES GOVERNING ALPR 201

APPENDIX J: CTO NOTICE OF SURVEILLANCE TECHNOLOGY 358

SUBMITTING DEPARTMENT SIR RESPONSE

Seattle
Police Department

Memo

Date: 11/27/2018
To: City Council
From: Deputy Chief Marc Garth Green, Seattle Police Department
Subject: ALPR - Patrol

Description

Automated License Plate Readers (ALPRs) are vehicles equipped with high definition infrared digital cameras that are mounted on the vehicle. SPD has eleven patrol vehicles that are equipped with ALPRs. These eleven patrol vehicles are distributed across SPD's five precincts, and the Canine and Major Crimes Units also each have an ALPR-equipped vehicle. The high-speed cameras capture images of license plates as they move into view, and associated software deciphers, or "reads," the characters on the license plate. These reads are immediately checked a "HotList" that is uploaded into the ALPR system. The Hotlist, formally known as the License Plate Reader File, is a list of license plate numbers from Washington Crime Information Center, the FBI's National Crime Information Center, and SPD's own investigations and may include stolen vehicles, vehicles wanted in conjunction with felonies, and wanted persons. When a match between the ALPR read and the HotList is found, the system will register a "hit." The police officer must verify that the hit was accurate. Only after verification may the officer take further law enforcement action, such as stopping the vehicle. SPD routinely recovers stolen vehicles from ALPR hits.

ALPRs collect the reads, which include the image of the license plate, the computer-interpreted read of the license plate, the date, time, and GPS location of the read. This data is retained exclusively by SPD for 90 days and used in investigations such as homicides, robberies, kidnappings, and Silver and Amber alerts. This data allows investigators to determine whether a suspect vehicle was at the scene of a crime prior to the crime, or is routinely found at a specific location. This technology has been an important tool in solving serious crimes.

Purpose

Seattle Police Department uses ALPR technology to maintain public safety, enforce applicable laws related to stolen vehicles and other crimes, and perform its community caretaking responsibilities. ALPR systems can be used during routine patrol or in specific criminal investigations, e.g., to locate stolen vehicles. Prior to ALPR technology, officers were provided a printed list of wanted and stolen vehicles and had to visually watch for those vehicles while on routine patrol. Now, the ALPR vehicles act as eyes for officers who are driving the ALPR-equipped vehicles, allowing the officers to concentrate on driving while capturing

accurately information that is read by the ALPR system. When the ALPR system hits on a license plate, the officer will then verify the hit by comparing the ALPR data with the license plate on the vehicle to ensure an accurate match.

SPD retains collected ALPR data for 90 days and uses it in investigations such as homicides, rapes, robberies, kidnappings, and Silver and Amber alerts. This data allows investigators to determine whether an identified suspect vehicle was at the scene of a crime prior to the crime, or is routinely found at a specific location. This technology has been an important tool in solving serious crimes.

Benefits to the Public

Our primary concern as a law enforcement agency is to reduce crime and disorder. SPD uses ALPR to help achieve this goal. SPD Patrol uses ALPR to recover stolen vehicles that are often used by thieves in committing other, more serious crimes. ALPR may locate fugitives where vehicle license plate information is available, and ALPR has proven to be an essential tool for locating subjects of Amber and Silver Alerts. SPD also utilizes ALPR to find the vehicles of people who have been reported as suicidal. ALPR has assisted in apprehending murder suspects, rape and robbery suspects, and other serious, violent offenders.

Privacy and Civil Liberties Considerations

During the public comment period, SPD heard concerns about privacy and civil liberties from community members. They raised concerns around the perceived overcollection of data, data-sharing with other agencies, policies that may need updating, and a 90-day retention period for data that is stored onsite at SPD.

SPD recognizes the privacy concerns about the data collected by ALPRs while officers are on routine patrol. Because ALPRs collect license plate information from vehicles, that information could be correlated with other information that may personally identify innocent individuals, determine where they were parked at a given time, track their movements, or be pooled with ALPR data from other agencies. To attempt to mitigate these concerns, SPD requires its officers to follow SPD and City policies, and the laws of the city, state, and federal government. SPD also audits usage of the ALPR systems and access to stored ALPR data, and welcomes independent audits from the Office of the Inspector General. To address specific concerns, please see below:

- **Data-sharing policies**: SPD does not pool its ALPR data with any other agency's data. SPD limits data-sharing with other law enforcement agencies for official law enforcement purposes and requires an audit-trail whenever an SPD officer accesses the ALPR data. Further, SPD complies with the Mayoral Directive dated February 6, 2018, requiring all City departments to seek approval from the Mayor's Office before sharing data and information with ICE. However, individuals may request ALPR data through a public records request, and no court has determined whether ALPR data is exempt from disclosure under the Washington State Public Records Act. Individuals also have the right to inspect their criminal history record information maintained by the department.

- **Overcollection of data**: Patrol ALPR vehicles do not automatically link their captured data to private data such as Department of Licensing information about the registered owner or the driver. Any link between the vehicle and the driver or owner must be instigated by an officer who is inspecting a specific crime. Further, SPD continues to comply with the City's intelligence ordinance (SMC 14.12) which only permits "the collection and recording of information for law enforcement purposes, so long as these police activities do not unreasonably: (a) infringe upon individual rights, liberties, and freedoms guaranteed by the Constitution of the United States or of the State—including, among others, the freedom of speech, press, association, and assembly; liberty of conscience; the exercise of religion; and the right to petition government for redress of grievances; or (b) violate an individual's right to privacy."

- **Ninety-day retention period**: SPD maintains the downloaded data collected by Scofflaw enforcement vehicles for 90 days and then automatically deletes it, which is commensurate with the Washington Secretary of State's retention policy for 911 audio recordings, in-car video recordings unrelated to specific incidents, and recordings of radio transmissions between law enforcement and dispatch staff. SPD investigators use the retained ALPR data to help solve serious offenses such as robberies, shootings, and kidnappings. SPD investigators also use ALPR data to help find vulnerable people, such as with "silver alerts" or at the request of family members concerned about a suicidal loved-one. By maintaining the data for 90 days, SPD balances the privacy concerns of the community with the needs of victims to have their cases solved. Every officer who uses the ALPR vehicles or accesses the ALPR data must comply with SPD policies and city, state, and federal laws.

- **New policies**: SPD recognizes that its current ALPR policy needs updating and anticipates that an updated ALPR policy will be in place by January 31, 2019. In addition, SPD has recently updated its policy related to Foreign Nationals, emphasizing that SPD has no role in immigration enforcement and will not inquire about any person's immigration status. In addition, SPD welcomes the OIG to audit its use of ALPR technologies and data.

Summary

ALPR technology is an effective tool for assisting SPD with a variety of responsibilities, from finding and assisting people in need to solving serious crimes. SPD utilizes this resource thoughtfully and efficiently by deploying ALPR primarily on the City's thoroughfares and streets where stolen vehicles are historically recovered. SPD remains committed to complying with laws, policies, and procedures, and sharing data with law enforcement agencies only for law enforcement purposes.

2019 POLICY UPDATE

Through the course of the completion of this Surveillance Impact Report, SPD recognized the need to update the existing ALPR Policy and on February 1, 2019 the new SPD ALPR policy went into effect. This new policy expanded on the previous by adding definitions of the terms used in the operation of the technology, expanding on the required training for employees prior to access and use of ALPR, detailing authorized and prohibited uses of ALPR, defining response to alerts, detailing how ALPR equipment is to be handled, detailing ALPR administrator roles, defining ALPR data storage and retention, and detailing policy around the release or sharing of ALPR data.

In the interest of transparency, the original SIR documents policy as it stood at the time of completion of the SIR (including public engagement and Working Group review). References to the new policy are placed next to original policy references and will be indicated underneath the section where they originally appeared.

SURVEILLANCE IMPACT REPORT OVERVIEW

The Seattle City Council passed Ordinance 125376, also referred to as the "Surveillance Ordinance", on September 1, 2017. This Ordinance has implications for the acquisition of new technologies by the City, and technologies that are already in use that may fall under the new, broader definition of surveillance.

SMC 14.18.020.B.1 charges the City's Executive with developing a process to identify surveillance technologies subject to the Ordinance. Seattle IT, on behalf of the Executive, developed and implemented a process through which a privacy and surveillance review is completed prior to the acquisition of new technologies. This requirement, and the criteria used in the review process, are documented in Seattle IT Policy PR-02, the "Surveillance Policy".

HOW THIS DOCUMENT IS COMPLETED

As Seattle IT and department staff complete the document, they should keep the following in mind.

- Responses to questions should be in the text or check boxes only; all other information (questions, descriptions, etc.) should **NOT** be edited by the department staff completing this document.
- All content in this report will be available externally to the public. With this in mind, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.

PRIVACY IMPACT ASSESSMENT

PURPOSE

A Privacy Impact Assessment ("PIA") is a method for collecting and documenting detailed information collected in order to conduct an in-depth privacy review of a program or project. A PIA asks questions about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. It also requests information about policies, training and documentation that govern use of the technology. The PIA responses are used to determine privacy risks associated with a project and mitigations that may reduce some or all of those risks. In the interests of transparency about data collection and management, the City of Seattle has committed to publishing all PIAs on an outward facing website for public access.

WHEN IS A PRIVACY IMPACT ASSESSMENT REQUIRED?

A PIA may be required in two circumstances.

1) When a project, technology, or other review has been flagged as having a high privacy risk.
2) When a technology is required to complete the Surveillance Impact Report process. This is one deliverable that comprises the report.

1.0 ABSTRACT

1.1 PLEASE PROVIDE A BRIEF DESCRIPTION (ONE PARAGRAPH) OF THE PURPOSE AND PROPOSED USE OF THE PROJECT/TECHNOLOGY.

Seattle Police Department uses Automated License Plate Reader (ALPR) technology to recover stolen vehicles, to locate subjects of Amber and Silver Alerts and fugitives where vehicle license plate information is available, to assist with active investigations, to facilitate the flow of traffic (by monitoring and enforcing City parking restrictions) and for Scofflaw Ordinance enforcement. This Surveillance Impact Report focuses on SPD use of Patrol ALPR as a necessary law enforcement tool in two capacities:

1. Property Recovery – SPD employs ALPR to locate stolen vehicles (usually abandoned), as well as other vehicles subject to search warrant.
2. Investigation – On occasion, SPD relies on stored ALPR data within the 90-day retention period to assist in criminal investigations by identifying and locating involved vehicles, including locating subjects of Amber and Silver Alerts.

Note that ALPR usage for parking enforcement is discussed in the Surveillance Impact Report entitled "Parking Enforcement Systems."

SPD has nineteen vehicles with ALPR. Eleven of these are Patrol vehicles and eight are Parking Enforcement vehicles. The eleven Patrol vehicles are distributed across SPD's five precincts, the Canine and Major Crimes Units also each have an ALPR-equipped vehicle. Although ALPR use by Patrol differs from ALPR use for Parking Enforcement in some respects as described in this Surveillance Impact Report and in the Parking Enforcement Systems (including ALPR) Surveillance Impact Report, all rules and policies that govern ALPR use by SPD as mentioned in the Parking Enforcement Systems Surveillance Impact Report are applicable in the same manner as they are when ALPR is utilized by Patrol.

SPD does not pool ALPR data with other federal agencies. However, ALPR data is subject to the Public Records Act.

The surveillance technology in this Surveillance Impact Report (SIR) is:

1. **Neology PIPS** mobile license plate recognitions system, which is installed in eleven Patrol vehicles.
2. **Neology Back Office System Software (BOSS),** through which camera reads are interpreted and administrative control is managed. This includes the ability to set and verify retention periods, track and log user activity, view camera "read" and "hit" data, and manage user permissions.

1.2 EXPLAIN THE REASON THE PROJECT/TECHNOLOGY IS BEING CREATED OR UPDATED AND WHY THE PIA IS REQUIRED.

ALPR collects license plate information from vehicles, which could, if unregulated and indiscriminately used, be linked to other data to personally identify individuals' vehicles and determine where they were parked at a given time, track the movements of innocent individuals, or be pooled with ALPR data from other agencies.

2.0 PROJECT / TECHNOLOGY OVERVIEW

2.1 describe the benefits of the project/technology.

The benefit of ALPR is many-fold. Patrol ALPR and Parking Enforcement ALPR assist the City in locating and recovering stolen vehicles. Parking Enforcement ALPR assists the City in managing the flow of traffic (by monitoring and enforcing City Traffic Code provisions). Additionally, both ALPR systems may assist with active investigations by helping to determine the location of vehicles of interest – specifically those that have been identified as being associated with an investigation.

SPD uses ALPR to recover stolen vehicles, which are often used by thieves in committing other crimes. SPD uses ALPR to locate subjects of Amber and Silver Alerts, fugitives where vehicle license plate information is available, and ALPR has proven to be an essential tool for locating vehicles involved in serious crimes. Some examples include:

- A murder, in which the victim who, while dropping off passengers, was confronted and shot. A search of ALPR data located images of the vehicle plate the day of and day after the homicide. The images showed that the vehicle had been painted from black to gold in an attempt to conceal it. This assisted in apprehending the suspect.
- SPD used ALPR to identify a suspect's vehicle parked in the vicinity of a murder. Security video from surrounding businesses showed the suspect vehicle being driven in the area, which was critical in the arrest and charging of the two responsible suspects.
- SPD obtained a partial plate and a description of the car in a drive-by-shooting with three innocent victims. SPD ran several partial plate searches and found one in the ALPR system that had been in the area of the shooting at the time. The vehicle matched the description and led to identification of the vehicle and ultimately to the arrest of the shooting suspects.
- A victim at a charity-operated homeless shelter was threatened and nearly stabbed by an individual who was known only by his first name. The victim reported that the suspect had stabbed people before, was extremely violent, and had left the scene in an agitated state. The victim was able to provide a partial license plate, which with other description information, enabled SPD to use the ALPR database to determine the car was routinely parked under a nearby overpass in the middle of the night. SPD then located the vehicle and the suspect before he hurt anyone else.

2.1 CONTINUED

- A violent robbery in Tukwila involved a stolen VW Toureg. The suspects in that crime were involved in subsequent incidents including gun theft and a road rage incident in which a victim was shot at. Using ALPR data, SPD found several locations where the vehicle had been in the North Precinct area. Photos from the ALPR database provided pictures of the current color of the vehicle as the registration reported a different color. A bulletin describing the vehicle and indicating the possible location assisted SPD in locating the vehicle in north Seattle and arresting the suspects in these violent crimes.
- Snohomish County Detectives asked for assistance locating a stranger rape suspect. Images of the suspect's vehicle had been captured on a convenience store security camera when the victim had been picked up. The security video allowed SPD to read the license plate of the potential suspect vehicle. Using the ALPR system, SPD found that the vehicle had parked several times in a business parking lot in Seattle around the same time every day. This was most likely a work location for a potential suspect. The ALPR led to identification and arrest of the suspect, who worked at the Seattle business.

2.2 PROVIDE ANY DATA OR RESEARCH DEMONSTRATING ANTICIPATED BENEFITS.

Research studies:

- Gierlack, Keith, et al. *License Plate Readers for Law Enforcement: Opportunities and Obstacles*. RAND Corporation. https://www.ncjrs.gov/pdffiles1/nij/grants/247283.pdf
- Roberts, David & Meghann Casanova. *Automated License Plate Recognition Systems: Policy and Operational Guidance for Law.* U.S. Department of Justice. https://www.ncjrs.gov/pdffiles1/nij/grants/239604.pdf

General news reporting about ALPR Benefits:

- "Auto thefts up 10 percent in Seattle's North Police Precinct". Sep. 13, 218. KIRO News. https://www.kiro7.com/news/local/auto-thefts-up-10-percent-in-seattles-north-police-precinct/832872563
- "Suspect in New York murder arrested in Spokane". Kelsie Morgan. Jun. 21, 2018. KXLY News. https://www.kxly.com/news/local-news/suspect-in-new-york-murder-arrested-in-spokane/756515490
- "Man suspect of sexual assault of child arrested for brazen Fremont home-invasion robbery". Mark Gomez. Sep 13, 2018. Mercury News. https://www.mercurynews.com/2018/09/13/fremont-police-arrest-man-suspected-of-home-invasion-robbery-sexual-assault-of-child/
- "Man Sentenced to 7 Years for Northeast DC Gunpoint Carjacking of Nun". Sophia Barnes. Sep 7, 2018. NBC Washington. https://www.nbcwashington.com/news/local/Man-Sentenced-to-7-Years-for-Carjacking-Nun-in-Northeast-DC-Brookland-492714631.html
- "License plate readers help Miami Beach police crack down on crime". Andrew Perez. Jul 31, 2018. ABC 10. https://www.local10.com/news/florida/miami-beach/license-plate-readers-help-miami-beach-police-crack-down-on-crime
- "License plate readers helping police in many ways". Tony Terzi. Sep 5, 2018. FOX 61. https://fox61.com/2018/09/05/license-plate-readers-helping-police-in-many-ways/
- "License plate reader technology scores break in hit-and-run probe". Paul Mueller. Sep 20, 2018. CBS 12. https://cbs12.com/news/local/license-plate-reader-technology-scores-break-in-hit-and-run-probe
- "License-plate scanners result in few 'hits,' but are invaluable in solving crimes, police say". Karen Farkas. Dec 4, 2017. Cleveland.com. https://www.cleveland.com/cuyahoga-county/index.ssf/2017/12/license_plate_readers_result_in_few_hits_but_are_invaluable_in_solving_crimes_police_say.html

2.3 DESCRIBE THE TECHNOLOGY INVOLVED.

ALPR hardware consists of high definition infrared digital cameras that are mounted on eleven Patrol cars (one of which is unmarked).

The high-speed cameras capture images of license plates as they move into view, and associated software deciphers the characters on the plate, using optical character recognition. This interpretation is then immediately checked against any license plate numbers that have been uploaded into the onboard, in-vehicle software system. Twice a day, the License Plate Reader File (known as the HotList), a list of license plate numbers from Washington Crime Information Center (WACIC) and the FBI's National Crime Information Center (NCIC), is uploaded into the ALPR system (via a connection to WACIC), which is a source of "hits" for the license plate reader system. The license plate numbers compiled on the HotList "may be stolen vehicles, vehicles wanted in conjunction with felonies, wanted persons, and vehicles subject to seizure based on federal court orders" (WSP Memorandum of Understanding No. C141174GSC; March 11, 2014). Other sources include the City of Seattle Municipal Court's scofflaw list and content uploaded for over-time and metered parking enforcement (which are covered in the Parking Enforcement Systems SIR). No ALPR data collected by SPD ALPR-equipped Patrol vehicles are automatically uploaded into any system outside of SPD.

SPD contracts with Neology to provide both hardware and software for the PIPS ALPR system, used in Patrol. In addition to the cameras, Neology provides the backend server, known as BOSS, through which camera reads are interpreted and administrative control is managed. This includes the ability to set and verify retention periods, track and log user activity, view camera "read" and "hit" data, and manage user permissions.

The configuration is designed so that the cameras capture the images and filter the reads through the linked software to determine if/when a hit occurs. When the software identifies a hit, it issues an audible alert, and a visual notification informs the user which list the hit comes from – HotList; Scofflaw; time-restricted over time parking.

In ALPR-equipped Patrol vehicles, this triggers a chain of responses from the user that includes visual confirmation that the computer interpretation of the camera image is accurate, and the officer verbally checks with Dispatch for confirmation that the license plate is truly of interest before any action is taken. This is done to ensure the system accurately read a license plate. When an inaccuracy is detected, users may choose to enter a note into the system that the "hit" was a misread.

All data collected by the Patrol ALPR systems (images, computer-interpreted license plate numbers, date, time, and GPS location) are stored on-premises on a secure server within SPD and retained for 90 days. Similar ALPR data collected by three ALPR-equipped Parking Enforcement boot vans equipped with Paylock Bootview software is also stored with Patrol ALPR data in BOSS. After 90 days, all data collected by the patrol and boot van ALPR systems is automatically deleted unless specific data has been exported as serving an investigative purpose – in which case, it is included in an investigation file (see the Surveillance Impact Report for Parking Enforcement Systems (including ALPR) for further information).

2.4 DESCRIBE HOW THE PROJECT OR USE OF TECHNOLOGY RELATES TO THE DEPARTMENT'S MISSION.

Seattle Police Department uses ALPR technology in its pursuit of maintaining public safety and enforcing applicable laws related to stolen vehicles and other crimes. ALPR systems can be used during routine patrol or specific to a criminal investigation e.g., to locate stolen vehicles.

2.5 WHO WILL BE INVOLVED WITH THE DEPLOYMENT AND USE OF THE PROJECT / TECHNOLOGY?

As it relates to Patrol use, each precinct has the ability to utilize one or more of the vehicles at any time. Each precinct determines, based on its unique operational needs, for itself if/when/where it will deploy ALPR-equipped vehicles. Precincts work together to determine how to share the vehicles – dependent on their operational needs. ALPR- equipped vehicles in the Canine and Major Crimes Unit respond to calls and matters City-wide, thus providing coverage across the City.

Only sworn officers that have been trained in its use – carried out by another trained sworn officer and confirmed by the ALPR administrator – can sign out an ALPR-equipped vehicle in Patrol. Each precinct determines which officers will use the ALPR-equipped vehicles at which time, dependent on operational need. Officers assigned to the two specialty units, who have been trained in the use of ALPR, may operate it.

The Technical and Electronic Support Unit (TESU), a unit within SPD maintains administrative control of much of SPD's physical technology. The unit staff is knowledgeable about investigative and forensic technology. TESU's mission is to provide technical assistance to Detectives and Officers in connection with investigations. The BOSS ALPR administrator is a member of TESU. The ALPR administrator monitors and manages user access to the PIPS ALPR system for Patrol. The ALPR administrator purges users from system access when they leave the Department. Housing management of the Patrol ALPR system in one unit makes oversight and accountability more efficient than tasking individual units or precincts with this themselves.

3.0 USE GOVERNANCE

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities are bound by restrictions specified in the Surveillance Ordinance and Privacy Principles and must provide written procedures for how the entity will comply with any restrictions identified.

3.1 DESCRIBE THE PROCESSES THAT ARE REQUIRED PRIOR TO EACH USE, OR ACCESS TO/ OF THE PROJECT / TECHNOLOGY, SUCH AS A NOTIFICATION, OR CHECK-IN, CHECK-OUT OF EQUIPMENT.

Prior to gaining access to the ALPR system, potential users must be trained by other trained officers. Once this training has been verified with the ALPR administrator, users are given access and must log into the system with unique login and password information whenever they employ the technology. They remained logged into the system the entire time that the ALPR system is in operation. The login is logged and auditable. Officers are assigned the vehicles to use while on-shift.

3.2 LIST THE LEGAL STANDARDS OR CONDITIONS, IF ANY, THAT MUST BE MET BEFORE THE PROJECT / TECHNOLOGY IS USED.

ALPR systems can be used during routine patrol or specific to a criminal investigation (i.e., to locate a stolen vehicle), as per SPD Policy 16.170. The policy specifies that the ALPR system administrator will be a member of the Technical and Electronic Support Unit (TESU). It further requires that users must be trained; they must be certified in A Central Computerized Enforcement Service System (ACCESS) – a computer controlled communications system maintained by Washington State Patrol that extracts data from multiple repositories, including Washington Crime Information Center, Washington State Identification System, the National Crime Information Center, the Department of Licensing, the Department of Corrections Offender File, the International Justice and Public Safety Network, and PARKS - and trained in the proper use of ALPR. In addition, the policy limits* use of the technology to strictly routine patrol or criminal investigation. Further, the policy clarifies that users may only access ALPR data when that data relates to a specific criminal investigation**. Records of these requests are purged after 90 days.

Policy Update

*the policy limits use of ALPR to the "search of specific or partial plate(s) and/or vehicle identifiers as related to: a crime in progress, a search of a specific area as it relates to a crime in-progress, a criminal investigation, a search for a wanted person, or community caretaking functions such as locating an endangered or missing person."

** and will complete a "Read Query" justification form documenting the search and applicable case number.

3.3 DESCRIBE THE POLICIES AND TRAINING REQUIRED OF ALL PERSONNEL OPERATING THE PROJECT / TECHNOLOGY, AND WHO HAS ACCESS TO ENSURE COMPLIANCE WITH USE AND MANAGEMENT POLICIES.

SPD Policy 16.170 addresses Automatic License Plate Readers. The policy requires that users must be trained; they must be certified in A Central Computerized Enforcement Service System (ACCESS) – a computer controlled communications system maintained by Washington State Patrol that extracts data from multiple repositories, including Washington Crime Information Center, Washington State Identification System, the National Crime Information Center, the Department of Licensing, the Department of Corrections Offender File, the International Justice and Public Safety Network, and PARKS - and trained in the proper use of ALPR. In addition, the policy limits use of the technology to strictly routine patrol or criminal investigation.* Further, the policy clarifies that users may only access ALPR data when that data relates to a specific criminal investigation. A record of these requests is maintained by the ALPR administrator.

A member of TESU monitors compliance for ALPR use for ALPR-equipped Patrol vehicles.**

Policy Update

* By policy, SPD instruction on ALPR technology will include the appropriate use and collection of ALPR data with emphasis on the requirement to document the reason for any data inquiry. The training will also include any Surveillance Impact Reporting regarding ALPR adopted by the City Council.

** and will update access for approved, trained users. Also the ALPR administrator will assist the Office of Inspector General in conducting periodic audits of the Department's ALPR systems.

4.0 DATA COLLECTION AND USE

Provide information about the policies and practices around the collection and use of the data collected.

4.1 PROVIDE DETAILS ABOUT WHAT INFORMATION IS BEING COLLECTED FROM SOURCES OTHER THAN AN INDIVIDUAL, INCLUDING OTHER IT SYSTEMS, SYSTEMS OF RECORD, COMMERCIAL DATA AGGREGATORS, PUBLICLY AVAILABLE DATA AND/OR OTHER CITY DEPARTMENTS.

Data collected from ALPR include license plate image, computer-interpreted read of the license plate number, date, time, and GPS location.

All ALPR-equipped vehicles upload a daily HotList from the Washington State Patrol that contains national stolen vehicle plate data published daily by the FBI. The Washington State Patrol places the HotList file on a server available through ACCESS to those agencies that have a specific and signed agreement with WSP to access and use the information. The receiving local law enforcement may supplement the list with additional information, such as vehicles sought with reasonable suspicion that they are involved in an incident or vehicles sought pursuant to a warrant. (see the Surveillance Impact Report for Parking Enforcement Systems (including ALPR) for further information regarding ALPR use by Parking Enforcement Officers).

4.2 WHAT MEASURES ARE IN PLACE TO MINIMIZE INADVERTENT OR IMPROPER COLLECTION OF DATA?

When the ALPR system registers a hit, a match to a license plate number listed on the HotList (as described in 2.3 above), the user must verify accuracy before taking any action. For instance, when the system registers a hit on a stolen vehicle, the user must visually verify that the system accurately read the license plate and, if so, must then contact Dispatch to verify accuracy of the hit – that the vehicle is actually listed as stolen. Only then does the user take action.

Unless a hit has been flagged for investigation and exported from the database for this purpose, all captured data is automatically deleted after 90 days, per department retention policy. Data related to a flagged hit is downloaded and maintained with the investigation file for the retention period related to the incident type.

4.3 HOW AND WHEN WILL THE PROJECT / TECHNOLOGY BE DEPLOYED OR USED? BY WHOM? WHO WILL DETERMINE WHEN THE PROJECT / TECHNOLOGY IS DEPLOYED AND USED?

ALPR systems are used in Patrol on a daily basis by authorized sworn users (see 2.5 above). Supervisors within each precinct determine when ALPR-equipped vehicles will be on patrol and by which trained personnel. Detectives may access ALPR data in connection with investigations of criminal incidents based on reasonable suspicion.

4.4 HOW OFTEN WILL THE TECHNOLOGY BE IN OPERATION?

ALPR equipped vehicles are deployed within precincts and Canine and Major Crimes Units based on operational need, as determined by supervisors within each precinct or specialty unit. (See SPD Policy 16.170, 3.3 and 4.3 above).

16.170 - Automatic License Plate Readers*
Effective Date: 8/15/2012
16.170-POL
This policy applies to the use of automatic license plate readers (ALPR) by Department employees.
1. Criminal Intelligence Section has Operational Control
The ALPR system administrator will be a member of the Technical and Electronic Support Unit (TESU).
2. Operators Must be Trained
Operators must be ACCESS certified and trained in the proper use of ALPR.
Training will be administered by TESU and Parking Enforcement, as applicable.
3. ALPR Operation Shall be for Official Department Purposes
ALPR may be used during routine patrol or any criminal investigation.
4. Only Employees With ACCESS Level 1 Certification May Access ALPR Data
Employees are permitted to access ALPR data only when the data relates to a specific criminal investigation.
A record of requests to review stored ALPR data will be maintained by TESU.

Policy Update

***Policy 16.170 has been significantly updated and updates are reflected below:**

16.170-POL – 3 ALPR Equipment
1. ALPR Operators Will Ensure ALPR Cameras Are Properly Affixed to the Assigned Police Vehicle Prior to the Start of Their Shift
Operators will inspect cameras for damage or excessive wear.
2. Operators Will Notify the ALPR Administrator Upon Discovery of any Damaged or Inoperable ALPR Equipment
Operators will document the damage/issue on the Vehicle Damage Report form 1_35 found in Word Templates.
3. Operators Will Activate the ALPR Software and Receive the Automatic Updated Hot List at the Start of Each Shift
ALPR units installed on marked patrol and PEO vehicles will be activated and used at all times unless the operator of the vehicle has not been trained.
4. Operators Will Ensure that the ALPR System is Operational by Confirming all Three Cameras and GPS are Functioning Properly at the Beginning of Their Shift
Operators will alert Seattle ITD and the ALPR administrator of any equipment defects.
5. Operators Will Upload, Their ALPR Data Accumulated from Their Shift to the BOSS Server Prior to Shutting Down Their Computer

4.5 WHAT IS THE PERMANENCE OF THE INSTALLATION? IS IT INSTALLED PERMANENTLY, OR TEMPORARILY?

SPD has eleven patrol vehicles with ALPR cameras that are permanently installed. The vehicles are temporarily collecting data when in use. The data collected is maintained on the SPD internal BOSS ALPR system for 90 days or in investigative files for the retention period related to the incident type. (See 4.2 above).

4.6 IS A PHYSICAL OBJECT COLLECTING DATA OR IMAGES VISIBLE TO THE PUBLIC? WHAT ARE THE MARKINGS TO INDICATE THAT IT IS IN USE? WHAT SIGNAGE IS USED TO DETERMINE DEPARTMENT OWNERSHIP AND CONTACT INFORMATION?

Ten of the eleven ALPR-equipped patrol cars are marked as police vehicles, and the cameras are visible to the naked eye. One patrol car is unmarked, and the camera is not visible to the naked eye.

Additional markings on the ten marked vehicles are unnecessary because the vehicles are plainly marked as police vehicles. Additional markings on the unmarked patrol vehicle would render it ineffective as an investigative tool.

4.7 HOW WILL DATA THAT IS COLLECTED BE ACCESSED AND BY WHOM?

Please do not include staff names; roles or functions only.

All data collected for Parking Enforcement systems are hosted on City SPD servers and are not accessible by vendors without knowledge and/or permission of City personnel. Unlike some ALPR systems, SPD's systems do not "pool" SPD's ALPR data with that collected by other agencies.

Only authorized users can access the data collected by ALPR. Per SPD Policy 16.170, authorized users must access the data only for active investigations and all activity by users in the system is logged and auditable. SPD personnel within specific investigative units have access to ALPR data during its retention window of 90 days, during which time they can reference the data if it relates to a specific investigation.

Data removed from the system/technology and entered into investigative files is securely input and used on SPD's password-protected network with access limited to detectives and identified supervisory personnel.

All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.

4.8 IF OPERATED OR USED BY ANOTHER ENTITY ON BEHALF OF THE CITY, PROVIDE DETAILS ABOUT ACCESS, AND APPLICABLE PROTOCOLS. PLEASE LINK MEMORANDUMS OF AGREEMENT, CONTRACTS, ETC. THAT ARE APPLICABLE.

Access to the Patrol ALPR system front-end and back-end is limited to ALPR-trained officers, authorized SPD administrators, and authorized Seattle City IT administrators.

4.9 WHAT ARE ACCEPTABLE REASONS FOR ACCESS TO THE EQUIPMENT AND/OR DATA COLLECTED?

Users can only access the equipment for purposes earlier outlined– recovery of stolen vehicles to assist with active investigations, Scofflaw Law enforcement, and parking enforcement. Per SPD Policy 16.170, "ALPR may be used during routine patrol or any criminal investigation," and ALPR data may be accessed "only when the data relates to a specific criminal investigation." *

Policy Update

* ALPR systems will only be deployed for official law enforcement purposes. These deployments are limited to:

- Locating stolen vehicles;
- Locating stolen license plates;
- Locating wanted, endangered or missing persons; or those violating protection orders;
- Canvassing the area around a crime scene;
- Locating vehicles under SCOFFLAW; and
- Electronically chalking vehicles for parking enforcement purposes.

ALPR data maintained on BOSS will only be accessed by trained, SPD employees for official law enforcement purposes. This access is limited to:

- Search of specific or partial plate(s) and/or vehicle identifiers as related to:
- A crime in-progress;
- A search of a specific area as it relates to a crime in-progress;
- A criminal investigation; or
- A search for a wanted person; or
- Community caretaking functions such as, locating an endangered or missing person.

Officers/detectives conducting searches in the system will complete the Read Query screen documenting the justification for the search and applicable case number.

ALPR will not be used to intentionally capture images in private area or areas where a reasonable expectation of privacy exists, nor shall it be used to harass, intimidate or discriminate against any individual or group.

4.10 WHAT SAFEGUARDS ARE IN PLACE, FOR PROTECTING DATA FROM UNAUTHORIZED ACCESS (ENCRYPTION, ACCESS CONTROL MECHANISMS, ETC.) AND TO PROVIDE AN AUDIT TRAIL (VIEWER LOGGING, MODIFICATION LOGGING, ETC.)?

Individuals can only access the ALPR system via unique login credentials. Hardware systems can only be accessed in-vehicle (which are assigned by superiors for each shift), and software systems can only be accessed in-vehicle or on-site of SPD. As previously noted, all activity in the system is logged and can be audited.

Further, City IT manages SQL backend that purges ALPR data at the required intervals (90 days). A record of the purge is generated and accessible at any time for verification of purges.

5.0 DATA STORAGE, RETENTION AND DELETION

5.1 HOW WILL DATA BE SECURELY STORED?

All data collected from the ALPR system is stored, maintained, and managed on premises. Retention is automated. Unless a record is identified as being related to a criminal investigation and exported in support of that investigation prior to 90 days, all ALPR data is deleted after 90 days. No backup data is captured or retained.

5.2 HOW WILL THE OWNER ALLOW FOR DEPARTMENTAL AND OTHER ENTITIES, TO AUDIT FOR COMPLIANCE WITH LEGAL DELETION REQUIREMENTS?

ALPR systems maintain access logs on backend servers that are accessible for audit The Office of Inspector General may access all data and audit for compliance at any time.

5.3 WHAT MEASURES WILL BE USED TO DESTROY IMPROPERLY COLLECTED DATA?

Once a license plate has been read, this data is automatically retained. Any action taken as a result of a HotList hit can be contested by involved individuals. Users may make notes in records about license plate data captured that reflects that the hit is a misread, or that the hit was in error. The data unrelated to a specific investigation is retained for 90 days.

All information must be gathered and recorded in a manner that is consistent with SPD Policy 6.060, such that it does not reasonably infringe upon “individual rights, liberties, and freedoms guaranteed by the Constitution of the United States and the State of Washington, including freedom of speech, press, association, and assembly; liberty of conscience the exercise of religion; the right to petition government for redress of grievances; and the right to privacy.”

All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

5.4 WHICH SPECIFIC DEPARTMENTAL UNIT OR INDIVIDUAL IS RESPONSIBLE FOR ENSURING COMPLIANCE WITH DATA RETENTION REQUIREMENTS?

Seattle City IT, in conjunction with SPD's ALPR administrator in the Technical and Electronic Support Unit, is responsible for ensuring compliance with data retention requirements. Additionally, external audits by OIG can review and ensure compliance, at any time.

6.0 DATA SHARING AND ACCURACY

6.1 WHICH ENTITY OR ENTITIES INSIDE AND EXTERNAL TO THE CITY WILL BE DATA SHARING PARTNERS?

SPD has no data sharing partners for ALPR. No person, outside of SPD, has direct access to the PIPS system or the data while it resides in the system or technology.

Data obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law.

Data may be shared with outside entities in connection with criminal prosecutions:

- Seattle City Attorney's Office
- King County Prosecuting Attorney's Office
- King County Department of Public Defense
- Private Defense Attorneys
- Seattle Municipal Court
- King County Superior Court
- Similar entities where prosecution is in Federal or other State jurisdictions

Data may be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

Discrete pieces of data collected by the ALPR may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by SPD Policy 12.050 and 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayor's Directive, dated February 6, 2018.

SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the ALPR system.

6.2 WHY IS DATA SHARING NECESSARY?

Data sharing is necessary for SPD to fulfill its mission as a law enforcement agency and to comply with legal requirements.

6.3 ARE THERE ANY RESTRICTIONS ON NON-CITY DATA USE?

Yes ☒ No ☐

6.3.1 If you answered Yes, provide a copy of the department's procedures and policies for ensuring compliance with these restrictions.

Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

Once disclosed in response to PRA request, there are no restrictions on non-City data use; however, applicable exemptions will be applied prior to disclosure to any requestor who is not authorized to receive exempt content.

6.4 HOW DOES THE PROJECT/TECHNOLOGY REVIEW AND APPROVE INFORMATION SHARING AGREEMENTS, MEMORANDUMS OF UNDERSTANDING, NEW USES OF THE INFORMATION, NEW ACCESS TO THE SYSTEM BY ORGANIZATIONS WITHIN CITY OF SEATTLE AND OUTSIDE AGENCIES?

Please describe the process for reviewing and updating data sharing agreements.

Research agreements must meet the standards reflected in SPD Policy 12.055. Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

Following Council approval of the SIR, SPD must seek Council approval for any material change to the purpose or manner in which ALPR may be used.

6.5 EXPLAIN HOW THE PROJECT/TECHNOLOGY CHECKS THE ACCURACY OF THE INFORMATION COLLECTED. IF ACCURACY IS NOT CHECKED, PLEASE EXPLAIN WHY.

System users are trained to visually verify accuracy, comparing a license plate hit to the physical plate/vehicle that the system read before taking any action. If they note a misread, they can enter a note into the system recognizing the read, as such. If they cannot verify visually, no action is taken.

6.6 DESCRIBE ANY PROCEDURES THAT ALLOW INDIVIDUALS TO ACCESS THEIR INFORMATION AND CORRECT INACCURATE OR ERRONEOUS INFORMATION.

Individuals would not know that their information is collected inaccurately or erroneously in the normal course of ALPR data reading. This would only come to an individual's attention if a user acts on a hit received. Any action taken as a result of a HotList or other hit can be contested by involved individuals. Individuals have the right to challenge citations, alleged code violations, or criminal charges and provide correct information.

Individuals may request records pursuant to the PRA, and individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

7.0 LEGAL OBLIGATIONS, RISKS AND COMPLIANCE

7.1 WHAT SPECIFIC LEGAL AUTHORITIES AND/OR AGREEMENTS PERMIT AND DEFINE THE COLLECTION OF INFORMATION BY THE PROJECT/TECHNOLOGY?

ALPR use is not legally constrained at the local, state, or federal level. Instead, retention of data is restricted. SPD retains license plate data that is not case specific (i.e., related to an investigation) for 90 days.

Case specific data is maintained for the retention period applicable to the specific case type.

7.2 DESCRIBE WHAT PRIVACY TRAINING IS PROVIDED TO USERS EITHER GENERALLY OR SPECIFICALLY RELEVANT TO THE PROJECT/TECHNOLOGY.

For example, police department responses may include references to the Seattle Police Manual.

Users are trained in how to use the system and how to properly access data by other trained SPD users. The TESU administrator confirms the training before providing access to new users.

SPD Policy 12.050 mandates that all employees, including ALPR users, who use terminals that have access to information in WACIC/NCIC files must be certified by completing complete Security Awareness Training (Level 2) with recertification testing required every two years, and all employees also complete City Privacy Training. Failure to comply with ACCESS/NCIC/WACIC user requirements can result in termination of the right to continue using ACCESS services.

7.3 GIVEN THE SPECIFIC DATA ELEMENTS COLLECTED, DESCRIBE THE PRIVACY RISKS IDENTIFIED AND FOR EACH RISK, EXPLAIN HOW IT WAS MITIGATED. SPECIFIC RISKS MAY BE INHERENT IN THE SOURCES OR METHODS OF COLLECTION, OR THE QUALITY OR QUANTITY OF INFORMATION INCLUDED.

Please work with the Privacy Team to identify the specific risks and mitigations applicable to this project / technology.

Each component of data collected, on its own, does not pose a privacy risk. Paired with other known or obtainable information, however, an individual may be able to personally identify owners of vehicles, and then use that information to determine, to a certain degree, where specific vehicles have been located. Because SPD's ALPR cameras are few in number, not fixed in location, vehicles equipped with ALPR generally do not follow the same routes, and the records not related to a specific incident are only retained for 90 days, privacy risk is substantially mitigated because of the limited ability to identify vehicle patterns.

Per SPD Policy 16.170, general users of ALPR are restricted from accessing stored data, except as it relates to a specific criminal investigation. Any activity by a user to access this information is logged and auditable. The Washington Public Records Act requires release of collected ALPR data, however, making it possible for members of the public to make those identification connections on their own if they have access to the information necessary to do so, such as an independent knowledge of a particular individual's license plate number.

7.4 IS THERE ANY ASPECT OF THE PROJECT/TECHNOLOGY THAT MIGHT CAUSE CONCERN BY GIVING THE APPEARANCE TO THE PUBLIC OF PRIVACY INTRUSION OR MISUSE OF PERSONAL INFORMATION?

Examples might include a push of information out to individuals that is unexpected and appears to be intrusive, or an engagement with a third party to use information derived from the data collected, that is not explained in the initial notification.

As mentioned in 7.3, the data could be used to personally identify individuals; however, SPD policy prohibits the use of data collected by ALPR to be used in any capacity beyond its relation to a specific criminal investigation or parking enforcement action. Additionally, all collected data that is not relevant to an active investigation is deleted 90 days after collection.

8.0 MONITORING AND ENFORCEMENT

8.1 DESCRIBE HOW THE PROJECT/TECHNOLOGY MAINTAINS A RECORD OF ANY DISCLOSURES OUTSIDE OF THE DEPARTMENT.

Data collected by ALPR is only disclosed pursuant to the public under the PRA. The only data available for disclosure is that data that remains in the system within the 90-day retention window.

Per SPD Policy 12.080, the Crime Records Unit is responsible to receive and record all requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

Discrete pieces of data collected by ALPR may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by SPD Policy 12.050 and SPD Policy 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayoral Directive, dated February 6, 2018. SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the devices.

Any requests for disclosure are logged by SPD's Crime Records Unit or Legal Unit, as appropriate . Any action taken, and data released subsequently, is then tracked through the request log. Responses to Public Disclosure Requests, including responsive records provided to a requestor, are logged in SPD's GovQA system and retained by SPD for two years after the request is completed.

8.2 WHAT AUDITING MEASURES ARE IN PLACE TO SAFEGUARD THE INFORMATION, AND POLICIES THAT PERTAIN TO THEM, AS WELL AS WHO HAS ACCESS TO THE AUDIT DATA? EXPLAIN WHETHER THE PROJECT/TECHNOLOGY CONDUCTS SELF-AUDITS, THIRD PARTY AUDITS OR REVIEWS.

The ALPR system does not self-audit. Instead, third-party audits exist, as follows: 1) The ALPR administrator has the responsibility of managing the user list and ensuring proper access to the system; 2) The Office of Inspector General (OIG) can conduct an audit at any time. Violations of policy may result in referral to Office of Professional Accountability (OPA).

FINANCIAL INFORMATION

PURPOSE

This section provides a description of the fiscal impact of the surveillance technology, as required by the Surveillance Ordinance.

1.0 FISCAL IMPACT

Provide a description of the fiscal impact of the project/technology by answering the questions below.

1.1 CURRENT OR POTENTIAL SOURCES OF FUNDING: INITIAL ACQUISITION COSTS

Current ☒ Potential ☐

Date of Initial Acquisition	Date of Go Live	Direct Initial Acquisition Cost	Professional Services for Acquisition	Other Acquisition Costs	Initial Acquisition Funding Source
2006 ($3M – purchased by Neology in 2016)	2006	Unable to locate record of initial acquisition. However, costs 2015-2018 $217,297.47			SPD Budget

Notes:

The PIPS ALPR system dates back to 2006, for which limited initial acquisition cost data is available. More recent costs are identified.

1.2 CURRENT OR POTENTIAL SOURCES OF FUNDING: ON-GOING OPERATING COSTS, INCLUDING MAINTENANCE, LICENSING, PERSONNEL, LEGAL/COMPLIANCE USE AUDITING, DATA RETENTION AND SECURITY COSTS.

Current ☐ Potential ☐

Annual Maintenance and Licensing	Legal/compliance, audit, data retention and other security costs	Department Overhead	IT Overhead	Annual Funding Source
N/A				

Notes:

N/A

1.3 COST SAVINGS POTENTIAL THROUGH USE OF THE TECHNOLOGY

These are not quantified; however, potential cost savings may result from enhanced patrol efficiency. The technology increases investigative efficiency by reducing the need to canvass neighboring residences and businesses in efforts to identify involved vehicles following an incident. It may reduce distractions for officers while driving because they do not have to visually scan license plates in search of stolen vehicles.

1.4 CURRENT OR POTENTIAL SOURCES OF FUNDING INCLUDING SUBSIDIES OR FREE PRODUCTS OFFERED BY VENDORS OR GOVERNMENTAL ENTITIES

N/A

EXPERTISE AND REFERENCES

PURPOSE

The following information is provided to ensure that Council has a group of experts to reference while reviewing the completed Surveillance Impact Report ("SIR"). Any individuals or agencies referenced must be made aware ahead of publication that their information has been included. All materials must be available for Council to access or review, without requiring additional purchase or contract.

1.0 OTHER GOVERNMENT REFERENCES

Please list any other government bodies that have implemented this technology and can speak to the implementation of this technology.

Agency, Municipality, etc.	Primary Contact	Description of Current Use
Washington State Patrol		

2.0 ACADEMICS, CONSULTANTS, AND OTHER EXPERTS

Please list any experts in the technology under consideration, or in the technical completion of the service or function the technology is responsible for.

Agency, Municipality, etc.	Primary Contact	Description of Current Use
Bryce Newell, PhD	Brycenewell@uky.edu	"Transparent Lives and the Surveillance State: Policing, New Visibility, and Information Policy" – A Dissertation

3.0 WHITE PAPERS OR OTHER DOCUMENTS

Please list any authoritive publication, report or guide that is relevant to the use of this technology or this type of technology.

Title	Publication	Link
Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement	US Department of Justice (federally-funded grant report)	https://www.ncjrs.gov/pdffiles1/nij/grants/239604.pdf
License Plate Readers for Law Enforcement: Opportunities and Obstacles	Rand Corporation	https://www.ncjrs.gov/pdffiles1/nij/grants/247283.pdf
Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information	66 Maine Law Review 398, 2014 Bryce Clayton Newell	https://cpb-us-w2.wpmucdn.com/wpsites.maine.edu/dist/d/46/files/2014/06/03-Newell.pdf

RACIAL EQUITY TOOLKIT AND ENGAGEMENT FOR PUBLIC COMMENT WORKSHEET

PURPOSE

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit ("RET").

1. To provide a framework for the mindful completion of the Surveillance Impact Reports in a way that is sensitive to the historic exclusion of vulnerable and historically underrepresented communities. Particularly, to inform the public engagement efforts Departments will complete as part of the Surveillance Impact Report.
2. To highlight and mitigate any impacts on racial equity from the adoption and the use of the technology.
3. To highlight and mitigate any disparate impacts on individuals or vulnerable communities.
4. To fulfill the public engagement requirements of the Surveillance Impact Report.

ADAPTION OF THE RET FOR SURVEILLANCE IMPACT REPORTS

The RET was adapted for the specific use by the Seattle Information Technology Departments' ("Seattle IT") Privacy Team, the Office of Civil Rights ("OCR"), and Change Team members from Seattle IT, Seattle City Light, Seattle Fire Department, Seattle Police Department, and Seattle Department of Transportation.

RACIAL EQUITY TOOLKIT OVERVIEW

RACIAL EQUITY TOOLKIT: TO ASSESS POLICIES, INITIATIVES, PROGRAMS, AND BUDGET ISSUES
The vision of the Seattle Race and Social Justice Initiative is to eliminate racial inequity in the community. To do this requires ending individual racism, institutional racism and structural racism. The Racial Equity Toolkit lays out a process and a set of questions to guide the development, implementation and evaluation of policies, initiatives, programs, and budget issues to address the impacts on racial equity.

WHEN DO I USE THIS TOOLKIT?

Early. Apply the toolkit early for alignment with departmental racial equity goals and desired outcomes.

HOW DO I USE THIS TOOLKIT?

With inclusion. The analysis should be completed by people with different racial perspectives.

Step by step. The Racial Equity Analysis is made up of six steps from beginning to completion:

Please refer to the following resources available on the Office of Civil Rights' website here: Creating effective community outcomes; Identifying stakeholders & listening to communities of color; Data resources

1.0 SET OUTCOMES

1.1. SEATTLE CITY COUNCIL HAS DEFINED THE FOLLOWING INCLUSION CRITERIA IN THE SURVEILLANCE ORDINANCE, AND THEY SERVE AS IMPORTANT TOUCHSTONES FOR THE RISKS DEPARTMENTS ARE BEING ASKED TO RESOLVE AND/OR MITIGATE. WHICH OF THE FOLLOWING INCLUSION CRITERIA APPLY TO THIS TECHNOLOGY?

☐ The technology disparately impacts disadvantaged groups.

☐ There is a high likelihood that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service.

☒ The technology collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection.

☐ The technology raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice.

1.2 What are the potential impacts on civil liberties through the implementation of this technology?

Without appropriate policy, license plate data could be paired with other identifiable information about individuals that could be used to identify individuals without reasonable suspicion of having committed a crime, or to data mine for information that is not incidental to any active investigation. SPD Policy 16.170 mitigates this concern by limiting operation to solely routine patrol or criminal investigation.

An additional potential civil liberties concern is that the SPD would over-surveil vulnerable or historically targeted communities, deploying ALPR to diverse neighborhoods more often than to other areas of the City.

1.3 What does your department define as the most important racially equitable community outcomes RELATED TO THE IMPLEMENTATION OF THIS TECHNOLOGY?

Trust in SPD is affected by its treatment of all individuals. Equity in treatment, regardless of actual or perceived race, gender, sex, sexual orientation, country of origin, religion, ethnicity, age, and ability is critical to establishing and maintaining trust.

Per the 2016 Race and Social Justice Initiative Community Survey, measuring "the perspectives of those who live, work, and go to school in Seattle, including satisfaction with City services, neighborhood quality, housing affordability, feelings about the state of racial equity in the city, and the role of government in addressing racial inequities," 56.1% of African American/Black respondents, 47.3% of Multiracial respondents, and 47% of Indian/Alaska Native respondents have little to no confidence in the police to do a good job enforcing the law, as compared with 31.5% of White respondents. Further, while 54.9% of people of color have a great deal or fair amount of confidence in the police to treat people of color and White people equally, 45.1% of people of color have little to no confidence in the police to treat people equitably. This is contrasted with White respondents, of which 67.5% have a great deal or fair amount of confidence in the police to treat people of color and White people equally. This may be rooted in feelings of disparate types of contact with the police, across racial groups. While 14.3% of White respondents, 14.7% of Asian/Pacific Islander respondents, and 16.7% of Latino/Hispanic respondents reported being questioned by the police, charged, or arrested when they had not committed a crime, some communities of color reported much higher rates (American Indian/Alaska Native -52.7%; Black/African American - 46.8%; and Multiracial - 36.8%) of this type of contact with the criminal justice system.

As it relates to ALPR, it is important that SPD continue to follow its policy of limiting use of the technology to strictly routine patrol or criminal investigations and community caretaking functions, as well as limiting access to ALPR data to only instances in which it relates to a specific criminal investigations or community caretaking functions. Further, continuing to audit the system on a regular basis, provides a measure of accountability. In doing so, SPD can mitigate the appearance of disparate treatment of individuals based on factors other than true criminal activity.

1.4 What racial equity opportunity area(s) will be affected by the application of the technology?

- ☐ Education
- ☐ Community Development
- ☐ Health
- ☐ Environment
- ☒ Criminal Justice
- ☐ Jobs
- ☐ Housing
- ☐ Other

1.5 Are there impacts on:

- ☐ Contracting Equity
- ☐ Workforce Equity
- ☐ Immigrant and Refugee Access to Services
- ☐ Inclusive Outreach and Public Engagement
- ☒ Other

2.0 INVOLVE STAKEHOLDERS, ANALYZE DATA

2.1 Departmental conclusions about potential neighborhood impacts of the technology. Are the impacts on geographic areas?

☒ Yes ☐ No

Check all neighborhoods that apply *(see map of neighborhood boundaries in Appendix A: Glossary, under "Seattle Neighborhoods"):*

☒ All Seattle neighborhoods

☐ Ballard
☐ North
☐ Northeast
☐ Central
☐ Lake Union
☐ Southwest
☐ Southeast
☐ Delridge
☐ Greater Duwamish
☐ East District
☐ King County (outside Seattle)

☐ Outside King County. Please describe:

N/A

2.2 What are the racial demographics of those living in the area or impacted by the issue?

(see Stakeholder and Data Resources here.)

The demographics for the City of Seattle: White - 69.5%; Black or African American - 7.9%; Amer. Indian & Alaska Native - 0.8%; Asian - 13.8%; Native Hawaiian & Other Pac. Islander - 0.4; Other race - 2.4%; Two or more races - 5.1%; Hispanic or Latino ethnicity (of any race): 6.6%; Persons of color: 33.7%.

STOP: Department should complete RET questions 2.3 – 6 and Appendices B-I AFTER completing their public comment and engagement requirements.

2.3 Have you completed the following steps to engage the public?

If you have not completed these steps, pause here until public outreach and engagement has been completed. (*See OCR's RET worksheet here for more information about engaging the public at this point in the process to ensure their concerns and expertise are part of analysis.*)

☒ **Create a public outreach plan.** Residents, community leaders, and the public were informed of the public meeting and feedback options via:

☒ Email
☐ Mailings
☐ Fliers
☒ Phone calls
☒ Social media
☐ Other

☒ The following community leaders were identified and invited to the public meeting(s):

☒ American Civil Liberties Union (ACLU)
☒ CARE
☒ Northwest Immigrant Rights
☒ OneAmerica
☒ JACL
☒ For Seattle Police Department only, Community Police Commissions
☒ Other:

[Please describe]

☒ **Engagement for Public Comment #1**

Date of meeting: 10/22/18

Location of meeting: Columbia City Branch Library

Summary of discussion:

See Appendix B for an overview of comments received, and demographics on attendees. See Appendix E for the transcript of all comments received for this technology.

☒ **Engagement for Public Comment #2**

Date of meeting: 10/29/18

Location of meeting: Bertha Knight Landes Room

Summary of discussion:

See Appendix B for an overview of comments received, and demographics on attendees. See Appendix E for the transcript of all comments received for this technology.

☒ **Engagement for Public Comment #3 (if applicable)**

Date of meeting: 10/30/18

Location of meeting: Greenlake Branch Library

Summary of discussion:

See Appendix B for an overview of comments received, and demographics on attendees. See Appendix E for the transcript of all comments received for this technology.

☒ **Collect public feedback via mail and email**

Number of feedback submissions received: 2

Summary of feedback: See Appendix B for an overview of comments received, and demographics on attendees. See Appendix E for the transcript of all comments received for this technology.

Open comment period: October 8, 2018 – November 5, 2018

☐ **Community Technology Advisory Board (CTAB) Presentation**

Date of presentation: N/A

Summary of comments:

N/A

2.4 What does data and conversations with stakeholders tell you about existing racial inequities that influence people's lives and should be taken into consideration when applying/implementing/using the technology?

(See OCR's RET worksheet here for more information; King County Opportunity Maps are a good resource for information based on geography, race, and income.)

SPD has heard concerns that our ALPR data will be shared with other agencies and governments that do not share Seattle's values. Community members have expressed concern that ALPR data will be used for purposes other than law enforcement. SPD has also heard that community members may be concerned that ALPR may be used to track movement of people around sensitive areas, such as local mosques, and may be used to infringe upon people's First Amendment rights.

2.5 What are the root causes or factors creating these racial inequities?

Mitigation strategies will be addressed in 4.1 and 5.3. *Examples: bias in process; lack of access or barriers; lack of racially inclusive engagement.*

Root causes are related to historical over-surveillance and over-enforcement of minor violations in neighborhoods and areas where historically targeted communities reside or congregate.

3.0 DETERMINE BENEFIT AND/OR BURDEN

Provide a description of any potential disparate impact of surveillance on civil rights and liberties on communities of color and other marginalized communities. Given what you have learned from data and from stakeholder involvement…

3.1 How will the technology, or use of the technology increase or decrease racial equity?

What are potential unintended consequences? What benefits may result? Are the impacts aligned with your department's community outcomes that were defined in 1.0?

ALPR is content-neutral; it does not identify the race of the driver or the registered owner of the vehicle. To ensure that SPD continues build trust with community members and increase racial equity, SPD must continue to follow its policy of limiting use of the ALPR cars to strictly routine patrol and use of collected ALPR data to specific criminal investigations or community caretaking functions, as well as limiting access to the ALPR system to authorized SPD personnel. Further, SPD must also continue to audit the system on a regular basis to provide a measure of accountability. In doing so, SPD can mitigate the appearance of disparate treatment of individuals based on factors other than true criminal activity and minimize perceived oversurveillance of areas where historically targeted communities reside or congregate.

3.2 What benefits to the impacted community/demographic may result?

All individuals across Seattle benefit from the use of ALPR to address true criminal activities in the community. SPD can mitigate the appearance of disparate treatment on individuals based on factors other than true criminal activities by limiting the use of ALPR cars and collected data through policy.

3.3 What are potential unintended consequences (both negative and positive potential impact)?

Because SPD does not collect data on the demographics of the vehicle owners or operators, unintended consequences may be difficult to determine. However, because ALPR patrol vehicles are assigned to each precinct and deployed throughout the entire City, SPD that overuse of ALPRs is not occurring in neighborhoods where historically targeted communities reside or congregate.

3.4 Are the impacts aligned with your department's community outcomes that were defined in step 1.0?

Yes. The desired outcome is to ensure that law enforcement occurs throughout the City equitably, so it is important that SPD continue to follow its policy of limiting use of the technology to strictly routine patrol or criminal investigations and community caretaking functions, as well as limiting access to ALPR data to only instances in which it relates to a specific criminal investigations or community caretaking functions.

4.0 ADVANCE OPPORTUNITY OR MINIMIZE HARM

Provide a mitigation plan for the impacts described in step 3.

4.1 How will you address the impacts (including unintended consequences) on racial equity?
What strategies address immediate impacts? What strategies address root causes of inequity listed in 2.5? How will you partner with stakeholders for long-term positive change? If impacts are not aligned with desired community outcomes for surveillance technology (see 1a), how will you re-align your work?

Program Strategies:

SPD will ensure that ALPR vehicles are distributed throughout the City so that specific neighborhoods do not receive the bulk of SPD's ALPR use. SPD will also ensure that is policies related to ALPR and Foreign Nationals are up-to-date and will ensure that all SPD employees comply with the Mayoral Directive, dated February 6, 2018. SPD will also continue to comply with SMC 14.18, the City's Intelligence Ordinance, and ensure that law enforcement personnel shall not "unreasonably infringe upon individuals, rights, liberties and freedoms guaranteed by the Constitution of the United States."

Policy Strategies:

SPD recognizes that its current ALPR policy needs updating and anticipates that an updated policy will be in place by January 31, 2019.* Further, SPD complies with the Mayoral Directive dated February 6, 2018, requiring all City departments to seek approval from the Mayor's Office before sharing data and information with ICE. In addition, SPD has recently updated its policy related to Foreign Nationals, emphasizing that SPD has no role in immigration enforcement and will not inquire about any person's immigration status. In addition, SPD welcomes the OIG to audit its use of ALPR technologies and data.

Policy Update

*Through the course of the completion of this Surveillance Impact Report, SPD recognized the need to update the existing ALPR Policy and on February 1, 2019 the new SPD ALPR policy went into effect. This new policy expanded on the previous by adding definitions of the terms used in the operation of the technology, expanding on the required training for employees prior to access and use of ALPR, detailing authorized and prohibited uses of ALPR, defining response to alerts, detailing how ALPR equipment is to be handled, detailing ALPR administrator roles, defining ALPR data storage and retention, and detailing policy around the release or sharing of ALPR data.

Partnership Strategies:

N/A

5.0 EVALUATE, RAISE RACIAL AWARENESS, BE ACCOUNTABLE

The following information must be provided to the CTO, via the Privacy Office, on an annual basis for the purposes of an annual report to the City Council on the equitable use of surveillance technology. For Seattle Police Department, the equity impact assessments may be prepared by the Inspector General for Public Safety.

The following information does not need to be completed in the SIR submitted to Council, unless this is a retroactive review.

5.1 WHICH NEIGHBORHOODS WERE IMPACTED/TARGETED BY THE TECHNOLOGY over the past year and how many people in each neighborhood were impacted?

☒ All Seattle neighborhoods
☐ Ballard
☐ North
☐ NE
☐ Central
☐ Lake Union
☐ Southwest
☐ Southeast
☐ Greater Duwamish
☒ East District
☐ King County (outside Seattle)
☐ Outside King County. Please describe:

[Respond here, if applicable.]

5.2 Demographic information of people impacted/targeted by the technology over the past year.

To the best of the department's ability, provide demographic information of the persons surveilled by this technology. If any of the neighborhoods above were included, compare the surveilled demographics to the neighborhood averages and City averages.

ALPR does not collect demographic data about the owners or operators of cars that have been captured by the ALPR systems. Each police precinct has an ALPR, so ALPRs are dispatched throughout the city and are focused primarily on major thoroughfares and in locations where stolen vehicles have previously been recovered.

5.3 Which of the mitigation strategies that you identified in step 4 were implemented in the past year?

Specifically, what adjustments to laws and policies should be made to remedy any disproportionate impacts so as to achieve a more equitable outcome in the future.

Type of Strategy (program, policy, partnership)	**Description of Strategy**	**Percent complete of implementation**	**Describe successes and challenges with strategy implementation**
Updated ALPR Policy	Expanding and clarifying SPD's ALPR policies both for Parking Enforcement and Patrol	90%	
Updated Foreign Nationals Policy	Updated SPD policy related to Foreign Nationals	100%	

5.4 HOW HAVE YOU INVOLVED STAKEHOLDERS SINCE THE IMPLEMENTATION/APPLICATION OF THE TECHNOLOGY BEGAN?

☒ Public Meeting(s)
☐ CTAB Presentation
☒ Postings to Privacy webpage seattle.gov/privacy
☒ Other external communications
☐ Stakeholders have not been involved since the implementation/application

5.5 What is unresolved? What resources/partnerships do you still need to make changes?

N/A

6.0 REPORT BACK

Responses to Step 5 will be compiled and analyzed as part of the CTO's Annual Report on Equitable Use of Surveillance Technology.

Departments will be responsible for sharing their own evaluations with department leadership, Change Team Leads, and community leaders identified in the public outreach plan (Step 2c).

PRIVACY AND CIVIL LIBERTIES ASSESSMENT

PURPOSE

This section shall be completed after public engagement has concluded and the department has completed the Racial Equity Toolkit section above. The Privacy and Civil Liberties Assessment is completed by the Community Surveillance Working Group ("Working Group"), per the Surveillance Ordinance which states that the Working Group shall:

> "*[P]rovide to the Executive and the City Council a privacy and civil liberties impact assessment for each SIR that must be included with any departmental request for surveillance technology acquisition or in-use approval. The impact assessment shall include a description of the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities. The CTO shall share with the Working Group a copy of the SIR that shall also be posted during the period of public engagement. At the conclusion of the public engagement period, the CTO shall share the final proposed SIR with the Working Group at least six weeks prior to submittal of the SIR to Council for approval. The Working Group shall provide its impact assessment in writing to the Executive and the City Council for inclusion in the SIR within six weeks of receiving the final proposed SIR. If the Working Group does not provide the impact assessment before such time, the Working Group must ask for a two-week extension of time to City Council in writing. If the Working Group fails to submit an impact statement within eight weeks of receiving the SIR, the department and City Council may proceed with ordinance approval without the impact statement."*

WORKING GROUP PRIVACY AND CIVIL LIBERTIES ASSESSMENT

The Working Group's Privacy and Civil Liberties Impact Assessment (PCLIA) for this technology is below, and is also included in the Ordinance submission package, available as an attachment.

Please note, the Working Group's PCLIA for SPD's Automated License Plate Readers was part of a larger report which included reviews of additional retroactive surveillance technologies not applicable to this Council submission. As such, the Working Group's assessment for these technologies has been removed from this report, and will be made available in the appropriate SIRs, to be submitted to Council at a later date.

From: Seattle Community Surveillance Working Group (CSWG)
To: Seattle City Council

Date: April 23, 2019

Re Privacy and Civil Liberties Impact Assessment for Automated License Plate Recognition, ~~Parking Enforcement Systems, and License Plate Readers~~

Executive Summary

On March 28th, 2019, CSWG received the Surveillance Impact Reports, or SIRs, for the three Automated License Plate Reader (ALPR) surveillance technologies included in Group 1 of the Seattle Surveillance Ordinance technology review process (Automated License Plate Recognition, Parking Enforcement Systems, and License Plate Readers). This document is CSWG's Privacy and Civil Liberties Impact Assessment for those technologies as set forth in SMC 14.18.080(B)(1), which we provide for inclusion in the final SIRs submitted to the City Councils.

This document first details the civil liberties concerns regarding ALPR surveillance technologies in general, and then provides specific concerns and recommendations for each of the three specific ALPR technologies under review.

Our assessment of the ALPR surveillance technologies focuses on three key issues:

1. The use of these systems and the data collected by them for purposes other than those intended.
2. Over-collection and over-retention of data.
3. Sharing of that data with third parties (such as federal law enforcement agencies).

For all three of these systems, the Council should adopt, via ordinance, clear and enforceable rules that ensure, at a minimum, the following:

1. The purposes of ALPR use must be clearly defined, and operation and data collected must be explicitly restricted to those purposes only.
2. Dragnet, suspicionless use of ALPR must be outlawed.
3. Data collected should be limited to license plate images, and no images of vehicles or occupants should be collected.
4. Data retention should be limited to the time needed to effectuate the purpose defined.
5. Data sharing with third parties must be limited to those held to the same restrictions as agency deploying the system.

Background: Civil Liberties Concerns with ALPR Systems

Automated License Plate Reader (ALPR) systems are powerful surveillance technologies that can significantly chill constitutionally protected activities by allowing the government to create a detailed picture of the movements—and therefore the lives—of a massive number of individuals. At the first public meeting seeking comment on the SPD Patrol ALPRs held on October 22, 2018, SPD stated that the ALPR system collects 37,000 license plates in a 24-hour period—which equates to over *13.5 million* scans over a full year. These drivers are not specifically suspected of any crime, which calls into question the scale and purpose of such data collection.

ALPR use creates a massive database of license plate information that allows agencies to comprehensively track and plot the movements of individual cars over time, even when the driver has not broken any law.[1] Such a database enables agencies, including law enforcement, to undertake widespread, systematic surveillance on a level that was never possible before. These surveillance concerns are exacerbated by long data retention periods because aggregate data becomes increasingly invasive and revealing when it is stored for long periods of time (as acknowledged by the U.S. Supreme Court in the *Carpenter* decision[2]). However, existing law in Seattle places no specific limits on the use of ALPR technology or data, meaning an agency can choose whether and how they want to retain data and track vehicle movements.

Currently, the use of ALPR technology in Seattle chills constitutionally protected activities because they can be used to target drivers who visit sensitive places such as centers of religious worship, protests, union halls, immigration clinics, or health centers. Whole communities can be targeted based on their religious, ethnic, or associational makeup, which is exactly what has happened in the United States and abroad. In New York City, police officers drove unmarked vehicles equipped with license plate readers near local mosques as part of a massive program of suspicionless surveillance of the Muslim community.[3] In the U.K., law enforcement agents installed over 200 cameras and license plate readers to target a predominantly Muslim community suburbs of Birmingham.[4] ALPR data obtained from the Oakland Police Department showed that police disproportionately deployed

ALPR-mounted vehicles in low-income communities and communities of color.[5] And the federal Immigration and Customs Enforcement (ICE) agency has sought access to ALPR data in order to target immigrants for deportation.[6]

The foregoing concerns suggest the Council should ensure strong protections in ordinance against the misuse of this technology, regardless of which agency is deploying it and for what purpose.

---

[1] https://www.eff.org/deeplinks/2013/05/alpr

[2] https://www.scotusblog.com/wp-content/uploads/2017/08/16-402-tsac-Scholars-of-Criminal-Procedure-and-Privacy.pdf

[3] https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques

[4] https://www.theguardian.com/uk/2010/jun/04/surveillance-cameras-birmingham-muslims

[5] https://www.eff.org/pages/automated-license-plate-readers-alpr

[6] https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/documents-reveal-ice-using-driver-location-data

Specific Comments and Recommendations

1. Automated License Plate Recognition (ALPR) (Patrol) (SPD)

The initial October 2018 Surveillance Impact Report (SIR) for this technology did not indicate the existence of clear policies imposing meaningful restrictions on the purposes for which ALPR data may be collected or used. The updated January 2019 SIR adds a November 2018 memo from SPD Deputy Chief Marc Garth Green (page 42), which states that SPD anticipates having an updated policy by January 31, 2019. The memo states:

> "**New policies:** SPD recognizes that its current ALPR policy needs updating and anticipates that an updated ALPR policy will be in place by January 31, 2019. In addition, SPD has recently updated its policy related to Foreign Nationals, emphasizing that SPD has no role in immigration enforcement and will not inquire about any person's immigration status. In addition, SPD welcomes the OIG to audit its use of ALPR technologies and data."

Although the updated SIR (with the November 2018 memo addition) was conveyed to CSWG in March 2019, the SIR does not indicate whether or not the new policies mentioned in the November 2018 memo have already been adopted by SPD, nor include those policies.

Additional concerns regarding this technology are listed below. To address these concerns, we recommend that the Council ensure not only that the minimum rules listed above in the Executive Summary apply to ALPR-Patrol Systems by ordinance, but that the issues noted below with SPD's current policies are addressed as set forth in the corresponding recommendations, all of which should be incorporated into the Council's approval of the technology.

SPD's policy:

- Does not impose meaningful restrictions on the purposes for which ALPR data may be collected or used.
  - *Recommendation: SPD's policy must clearly define and meaningfully restrict the purposes for which ALPR data may be collected, accessed, and used. These purposes should be limited to checking vehicles against specified hotlists connected to specific criminal investigations. SPD must have reasonable suspicion that a crime has occurred (in the context of a specifically defined criminal investigation) before examining collected license plate reader data; they must not examine license plate reader data in order to generate reasonable suspicion. While SPD's ALPR policy says there must be a specific criminal investigation in order for ALPR data to be accessed, it does not describe how such an investigation is defined or documented.*
- Does not justify SPD's 90-day retention period. SPD retains ALPR data for 90 days, but examples given in the SIR of crimes solved using ALPRs largely appear to involve immediate matches against a hotlist. We acknowledge that state law and technical considerations may impact this retention period.
  - *Recommendation: SPD's policy must require a shorter retention period of 48 hours at most, during which time it must use the data for the specified purpose, then immediately delete the data. SPD should retain no information at all when a passing vehicle does not match a hot list (particularly given that such data is subject to public disclosure, including to federal agencies).*
- Does not limit data sharing by policy or statute. The sharing of ALPR data with other agencies is of great concern, and SPD states a variety of situations in which such data may be shared (see SIR Section 6.1). However, the policies cited do not make clear the criteria for such sharing, nor any inter-agency agreement that governs such sharing, nor why the

data must be shared in the first place. The November 2018 memo only adds the statement, "SPD limits data-sharing with other law enforcement agencies for official law enforcement purposes," which does not address the concerns above.

  - *Recommendation: SPD's policy must limit sharing of ALPR data to third parties that have a written agreement holding those third parties to the same use, retention, and access rules as SPD; make clear to whom and under what circumstances the data are disclosed; and make publicly available a list of what disclosures have been made to which third parties.*

- Does not make clear whether and how audits of inquires to the system can be conducted (see SIR Sections 4.10 and 8.2, for example). The November 2018 memo does not add any new information.
  - *Recommendation: SPD's policy must include a regular audit system to protect against abuse.*
- Does not make clear how and to what degree Patrol and Parking Enforcement ALPR systems are separated, and whether SPD's policies on ALPR apply to the Parking Enforcement Systems (whose data may be equally prone to misuse).
  - *Recommendation: SPD's policy must include strong protections against abuse that are applied to all ALPR systems.*
- Does not include measures to minimize false matches.
  - *Recommendation: SPD's policy must specific that whenever a hit occurs, an officer, before taking any action, must confirm visually that a plate matches the number and state identified in the alert, confirm that the alert is still active by calling dispatch and, if the alert pertains to the registrant of the car and not the car itself, for example in a warrant situation, develop a reasonable belief that the vehicle's occupant(s) match any individual(s) identified in the alert.*
- Does not include systematic tracking to assess how many crimes each year are actually solved using ALPR data.
  - *Recommendation: SPD's policy must require detailed records of ALPR scans, hits, and crimes solved specifically attributable to those hits, as well as an accounting of how ALPR use varies by neighborhood and demographic*.
- Does not create clear restrictions on who can access the data.
  - *Recommendation: SPD's policy must require access controls on the ALPR databases, with only agents who have been trained in the policies governing such databases permitted access, and with every instance of access logged.*

~~2. Parking Enforcement Systems (Including ALPR) (SPD)~~

~~As with the updated ALPR Patrol SIR, the January 2019 Parking Enforcement Systems SIR includes a November 2018 memo from SPD Deputy Chief Marc Garth Green (page 39) stating that SPD anticipates having an updated policy by January 31, 2019. Again, although the updated SIR was conveyed to CSWG in March 2019, it does not indicate whether or not these new policies have already been adopted by SPD, nor address issues previously highlighted in public comment.~~

~~Particularly given the partly merged nature of the Parking Enforcement and Patrol ALPRs, including use of the Parking Enforcement ALPRs to check vehicle plates against hot lists, the concerns and recommendations stated above with respect to SPD Patrol ALPRs (e.g., data access, clear standards for data sharing with third party entities, clear purpose of sharing, auditing requirements) apply equally to Parking Enforcement Systems. The Council should therefore ensure that the same minimum rules (listed in the Executive Summary) apply to Parking Enforcement Systems via ordinance, and that the issues noted below with SPD's current policies are addressed as set forth in the corresponding recommendations, all of which should be incorporated into the Council's approval of the technology.~~

~~SPD's policy:~~

- ~~Does not make clear how the Parking Enforcement ALPR systems integrate with the Patrol ALPR systems—it appears that some integration occurs at least in the case of the Scofflaw enforcement vans that store collected data in the BOSS system.~~
    - ~~*Recommendation: SPD's policy must require that the data collected by Parking Enforcement ALPR systems is not shared with Patrol ALPR systems.*~~
- ~~Does not make clear whether software and hardware providers (as mentioned in Section 2.3 of the SIR) all contract directly with SPD itself, with each other, or with a third-party entity to provide ALPR and related services.~~
    - ~~*Recommendation: SPD's policy must require all data-sharing relationships to be disclosed to the public in clear terms, and, as stated above in the ALPR Patrol Section, SPD's policy must limit sharing of ALPR data to third parties that have a written agreement holding those third parties to the same use, retention, and access rules as SPD, and requiring disclosure of to whom and under what circumstances the data are disclosed.*~~
- ~~Does not include systematic tracking to assess the numbers of scans, hits, and revenue generated from the Parking Enforcement ALPR systems.~~
    - ~~*Recommendation: SPD's policy must require detailed records of ALPR scans, hits, and revenue generated specifically attributable to those hits, as well as an accounting of how ALPR use varies by neighborhood and demographic.*~~
- ~~Does not make clear whether pictures of the vehicle are being taken in addition to the license plate, and if so, if and for how long these pictures are stored (Section 4.1)~~
    - ~~*Recommendation: SPD's policy must make explicit what photos are taken by the ALPR on Parking Enforcement vehicles, and require the same 48-hour maximum retention period for all photos.*~~

~~3. License Plate Readers (LPR) (SDOT)~~

~~In contrast to the SPD SIRs, the License Plate Readers (SDOT) SIR clearly defines and states meaningful restrictions on the purposes for which LPRs data may be collected, accessed, and used; it states that no license plate data is retained by SDOT or WSDOT; and it states that the license plate information SDOT accesses will never be used as a part of any criminal investigation.~~

~~However, it remains unclear whether SDOT's stated no-retention practice is reflected in written policy. Furthermore, SDOT's use of LPRs poses the concern of data sharing with a state entity (WSDOT). It is unclear whether an explicit agreement exists between SDOT and WSDOT ensuring that WSDOT uses the data only for the purpose of calculating travel times, and deletes the data immediately after such use.~~

~~In addition to the minimum standards stated in the Executive Summary, the Council should in its approval of this technology ensure that:~~

1. ~~The LPR data collected by SDOT is used only for the purpose of calculating travel times, and explicitly never for criminal or law enforcement purposes.~~
2. ~~No LPR data is retained.~~
3. ~~No third party other than SDOT and WSDOT can access the LPR data at any time.~~
4. ~~A written agreement holds WSDOT to the above restrictions.~~

CTO RESPONSE

Memo

Date: 11/17/2020

To: Seattle City Council, Transportation and Utilities Committee

From: Saad Bashir

Subject: CTO Response to the Surveillance Working Group ALPR (including Patrol) SIR Review

---

To the Council Transportation and Utilities Committee Members,

I look forward to continuing to work together with Council and City departments to ensure continued transparency about the use of these technologies and finding a mutually agreeable means to use technology to improve City services while protecting the privacy and civil rights of the residents we serve. Specific concerns in the Working Group comments about ALPRs are addressed in the attached document.

As provided in the Surveillance Ordinance, SMC 14.18.080, this memo outlines the Chief Technology Officer's (CTO's) response to the Surveillance Working Group assessment on the Surveillance Impact Report for Seattle Police Department's Automated License Plate Readers.

Background

The Information Technology Department (ITD) is dedicated to the Privacy Principles and Surveillance Ordinance objectives to provide oversight and transparency about the use and acquisition of specialized technologies with potential privacy and civil liberties impacts. All City departments have a shared mission to protect lives and property while balancing technology use and data collection with negative impacts to individuals. This requires ensuring the appropriate use of privacy invasive technologies through technology limitations, policy, training and departmental oversight.

The CTO's role in the SIR process has been to ensure that all City departments are compliant with the Surveillance Ordinance requirements. As part of the review work for surveillance technologies, ITD's Privacy Office has facilitated the creation of the Surveillance Impact Report documentation, including collecting comments and suggestions from the Working Group and members of the public about these technologies. IT and City departments have also worked collaboratively with the Working Group to answer additional questions that came up during their review process.

Technology Purpose

Seattle Police Department uses Automated License Plate Reader (ALPR) technology to recover stolen vehicles, to locate subjects of Amber and Silver Alerts and fugitives where vehicle license plate information is available, to assist with active investigations, to facilitate the flow of traffic (by monitoring and enforcing City parking restrictions) and for Scofflaw Ordinance enforcement. This Surveillance Impact Report focuses on SPD use of Patrol ALPR as a necessary law enforcement tool in two capacities:

1. Property Recovery – SPD employs ALPR to locate stolen vehicles (usually abandoned), as well as other vehicles subject to search warrant.

2. Investigation – On occasion, SPD relies on stored ALPR data within the 90-day retention period to assist in criminal investigations by identifying and locating involved vehicles, including locating subjects of Amber and Silver Alerts.

Working Group Concerns

In their review, the Working Group has raised concerns about these cameras being used in a privacy impacting way, including video recording, data retention, data sharing, integration with other technologies and secondary uses of recorded video.

UPDATE: Through the course of the completion of the Surveillance Impact Report, SPD recognized the need to update the existing ALPR Policy and on February 1, 2019 the new SPD ALPR policy went into effect. This new policy expanded on the previous version by adding definitions of the terms used in the operation of the technology, expanding on the required training for employees prior to access and use of ALPR, detailing authorized and prohibited uses of ALPR, defining response to alerts, detailing how ALPR equipment is to be handled, detailing ALPR administrator roles, defining ALPR data storage and retention, and detailing policy around the release or sharing of ALPR data.

We believe that the updated policy, training and technology limitations enacted by SPD provide adequate mitigation for the potential privacy and civil liberties concerns raised by the Working Group about the use of this important operational technology.

Response to Specific Concerns: SPD ALPR

Concern: Policy does not impose meaningful restrictions on the purposes for which ALPR data may be collected or used.

CTO Assessment: SPD Policy outlines the specific situations or use cases that ALPR can be both used for and under which the data can be accessed. The specific limitations on use preclude a scenario of "dragnet" use where ALPR is constantly in use as a patrol vehicle moves throughout the City. The criteria outlined match with public safety functions where the use of technology allows for more effective outcomes and efficiency gains. Regarding data access, when ALPR data is used for an investigation, the creation of the "Read Query" justification creates an auditable trail of access to data to ensure it meets specified requirements under Policy 16.170

SIR Response:

Section 3.2 What legal standards or conditions, if any, that must be met before the Project / technology is used?

ALPR systems can be used during routine patrol or specific to a criminal investigation (i.e., to locate a stolen vehicle), as per SPD Policy 16.170. The policy specifies that the ALPR system administrator will be a member of the Technical and Electronic Support Unit (TESU). It further requires that users must be trained; they must be certified in A Central Computerized Enforcement Service System (ACCESS) – a computer controlled communications system maintained by Washington State Patrol that extracts data from multiple repositories, including Washington Crime Information Center, Washington State Identification System, the National Crime Information Center, the Department of Licensing, the Department of Corrections Offender File, the International Justice and Public Safety Network, and PARKS - and trained in the proper use of ALPR. In addition, the policy limits use of the technology to strictly routine patrol or criminal investigation. Further, the policy clarifies that users may only access ALPR data

when that data relates to a specific criminal investigation. Records of these requests are purged after 90 days.

New SPD Policy:

- The policy limits use of ALPR to the "search of specific or partial plate(s) and/or vehicle identifiers as related to: a crime in progress, a search of a specific area as it relates to a crime in-progress, a criminal investigation, a search for a wanted person, or community caretaking functions such as locating an endangered or missing person."
- Further, the policy clarifies that users may only access ALPR data when that data relates to a specific criminal investigation and will complete a "Read Query" justification form documenting the search and applicable case number.

Section 4.3 How and when will the project/technology be deployed or used? By whom? Who will determine when the project/technology is deployed and used?

ALPR systems are used in Patrol on a daily basis by authorized sworn users. Supervisors within each precinct determine when ALPR-equipped vehicles will be on patrol and by which trained personnel. Detectives may access ALPR data in connection with investigations of criminal incidents based on reasonable suspicion.

Concern: Policy does not justify SPD's 90-day retention period.

CTO Assessment: Individual city departments do not have the ability to set their own retention schedules, and in many cases must follow requirements set by the State of Washington. Regarding criminal justice data, there are additional requirements to ensure that the quality and availability of data follows legally required retention periods, ensuring that data is preserved after the investigation in case of any dispute. The data is protected and only accessible by those who are related to the investigation.

SIR Response:
Section 5.1 How will data be securely stored?

All data collected from the ALPR system is stored, maintained, and managed on premises. Retention is automated. Unless a record is identified as being related to a criminal investigation and exported in support of that investigation prior to 90 days, all ALPR data is deleted after 90 days. No backup data is captured or retained.

Section 5.3 What measures will be used to destroy improperly collected data?

Once a license plate has been read, this data is automatically retained. Any action taken as a result of a HotList hit can be contested by involved individuals. Users may make notes in records about license plate data captured that reflects that the hit is a misread, or that the hit was in error. The data unrelated to a specific investigation is retained for 90 days.

Section 5.4 Which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

Seattle IT, in conjunction with SPD's ALPR administrator in the Technical and Electronic Support Unit, is responsible for ensuring compliance with data retention requirements. Additionally, external audits by OIG can review and ensure compliance at any time.

Concern: SPD's policy does not limit data sharing by policy or statute.

CTO Assessment: While civil liberties groups have expressed great concern with this practice in other jurisdictions, it is important to note that SPD does not "pool" data with other agencies that create a large database of license plates. SPD's revised policy 16.170 addresses data sharing and states, "ALPR data will only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law." Specific examples of these agencies are outlined in the SIR documentation.

SIR Response:
Section 4.7 How will data that is collected be accessed and by whom?

- All data collected for Parking Enforcement systems are hosted on City SPD servers and are not accessible by vendors without knowledge and/or permission of City personnel. Unlike some ALPR systems, SPD's systems do not "pool" SPD's ALPR data with that collected by other agencies.
- Only authorized users can access the data collected by ALPR. Per SPD Policy 16.170, authorized users must access the data only for active investigations and all activity by users in the system is logged and auditable. SPD personnel within specific investigative units have access to ALPR data during its retention window of 90 days, during which time they can reference the data if it relates to a specific investigation.
- Data removed from the system/technology and entered into investigative files is securely input and used on SPD's password-protected network with access limited to detectives and identified supervisory personnel.
- All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.

Section 6.1 Which entity or entities inside and external to the city will be data sharing partners?

- SPD has no data sharing partners for ALPR. No person, outside of SPD, has direct access to the PIPS system or the data while it resides in the system or technology.
- Data obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law.
- Data may be shared with outside entities in connection with criminal prosecutions:
    - Seattle City Attorney's Office
    - King County Prosecuting Attorney's Office
    - King County Department of Public Defense
    - Private Defense Attorneys
    - Seattle Municipal Court
    - King County Superior Court

  - Similar entities where prosecution is in Federal or other State jurisdictions
- Data may be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.
- Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."
- Discrete pieces of data collected by the ALPR may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by SPD Policy 12.050 and 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayor's Directive, dated February 6, 2018.
- SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the ALPR system.

Section 6.2 Why is data sharing necessary?
Data sharing is necessary for SPD to fulfill its mission as a law enforcement agency and to comply with legal requirements.

Section 6.3.1 Are there any restrictions on non-city data use?

- Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.
- Once disclosed in response to PRA request, there are no restrictions on non-City data use; however, applicable exemptions will be applied prior to disclosure to any requestor who is not authorized to receive exempt content.

Concern: Policy does not make clear whether and how audits of inquiries to the system can be conducted.

CTO Assessment: SPD's Policy 16.170 outlines that the Office of Inspector General (OIG) is responsible for conducting periodic audits of the ALPR system, with support offered by system administrators, as necessary. According to the ALPR policy, the "system records when an employee accesses ALPR data by logging the employee's name, the date and the time of the request." These records are accessible by OIG at any time to ensure compliance.

SIR Response:
Section 5.2 How will the owner allow for departmental and other entities, to audit for compliance with legal deletion requirements?

ALPR systems maintain access logs on backend servers that are accessible for audit The Office of Inspector General may access all data and audit for compliance at any time.

Concern: Policy does not include measures to minimize false matches.

CTO Assessment: This concern is adequately covered in the SIR. SPD Policy 16.170 outlines confirmation of alerts or "hits". Users of ALPR systems must visually verify that the system has made an accurate match, and the system does not make any determinations on actions taken. The system does automatically match plates if they appear on the HotList; these must be verified by both the user and Dispatch to confirm that the information is accurate.

SIR Response:
Section 4.2 What measure are in place to minimize inadvertent or improper collection of data?

When the ALPR system registers a hit, a match to a license plate number listed on the HotList (as described in 2.3), the user must verify accuracy before taking any action. For instance, when the system registers a hit on a stolen vehicle, the user must visually verify that the system accurately read the license plate and, if so, must then contact Dispatch to verify accuracy of the hit – that the vehicle is actually listed as stolen. Only then does the user take action.

New SPD Policy

16.170-POL 2.4

ALPR Operators Will Respond to Hits/Alerts by Confirming the ALPR Information

When an operator receives a Hit/alert indicating a positive Hit from the Hotlist database, a digital image of the license plate will be displayed on the mobile data computer screen.

- ALPR operators will compare the digital image of the license plate to the Hotlist information to verify the Hit for both the state and characters on the plate.
- ALPR operators will confirm the ALPR information by radio or Mobile Data Computer (MDC) to immediately confirm the Hit prior to taking enforcement or other type of police action (absent exigent circumstances).
- ALPR operators will enter a disposition for all ALPR Hits by selecting either "Accept" or "Misread" before removing the Hit from the computer screen.

Dispositions include:

- Stolen Recovery – Arrest;
- Stolen Recovery – No Arrest;
- Eluded – Lost;
- Plates only;
- SCOFLAW; and
- Wanted person or vehicle Misread/Twin plate
- Positive ALPR hits leading to action requiring an incident report will be documented within the report narrative.

Concern: Policy does not include systematic tracking to assess how many crimes each year are actually solved using ALPR data.

CTO Assessment: While there is no systematic tracking of specific crimes solved using ALPR, auditing and reporting requirements, as outlined in SMC 14.18.060, require an Annual Surveillance Usage Review conducted by the Inspector General for Public Safety. The completed report should address usage patterns of this technology, as well as frequency and location of use.

SIR Response:
RET Section 5.2

ALPR does not collect demographic data about the owners or operators of cars that have been captured by the ALPR systems. Each police precinct has an ALPR, so ALPRs are dispatched throughout the city and are focused primarily on major thoroughfares and in locations where stolen vehicles have previously been recovered.

Section 5.3 What measures will be used to destroy improperly collected data?

- Once a license plate has been read, this data is automatically retained. Any action taken as a result of a HotList hit can be contested by involved individuals. Users may make notes in records about license plate data captured that reflects that the hit is a misread, or that the hit was in error. The data unrelated to a specific investigation is retained for 90 days.
- All information must be gathered and recorded in a manner that is consistent with SPD Policy 6.060, such that it does not reasonably infringe upon "individual rights, liberties, and freedoms guaranteed by the Constitution of the United States and the State of Washington, including freedom of speech, press, association, and assembly; liberty of conscience the exercise of religion; the right to petition government for redress of grievances; and the right to privacy."
- All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

Section 6.5 Explain how the project/technology checks the accuracy of the information collected. If accuracy is not checked, please explain why.

System users are trained to visually verify accuracy, comparing a license plate hit to the physical plate/vehicle that the system read before taking any action. If they note a misread, they can enter a note into the system recognizing the read, as such. If they cannot verify visually, no action is taken.

Section 6.6 Describe any procedures that allow individuals to access their information and correct inaccurate or erroneous information.

- Individuals would not know that their information is collected inaccurately or erroneously in the normal course of ALPR data reading. This would only come to an individual's attention if a user acts on a hit received. Any action taken as a result of a HotList or other hit can be contested by involved individuals. Individuals have the right to challenge citations, alleged code violations, or criminal charges and provide correct information.
- Individuals may request records pursuant to the PRA, and individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

Concern: Policy does not create clear restrictions on who can access the data.

CTO Assessment: SPD Policy clearly states that only authorized users within the Department can access the data collected by ALPR; all access is logged and auditable. Authorized users must undergo and meet the training requirements necessary before accessing the data. Additionally, as outlined in previous responses, there are restrictions on who data is shared with outside of the organization.

SIR Response:
Section 4.7 How will data that is collected be accessed and by whom?

- All data collected for Parking Enforcement systems are hosted on City SPD servers and are not accessible by vendors without knowledge and/or permission of City personnel. Unlike some ALPR systems, SPD's systems do not "pool" SPD's ALPR data with that collected by other agencies.
- Only authorized users can access the data collected by ALPR. Per SPD Policy 16.170, authorized users must access the data only for active investigations and all activity by users in the system is logged and auditable. SPD personnel within specific investigative units have access to ALPR data during its retention window of 90 days, during which time they can reference the data if it relates to a specific investigation.
- Data removed from the system/technology and entered into investigative files is securely input and used on SPD's password-protected network with access limited to detectives and identified supervisory personnel.
- All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.

Section 5.1 How will data be securely stored?

All data collected from the ALPR system is stored, maintained, and managed on premises. Retention is automated. Unless a record is identified as being related to a criminal investigation and exported in support of that investigation prior to 90 days, all ALPR data is deleted after 90 days. No backup data is captured or retained.

New SPD Policy

Only Employees Trained in the Use of ALPR Equipment Will Use and Access ALPR Devices and Data

- Before employees operate the ALPR system or access ALPR data, they will complete Department training on the proper and lawful use of the system.
- Parking Enforcement Officers (PEOs) will not have access to stored ALPR data in BOSS.
- Only trained Department employees can access stored ALPR data and all data search requests are logged within the system.

Concern: Policy does not make clear how and to what degree Patrol and Parking Enforcement ALPR systems are separated, and whether SPD's policies on ALPR apply to the Parking Enforcement Systems.

CTO Assessment: According to SPD policy, Autovu data (parking enforcement system) is used only during a shift of a Parking Enforcement Officer and is not retained after the completion of their shift. Patrol ALPR data is retained for 90 days. The two programs have separate ALPR administrators that are responsible for access and maintenance of each system. Parking Enforcement Officers do not have access to stored ALPR data in the Patrol system. The Parking Enforcement SIR outlines the acceptable uses for ALPR which is primarily used for Scofflaw enforcement, or enforcement of time-restricted parking areas and restricted parking zones. The system may also be used for identifying stolen vehicles or sought in connection with criminal investigation to be reported to Dispatch.

SIR Response:
Section 4.9 What are acceptable reasons for access to the equipment and/or data collected?
Users can only access the equipment for purposes earlier outlined– recovery of stolen vehicles to assist with active investigations, Scofflaw Law enforcement, and parking enforcement. Per SPD Policy 16.170, "ALPR may be used during routine patrol or any criminal investigation," and ALPR data may be accessed "only when the data relates to a specific criminal investigation."

New SPD Policy:

ALPR systems will only be deployed for official law enforcement purposes. These deployments are limited to:

- Locating stolen vehicles;
- Locating stolen license plates;
- Locating wanted, endangered or missing persons; or those violating protection orders;
- Canvassing the area around a crime scene;
- Locating vehicles under SCOFFLAW; and
- Electronically chalking vehicles for parking enforcement purposes.

ALPR data maintained on BOSS will only be accessed by trained, SPD employees for official law enforcement purposes. This access is limited to:

- Search of specific or partial plate(s) and/or vehicle identifiers as related to:
- A crime in-progress;
- A search of a specific area as it relates to a crime in-progress;
- A criminal investigation; or
- A search for a wanted person; or
- Community caretaking functions such as, locating an endangered or missing person.

Officers/detectives conducting searches in the system will complete the Read Query screen documenting the justification for the search and applicable case number.

ALPR will not be used to intentionally capture images in private area or areas where a reasonable expectation of privacy exists, nor shall it be used to harass, intimidate or discriminate against any individual or group.

APPENDIX A: GLOSSARY

Accountable: (Taken from the Racial Equity Toolkit.) Responsive to the needs and concerns of those most impacted by the issues you are working on, particularly to communities of color and those historically underrepresented in the civic process.

Community Outcomes: (Taken from the Racial Equity Toolkit.) The specific result you are seeking to achieve that advances racial equity.

Contracting Equity: (Taken from the Racial Equity Toolkit.) Efforts to achieve equitable racial outcomes in the way the City spends resources, including goods and services, consultants and contracting.

DON: "Department of Neighborhoods."

Immigrant and Refugee Access to Services: (Taken from the Racial Equity Toolkit.) Government services and resources are easily available and understandable to all Seattle residents, including non-native English speakers. Full and active participation of immigrant and refugee communities exists in Seattle's civic, economic and cultural life.

Inclusive Outreach and Public Engagement: (Taken from the Racial Equity Toolkit.) Processes inclusive of people of diverse races, cultures, gender identities, sexual orientations and socio-economic status. Access to information, resources and civic processes so community members can effectively engage in the design and delivery of public services.

Individual Racism: (Taken from the Racial Equity Toolkit.) Pre-judgment, bias, stereotypes about an individual or group based on race. The impacts of racism on individuals including white people internalizing privilege, and people of color internalizing oppression.

Institutional Racism: (Taken from the Racial Equity Toolkit.) Organizational programs, policies or procedures that work to the benefit of white people and to the detriment of people of color, usually unintentionally or inadvertently.

Neology Back Office System Software (BOSS): System through which ALPR camera reads are interpreted and administrative control is managed. This includes the ability to set and verify retention periods, track and log user activity, view camera "read" and "hit" data, and manage user permissions.

Neology PIPS: Mobile license plate recognitions system installed in eleven Patrol vehicles.

OCR: "Office of Arts and Culture."

Opportunity Areas: (Taken from the Racial Equity Toolkit.) One of seven issue areas the City of Seattle is working on in partnership with the community to eliminate racial disparities and create racial equity. They include: Education, Health, Community Development, Criminal Justice, Jobs, Housing, and the Environment.

Racial Equity: (Taken from the Racial Equity Toolkit.) When social, economic and political opportunities are not predicted based upon a person's race.

Racial Inequity: (Taken from the Racial Equity Toolkit.) When a person's race can predict their social, economic, and political opportunities and outcomes.

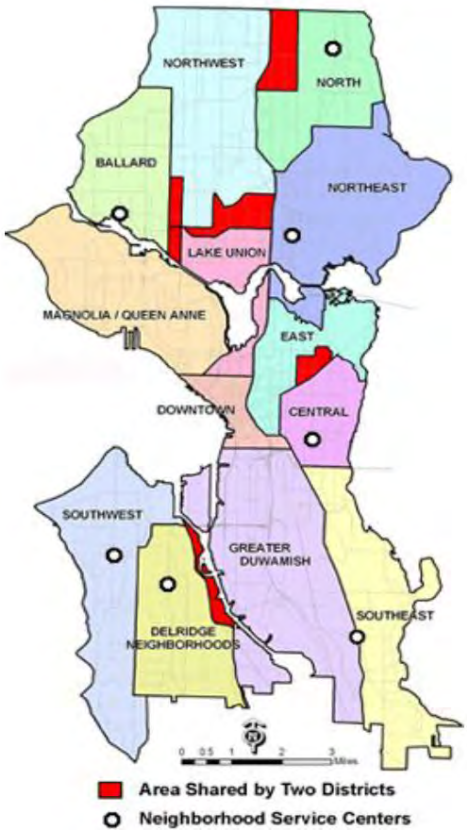
RET: "Racial Equity Toolkit"

Seattle Neighborhoods: (Taken from the Racial Equity Toolkit Neighborhood.) Boundaries defined for the purpose of understanding geographic areas in Seattle.

Stakeholders: (Taken from the Racial Equity Toolkit.) Those impacted by proposed policy, program, or budget issue who have potential concerns or issue expertise. Examples might include: specific racial/ethnic groups, other institutions like Seattle Housing Authority, schools, community-based organizations, Change Teams, City employees, unions, etc.

Structural Racism: (Taken from the Racial Equity Toolkit.) The interplay of policies, practices and programs of multiple institutions which leads to adverse outcomes and conditions for communities of color compared to white communities that occurs within the context of racialized historical and cultural conditions.

Surveillance Ordinance: Seattle City Council passed Ordinance 125376, also referred to as the "Surveillance Ordinance."



SIR: "Surveillance Impact Report", a document which captures the fulfillment of the Council-defined Surveillance technology review process, as required by Ordinance 125376.

TESU: "Technical and Electronic Support Unit"

Workforce Equity: (Taken from the Racial Equity Toolkit.) Ensure the City's workforce diversity reflects the diversity of Seattle.

APPENDIX B: PUBLIC COMMENT DEMOGRAPHICS AND ANALYSIS

OVERVIEW OF PUBLIC COMMENT ANALYSIS

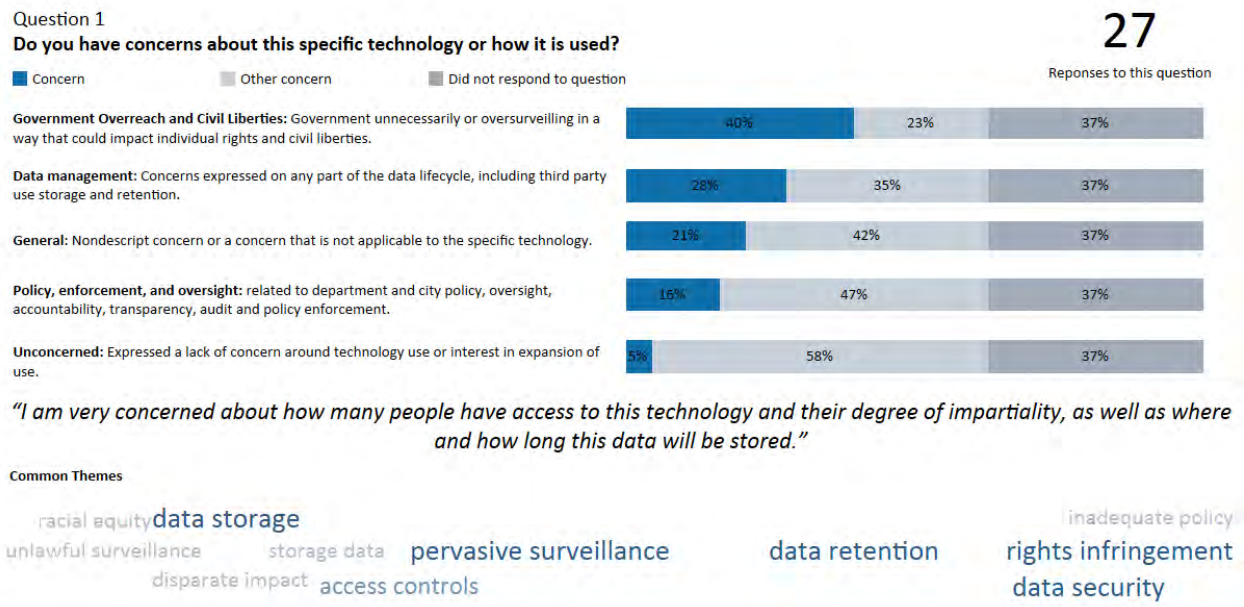
Analysis of public comments was completed using a combination of thematic analysis and qualitative coding. Comments were gathered from many sources, from public engagement meetings, an online survey form, letters, emails, and focus group discussions. All comments may be reviewed in the Surveillance Impact Report, Appendix E.

After assigning a theme and code for the content, City staff conducted an analysis using R. A high-level summary of the results of this analysis are shown below. A detailed description of the methodology is available in the Surveillance Impact Report, Appendix H.

Below is a summary of the responses by question, prepared by Privacy Office staff. This data includes comments from all submission methods (e.g. letter, email, public meeting, etc.). The total number of responses to this question is in the top right. The percentage of responses to that question, following the identified theme is shown in dark blue. The dark gray shows the percent of comments for this technology that did not answer that specific question. The light gray shows the percent of responses to that question that fall into other themes, (General, Data Management, Policy, Enforcement, and Oversight, etc.).

A word cloud of each qualitative sub-code identified appears at the bottom of each question to provide more context of the question response themes. If an appropriate quote could be identified to capture the overall tone of the majority of comments it was included.

COMMENTS SPECIFICALLY ADDRESSING ALPR

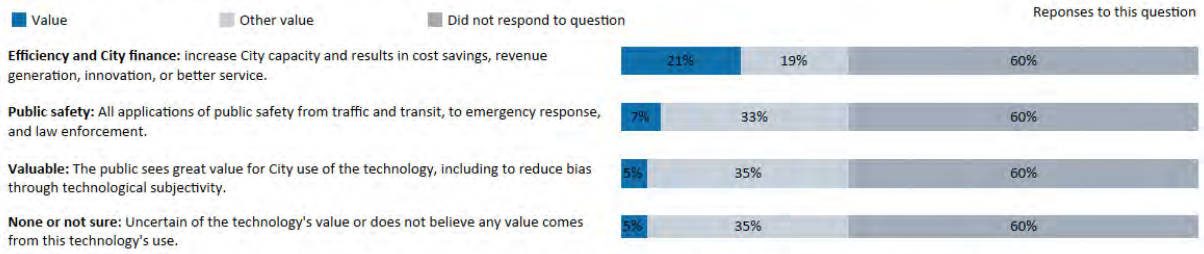


Question 2

What value do you think this technology brings to our city?

17

Reponses to this question



"The real value is in investigation/evidence of crime after a report is made."

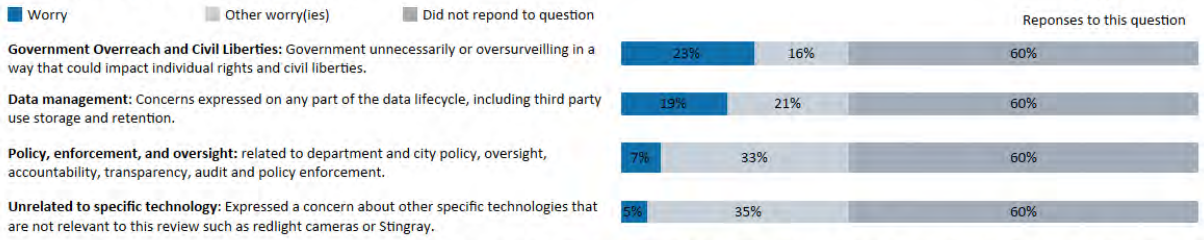
Common Themes

Question 3

What worries you about how this is used?

17

Reponses to this question



"The sheer volume of data maintained by SPD that is tracking innocent citizens, as collateral in case they maybe do something bad in the future."

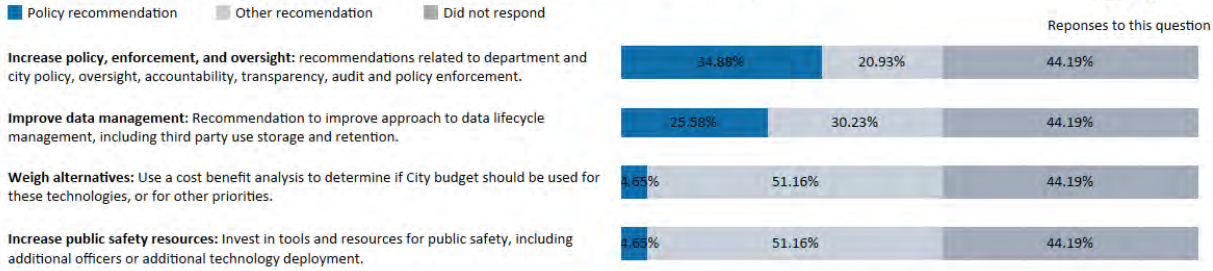
Common Themes

Question 4

What recommendations would you give policy makers at the City about this technology?

24

Reponses to this question



"Please let us know how you intend to safeguard the collection of this data so that no single person or unchecked group of people could use it for non-crime-related activities. Please let us know how you intend to dispose of this information so that it can't be hacked or accessed by folks who have goals motivated by prejudice."

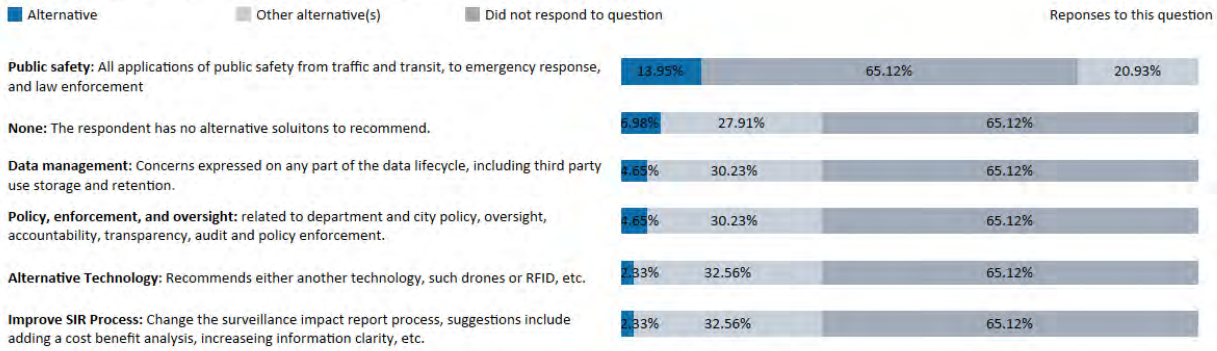
Common Themes

Question 5

Can you imagine another way to solve the problem this technology solves?

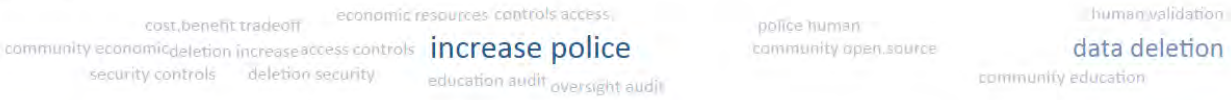
15

Reponses to this question



"Hiring more people to patrol our city."

Common Themes

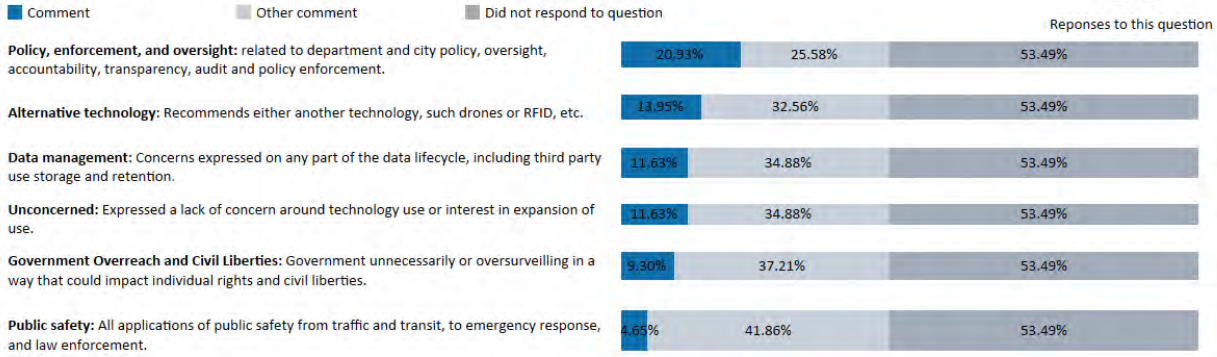


Question 6

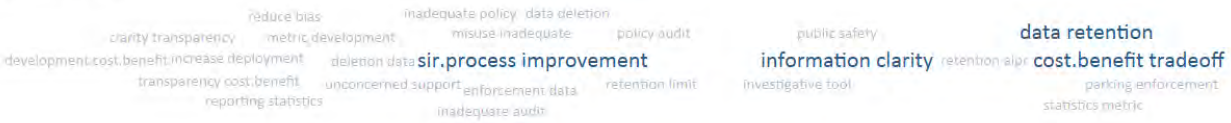
Do you have any other comments?

20

Reponses to this question



Common Themes



GENERAL SURVEILLANCE COMMENT THEMES

Many comments were submitted as part of the public comment period that were not specific to a technology, but to either the concept of surveillance in general, or to technologies which are not on the Master List.

Top themes	
public safety	Safety of the public, including first response, and in some cases traffic safety.
crime prevention	Tool or process to aid in the prevention of crime by police.
transit safety	Safety on or around public transit, roadways, or relating to traffic overall, including bicycle and pedestrian.
law enforcement	Enforce the laws, whether related to City policy, traffic law, or public safety law enforcement.
increase police	Policy recommendation or alternative solution that requires more police officers.
parking enforcement	Enforcement of laws specifically related to parking infractions.
facilitate traffic.flow	Improve the ability for cars, buses and bicycle to navigate through the City.
redlight cameras	Subject of comment was a camera technology exempt from SIR process by Ordinance and not under review.
add cameras	Desire for additional cameras, to include police, traffic, red-light or other.
investigative tool	Value or other comment of police to use technology as a tool for solving open or active crimes.
public oversight	Desire for public oversight of technology, may include voting, audits, or other transparency methods.
increase deployment	Increase the use and deployment of surveillance technology.

DEMOGRAPHICS FOR GROUP ONE COMMENTS

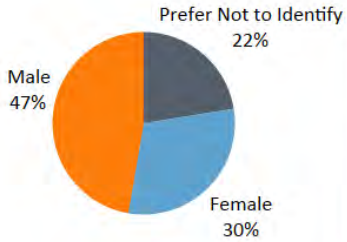
The number of reported demographics does not correspond to the number of comments received for the following reasons.

1. The demographic information includes all responses, regardless of which technology was commented on to protect the privacy of those who provided a response.
2. Some individuals offered more than one comment.
3. Some individuals did not provide any demographic information.

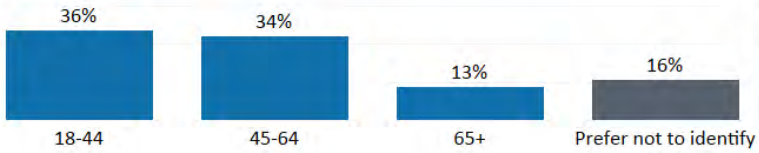
Method Submitted By

Focus Group 1	9
Focus Group 2	5
Meeting 1	15
Meeting 2	7
Meeting 3	10
Meeting 4	14
Meeting 5	5
Survey Monkey	64
Grand Total	129

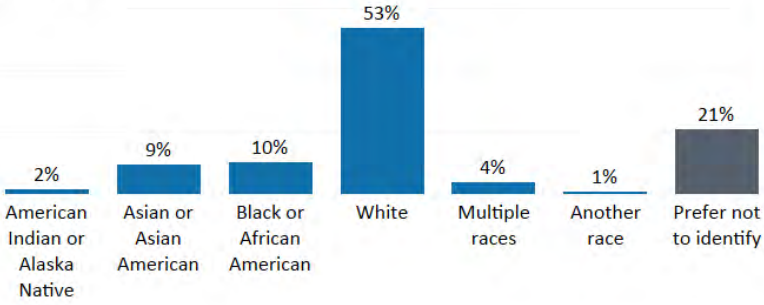
Gender



Age



Enthnicity



Neighborhoods

King County (outside Seattle)	8
Outside of King County	1
Prefer not to identify	10

APPENDIX C: PUBLIC MEETING NOTICE(S)

Notice of Public Meetings
Surveillance Technology Public Comment

This is the first round of public comment on previously acquired surveillance technologies. For more information on these technologies or Surveillance Ordinance visit **seattle.gov/privacy**.

	Meeting 1	Meeting 2	Meeting 3	Meeting 4	Meeting 5
Depts. Presenting	Police Dept.	Transportation, Fire Dept.	Police Dept.	Police Dept.	Transportation, Fire Dept.
Date & Time	October 22, 2018 5-6:30 p.m.	October 25, 2018 5-6:30 p.m.	October 29, 2018 5-6:30 p.m.	October 30, 2018 5-6:30 p.m.	November 5, 2018 4:30-5:30 p.m.
Location	**Columbia City Branch Library** 4721 Rainier Ave S, Seattle, WA 98118	**American Legion Hall: West Seattle** 3618 SW Alaska St. Seattle, WA 98126	**Bertha Knight Landes Room** 1st Floor City Hall - 600 4th Ave, Seattle, WA 98104 (5th Ave door)	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115

Technologies discussed at the meetings include:

Transportation (Meetings 2 & 5)	**Fire Dept.** (Meetings 2 & 5)	**Police Dept.** (Meetings 1, 3, & 4)
Traffic Cameras & License Plate Readers	Emergency Scene Cameras & Hazmat Cameras	Parking Enforcement Systems & Automated License Plate Readers

Here's how you can provide comments:

The open comment period for these technologies is **October 8 - November 5, 2018.** There are three ways to comment:

1. Attend the meeting. See the table above for locations and times.

2. Submit comment online at **seattle.gov/privacy.**

3. Send mail to Attn: Surveillance & Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.

Comments submitted will be included in the final Surveillance Impact Report submitted to City Council and available to the public. To comment after this period has closed, contact City Council staff at **seattle.gov/Council.**

Please note, this meeting will:

Be video recorded. **Ask for a sign-in record of attendees.** **Collect public comments.**

For meeting accommodations: Please let us know **two weeks in advance of the meeting date** if language translation, or other services are needed by emailing **Surveillance@seattle.gov.**

City of Seattle

Aviso de audiencias públicas

Comentarios del público sobre tecnologías de vigilancia

Esta es la primera ronda de audiencias públicas sobre tecnologías de vigilancia adquiridas previamente. Para obtener más información sobre estas tecnologías o sobre la Surveillance Ordinance (Ordenanza sobre Vigilancia), visite **seattle.gov/privacy**.

	Audiencia 1	Audiencia 2	Audiencia 3	Audiencia 4	Audiencia 5
Departamentos a cargo	Depto. de Policía	Depto. de Transporte y de Bomberos	Depto. de Policía	Depto. de Policía	Depto. de Transporte y de Bomberos
Fecha y hora	22 de octubre de 2018 5:00 a 6:30 p. m.	25 de octubre de 2018 5:00 a 6:30 p. m.	29 de octubre de 2018 5:00 a 6:30 p. m.	30 de octubre de 2018 5:00 a 6:30 p. m.	5 de noviembre de 2018 4:30 a 5:30 p. m.
Lugar	**Columbia City Branch Library** 4721 Rainier Ave S, Seattle, WA 98118	**American Legion Hall: West Seattle** 3618 SW Alaska St. Seattle, WA 98126	**Bertha Knight Landes Room** 1st Floor City Hall - 600 4th Ave, Seattle, WA 98104 (5th Ave door)	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115

En las audiencias se hablará de las siguientes tecnologías:

Transporte (audiencias 2 y 5)	**Depto. de Bomberos** (audiencias 2 y 5)	**Depto. de Policía** (audiencias 1, 3 y 4)
Cámaras de tránsito y lectores de placas de automóviles	Cámaras para escenas de emergencia y cámaras para Hazmat (hazardous materials, materiales peligrosos)	Sistemas de control de áreas de estacionamiento y lectores automáticos de placas de automóviles

Cómo puede enviar sus comentarios:

El período abierto para recibir comentarios sobre estas tecnologías es desde el **8 de octubre hasta el 5 de noviembre de 2018.** Existen tres formas de aportar comentarios:

1. Asista a la audiencia. Consulte la tabla anterior para conocer los horarios y los lugares.

2. Deje sus comentarios en línea en **seattle.gov/privacy**.

3. Envíe comentarios por correo postal a la siguiente dirección: Surveillance & Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.

Los comentarios enviados se incluirán en la versión final del Surveillance Impact Report (Informe del efecto de la vigilancia) que se presentará ante el Consejo de la Ciudad y estará disponible al público en general. Para aportar comentarios luego de este período, comuníquese con el personal del Consejo de la Ciudad desde la página web **seattle.gov/Council**.

Tenga en cuenta que esta audiencia tendrá las siguientes características:

Se grabará en video. **Se llevará un registro de asistencia.** **Se recolectarán comentarios del público.**

Adaptaciones para las audiencias: Si necesita servicios de traducción u otros servicios, envíenos un correo electrónico a **Surveillance@seattle.gov dos semanas antes de la audiencia.**

City of Seattle

Ogaysiiska Kulanada Dadwaynaha

Fikradaha Dadwayanaha ee ku aadan Qalabka Muraaqabaynta Casriga ah

Kani waa wareegi koowaad ee lagu aruurinaayo fikradaha dadwaynuhu kaqabaan qalabka muraaqabaynta casriga ah noociisii hore. Wixii macluumaad dheeraad ah oo kusaabsan qalabkaan ama Surveillance Ordinance (Qaabka Muraaqabaynta) booqo seattle.gov/privacy.

	Kulanka 1	Kulanka 2	Kulanka 3	Kulanka 4	Kulanka 5
Waaxaha. Soojeedinta	Waaxda Booliiska.	Gaadiidka, Waaxda Dab Damiska.	Waaxda Booliiska.	Waaxda Booliiska.	Gaadiidka, Waaxda Dab Damiska.
Tariikhda iyo waqtiga	Oktoobar 22, 2018 5-6:30 p.m.	Oktoobar 25, 2018 5-6:30 p.m.	Oktoobar 29, 2018 5-6:30 p.m.	Oktoobar 30, 2018 5-6:30 p.m.	Nofeembar 5, 2018 4:30-5:30 p.m.
Goobta	**Laanta Maktabada ee Magaalada Columbia** 4721 Rainier Ave S, Seattle, WA 98118	**American Legion Hall: West Seattle** 3618 SW Alaska St. Seattle, WA 98126	**Bertha Knight Landes Room** 1st Floor City Hall - 600 4th Ave, Seattle, WA 98104 (5th Ave door)	**Laanta Maktabada Green Lake** 7364 East Green Lake Dr. N, Seattle, WA 98115	**Laanta Maktabada Green Lake** 7364 East Green Lake Dr. N, Seattle, WA 98115

Tignoolojiyadaha looga dooday kulanada waxaa kamid ah:

Gaadiidka (kulanada 2 iyo 5)	**Waaxda Dab damiska.** (Kulanada 2 iyo 5)	**Waaxda Booliiska.** (Kulanada 1, 3, iyo 4)
Kaamirooyinka taraafikada iyo Qalabka Akhriya Aqoonsiga Shatiyada	Kaamirooyinka Dhacdooyinka Degdega ah iyo kaamiroyinka Hamzat	Nidaamyada Xakamaynta Baakinka iyo Qalabka Akhriya Aqoonsiga Shatiyada

Halkaan kabaro sida aad fikrado kudhiiban karto:

Mudada ay furantahay fikrad kadhiibashada qalabkaan casriga ah waa Oktoobar 8 - Nofeembar 5, 2018. Waxaa jira saddex qaab oo fikir lagu dhiiban karo:

1. Inaad kulanka kaqaybgasho. Fiiri shaxda kore oo ay kuqoran yihiin goobaha iyo xiliyada laqabanaayo kulanada.
2. Fikirkaaga kudir si oonleen ah seattle.gov/privacy.
3. Boosto udir: Surveillance & Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.

Fikrado kasta oo lasoo gudbiyo waxaa lagu darayaa War bixinta ugu danbaysa Surveillance Impact Report (Saamaraynta Qalabka Muraaqabada) ee loogudbiyo Dawlada hoose dadwaynuhuna ay akhri sankaraan. Si aad fikirkaaga udhiibato kadib marka mudadaan dhammaato, laxiriir Shaqaalaha Dawlada Hoose oo ciwaankoodu yahay seattle.gov/Council.

Fadlan ogsoonow, kulankaan waa:

Laduubayaa si muqaal ahaan ah. **Dalbo Diiwanka Galitaanka dadka Kaqaybgalaaya ay saxiixayaan.** **Aruuri Fikradaha Dadwaynaha.**

Wixi laxiriira adeegyada kulanada intay socdaan labixinaayo: Fadlan noosoosheeg **labo asbuuc kahor taariikhda kulanku dhacayo** haddii adeegyada turjumida luuqada, ama adeegyo kale loobaahdo adoo email noogusoo diraaya Surveillance@seattle.gov.

City of Seattle

公開會議通知
監視技術公開意見徵集會

這是第一輪會議，徵集公眾對之前取得的監控技術的建議。要獲取有關這些技術或 Surveillance Ordinance（監控條例）的更多資訊，請瀏覽 seattle.gov/privacy。

	會議 1	會議 2	會議 3	會議 4	會議 5
出席部門	警察署	交通、消防署	警察署	警察署	交通、消防署
日期及時間	2018 年 10 月 22 日 下午 5-6:30	2018 年 10 月 25 日 下午 5-6:30	2018 年 10 月 29 日 下午 5-6:30	2018 年 10 月 30 日 下午 5-6:30	2018 年 11 月 5 日 下午 4:30-5:30
地點	**Columbia City Branch Library** 4721 Rainier Ave S, Seattle, WA 98118	**American Legion Hall: West Seattle** 3618 SW Alaska St. Seattle, WA 98126	**Bertha Knight Landes Room** 1st Floor City Hall - 600 4th Ave, Seattle, WA 98104 (5th Ave door)	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115

會上討論的技術包括：

交通署（會議 2 和會議 5）	**消防署**（會議 2 和會議 5）	**警察署**（會議 1、3 和 4）
交通攝像頭和車輛牌照識別器	緊急現場攝像頭與危險品攝像頭	停車執行系統與車輛牌照自動識別器

您提交意見的方式：

針對這些技術的公眾意見徵集時間是 2018 年 10 月 8 日至 11 月 5 日。有三種方式可提交意見：

1. 出席會議。和時間見上表。
2. 透過 seattle.gov/privacy 網上提交意見。
3. 寄郵件至：Surveillance & Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124。

提交的所有意見都將收錄於最終的 Surveillance Impact Report（監控影響報告），遞交至市議會並向大眾開放。如果要在此期間結束後提交意見，請瀏覽 seattle.gov/Council，聯繫市議會的工作人員。

請注意，此會議將：

進行錄影。 **要求參會者簽到。** **收集公眾意見。**

會議輔助服務：如果需要語言翻譯或其他服務，請參照會議日期提前兩週發送電子郵件至 Surveillance@seattle.gov 告知我們。

City of Seattle

公开会议通知

监控技术公众意见征集会

这是第一轮会议，征集公众对之前取得的监控技术的意见。要获得有关这些技术或 Surveillance Ordinance（监控条例）的更多信息，请访问 seattle.gov/privacy。

	第 1 次会议	第 2 次会议	第 3 次会议	第 4 次会议	第 5 次会议
出席部门	警察局	交通、消防局	警察局	警察局	交通、消防局
日期与时间	2018 年 10 月 22 日 下午 5-6:30	2018 年 10 月 25 日 下午 5-6:30	2018 年 10 月 29 日 下午 5-6:30	2018 年 10 月 30 日 下午 5-6:30	2018 年 11 月 5 日 下午 4:30-5:30
地点	**Columbia City Branch Library** 4721 Rainier Ave S, Seattle, WA 98118	**American Legion Hall: West Seattle** 3618 SW Alaska St. Seattle, WA 98126	**Bertha Knight Landes Room** 1st Floor City Hall – 600 4th Ave, Seattle, WA 98104 (5th Ave door)	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115

会上讨论的技术包括：

交通局（第 2 和第 5 次会议）	消防局（第 2 和第 5 次会议）	警察局（第 1、3、4 次会议）
交通摄像头和车辆牌照识别器	紧急现场摄像头与危险品摄像头	停车执行系统与车辆牌照自动识别器

您提交意见的方式：

针对这些技术的公众意见征集时间是 **2018 年 10 月 8 日至 11 月 5 日。**提交意见的三种途径：

1. 出席会议。地点和时间见上表。
2. 通过网站 seattle.gov/privacy 在线提交意见。
3. 寄送邮件至：Surveillance & Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124。

提交的所有意见都将收录于最终的 Surveillance Impact Report（监控影响报告），递交至市议会并向大众开放。如果要在此期间结束后提交意见，请浏览 seattle.gov/Council，联系市议会的工作人员。

请注意，此会议将：

进行录像。 **要求参会者签到。** **收集公众意见。**

会议辅助服务：如果需要语言翻译或其他服务，请参照会议**日期提前两周**发送电子邮件至 Surveillance@seattle.gov

City of Seattle

Thông Báo Về Các Cuộc Họp Công Chúng

Ý Kiến Của Công Chúng Về Công Nghệ Giám Sát

Đây là vòng thu thập ý kiến của công chúng đầu tiên về các công nghệ giám sát đã được ứng dụng trước đây. Để có thêm thông tin về các công nghệ này hoặc Surveillance Ordinance (Sắc Lệnh Giám Sát), hãy truy cập **seattle.gov/privacy**.

	Cuộc họp 1	Cuộc họp 2	Cuộc họp 3	Cuộc họp 4	Cuộc họp 5
Các Sở Tổ Chức Cuộc Họp	Sở Cảnh Sát	Sở Giao Thông Vận Tải, Sở Cứu Hỏa	Sở Cảnh Sát	Sở Cảnh Sát	Sở Giao Thông Vận Tải, Sở Cứu Hỏa
Ngày & Giờ	Ngày 22 tháng 10 năm 2018 5 giờ - 6 giờ 30 phút chiều	Ngày 25 tháng 10 năm 2018 5 giờ - 6 giờ 30 phút chiều	Ngày 29 tháng 10 năm 2018 5 giờ - 6 giờ 30 phút chiều	Ngày 30 tháng 10 năm 2018 5 giờ - 6 giờ 30 phút chiều	Ngày 5 tháng 11 năm 2018 4 giờ 30 - 5 giờ 30 phút chiều
Địa điểm	**Columbia City Branch Library** 4721 Rainier Ave S, Seattle, WA 98118	**American Legion Hall: West Seattle** 3618 SW Alaska St. Seattle, WA 98126	**Bertha Knight Landes Room** 1st Floor City Hall - 600 4th Ave, Seattle, WA 98104 (5th Ave door)	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115

Các công nghệ được thảo luận tại các cuộc họp bao gồm:

Giao thông vận tải (Cuộc họp 2 & 5)	**Sở Cứu Hỏa** (Cuộc họp 2 & 5)	**Sở Cảnh Sát** (Cuộc họp 1, 3 & 4)
Các Máy Quay Giao Thông & Các Thiết Bị Đọc Biển Số Xe	Máy Quay Trường Hợp Khẩn Cấp & Máy Quay Hazmat	Hệ Thống Thực Thi Việc Đậu Xe & Các Thiết Bị Đọc Biển Số Xe Tự Động

Đây là cách quý vị có thể đưa ra ý kiến của mình:

Thời gian lấy ý kiến cho các công nghệ trên là **Ngày 8 tháng 10 – Ngày 5 tháng 11 năm 2018.** Có ba cách đưa ra ý kiến:

1. Tham dự cuộc họp. Xem bảng bên trên để biết thời gian và địa điểm.

2. Nộp ý kiến trực tuyến tại **seattle.gov/privacy**.

3. Gửi thư đến Attn: Surveillance & Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.

Các ý kiến được nộp sẽ được đưa vào bản Surveillance Impact Report (Báo Cáo Tác Động Giám Sát) cuối cùng nộp cho Hội Đồng Thành Phố và có sẵn dành cho công chúng. Để đưa ra ý kiến sau khi giai đoạn thu thập ý kiến đã kết thúc, hãy liên hệ với nhân viên của Hội Đồng Thành Phố tại **seattle.gov/Council**.

Vui lòng lưu ý, cuộc họp này sẽ:

Được ghi hình.

Yêu cầu lưu tên trong danh sách đăng ký tham dự.

Thu thập các ý kiến của công chúng.

Để đáp ứng các yêu cầu điều chỉnh: Vui lòng thông báo cho chúng tôi biết **hai tuần trước ngày diễn ra cuộc họp** nếu quý vị cần dịch vụ thông dịch ngôn ngữ hoặc các dịch vụ khác, bằng cách gửi email đến **Surveillance@seattle.gov**.

City of Seattle

Paunawa sa Mga Pampublikong Pagpupulong

Komento ng Publiko sa Teknolohiya sa Pagmamanman

Ito ang unang round para sa pagkomento ng publiko tungkol sa mga dating nakuhang teknolohiya sa pagmamanman. Para sa higit pang impormasyon tungkol sa mga teknolohiyang ito o sa Surveillance Ordinance (Ordinansa sa Pagmamanman), bumisita sa **seattle.gov/privacy**.

	Pagpupulong 1	Pagpupulong 2	Pagpupulong 3	Pagpupulong 4	Pagpupulong 5
Mga departamento na Naglalahad	Departamento ng Pulisya	Departamento ng Transportasyon, Bumbero	Departamento ng Pulisya	Departamento ng Pulisya	Departamento ng Transportasyon, Bumbero
Petsa at Oras	Oktubre 22, 2018 5-6:30 p.m.	Oktubre 25, 2018 5-6:30 p.m.	Oktubre 29, 2018 5-6:30 p.m.	Oktubre 30, 2018 5-6:30 p.m.	Nobyembre 5, 2018 4:30-5:30 p.m.
Lokasyon	**Columbia City Branch Library** 4721 Rainier Ave S, Seattle, WA 98118	**American Legion Hall: West Seattle** 3618 SW Alaska St. Seattle, WA 98126	**Bertha Knight Landes Room** 1st Floor City Hall - 600 4th Ave, Seattle, WA 98104 (5th Ave door)	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115

Kabilang sa mga teknolohiyang tatalakayin sa mga pagpupulong ang:

Transportasyon (Pagpupulong 2 at 5)	**Departamento ng Bumbero** (Pagpupulong 2 at 5)	**Departamento ng Pulisya** (Pagpupulong 1, 3, at 4)
Mga Camera sa Trapiko at License Plate Readers (Mga Tagabasa ng Lisensyadong Plaka)	Mga Camera sa Pinangyarihan ng Emergency at Mga Camera ng Hazmat	Mga Sistema sa Pagpapatupad ng Tamang Pagpaparada at Mga Automated License Plate Reader (Mga Awtomatikong Tagabasa ng Lisensyadong Plaka)

Narito ang mga paraan kung paano ka makapagbibigay ng mga komento:

Ang panahon ng bukas na pagkokomento para sa mga teknolohiyang ito ay mula **Oktubre 8 - Nobyembre 5, 2018.** May tatlong paraan upang makapagkomento:

1. Dumalo sa pulong. Tingnan ang talahanayan sa itaas para sa mga lokasyon at oras.
2. Magsumite ng komento online sa **seattle.gov/privacy**.
3. Magpadala ng liham sa Attn: Surveillance & Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.

Isasama ang anumang isinumiteng komento sa huling Surveillance Impact Report (Ulat sa Epekto ng Pagmamanman) na isusumite sa Konseho ng Lungsod at isasapubliko. Upang makapagbigay ng komento pagkalipas ng panahong ito, makipag-ugnayan sa mga kawani ng Konseho ng Lungsod sa **seattle.gov/Council**.

Mangyaring tandaan, ang pulong na ito ay:

Ire-record sa video.

Hihingi ng tala ng pag-sign in ng mga dadalo.

Mangongolekta ng mga komento ng publiko:

Para sa mga pangangailangan sa pagpupulong: Mangyaring ipaalam sa amin kung kailangan mo ng mga serbisyo sa pagsasalin ng wika o iba pang serbisyo **dalawang linggo bago ang petsa ng pagpupulong** sa pamamagitan ng pagpapadala ng email sa **Surveillance@seattle.gov**.

City of Seattle

공개 회의 통지
감시 기술 여론 수렴

본 회의는 과거 획득된 감시 기술에 대한 제1차 여론 수렴 회의입니다. 본 기술 또는 Surveillance Ordinance(감시 조례 관련) 자세한 정보는 **seattle.gov/privacy**를 참조해 주시기 바랍니다.

	회의1	회의2	회의3	회의4	회의5
발표 부처	경찰국	교통국, 소방국	경찰국	경찰국	교통국, 소방국
날짜 및 시간	2018년 10월 22일 5-6:30 p.m.	2018년 10월 25일 5-6:30 p.m.	2018년 10월 29일 5-6:30 p.m.	2018년 10월 30일 5-6:30 p.m.	2018년 11월 5일 4:30-5:30 p.m.
장소	**Columbia City Branch Library** 4721 Rainier Ave S, Seattle, WA 98118	**American Legion Hall: West Seattle** 3618 SW Alaska St. Seattle, WA 98126	**Bertha Knight Landes Room** 1st Floor City Hall - 600 4th Ave, Seattle, WA 98104 (5th Ave door)	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115	**Green Lake Branch Library** 7364 East Green Lake Dr. N, Seattle, WA 98115

회의에서 논의되는 기술 항목:

교통국(회의 2 & 5)	**소방국** (회의 2 & 5)	**경찰국** (회의 1, 3, & 4)
교통 카메라 및 번호판 판독기	응급 현장 카메라 및 Hazmat 카메라	주차 단속 시스템 및 자동 번호판 판독기

의견 전달 방법:

상기 기술에 대한 공개 의견 기간은 **2018년 10월 8일~11월 5일**입니다. 의견 전달 방법은 다음 세 가지입니다.

1. 회의에 참석합니다. 장소 및 시간은 상기 표를 참조해 주십시오.

2. 의견은 온라인 **seattle.gov/privacy**로 제출해 주십시오.

3. 우편 발송지: Surveillance & Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.

제출된 의견은 시의회에 전달되는 최종Surveillance Impact Report(감시 영향 보고서)에 수록되며 일반에게도 공개됩니다. 본 의견 수렴 기간 종료 후 의견을 제출하시려면, 시의회 담당 직원에게 **seattle.gov/Council**로 문의해 주시기 바랍니다.

회의 시 참고 사항은 다음과 같습니다.

비디오가 녹화됩니다. **참가 기록을 요청합니다.** **대중 의견을 수집합니다.**

회의 편의 제공: 언어 번역 또는 기타 서비스가 필요한 경우 **회의 개최일 2주 전**에 **Surveillance@seattle.gov**로 이메일을 보내 당국에 알려 주시기 바랍니다.

City of Seattle

APPENDIX D: MEETING SIGN-IN SHEET(S)

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☑ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☑ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☑ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☒ Female
☐ Central	☒ North	☐ Black or African American	☒ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☑ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☑ Northeast	☐ American Indian or Alaska Native	☑ 45-64	☐ Transgender
☐ East District	☐ Southeast	☑ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☑ Ballard	☐ Lake Union	☑ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☑ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☒ North	☐ Black or African American	☒ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☒ Female
☒ Central	☐ North	☐ Black or African American	☒ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☒ Female
☒ Central INTERNATIONAL DIST/CHINATOWN	☐ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☒ Asian	☒ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

10-22-18 - LIBRARY

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☑ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☑ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest Rainier Beach	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☒ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☒ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☒ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☒ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☑ White	☐ Under 18	☑ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☑ 45-64	☐ Transgender
☐ East District	☑ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☑ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☑ 45-64	☐ Transgender
☐ East District	☑ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☑ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☒ North	☐ Black or African American	☒ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☑ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☑ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☑ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☒ North	☐ Black or African American	☒ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☒ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☐ Central	☒ North	☒ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☒ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☒ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

QA

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☒ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☒ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☒ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☒ Female
☒ Central	☐ North	☒ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☒ Central	☐ North	☐ Black or African American	☒ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☒ Female
☐ Central	☐ North	☐ Black or African American	☒ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify outside of King Co		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☒ Female
☒ Central	☐ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☒ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☒ Female
☑ Central	☐ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☒ Asian	☒ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☐ Central	☑ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☑ Asian	☑ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☑ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☑ White	☐ Under 18	☐ Female
☑ Central	☐ North	☐ Black or African American	☑ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☑ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☒ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☒ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☑ Ballard	☐ Lake Union	☑ White	☐ Under 18	☑ Female
☐ Central	☐ North	☐ Black or African American	☑ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☒ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☒ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☐ Central	☑ North	☐ Black or African American	☐ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☑ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☑ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☑ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☑ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☑ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☑ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☐ Female
☐ Central	☑ North	☐ Black or African American	☐ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☑ Female
☑ Central	☐ North	☑ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☑ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☑ Female
☑ Central	☐ North	☑ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☑ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☒ Central	☐ North	☒ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☒ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☒ Central	☐ North	☒ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☐ Central	☐ North	☒ Black or African American	☐ 18-44	☒ Male
☒ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☒ Central	☐ North	☒ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☒ Central	☐ North	☒ Black or African American	☐ 18-44	☒ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☒ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☒ White	☐ Under 18	☒ Female
☒ Central	☐ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☒ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☑ White	☐ Under 18	☑ Female
☑ Central	☐ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☑ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☑ 18-44	☑ Male
☐ Delridge	☐ Northeast	☑ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify International District		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☑ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☑ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify CID		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☑ White	☐ Under 18	☐ Female
☐ Central	☐ North	☐ Black or African American	☐ 18-44	☑ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☒ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☒ South Seattle CID				
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☐ Female
☐ Central	☑ North	☐ Black or African American	☐ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☐ Asian	☐ 65 +	☑ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☑ Prefer not to identify	
☐ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☑ Prefer not to identify		

Neighborhood		Race/Ethnicity	Age	Gender
☐ Ballard	☐ Lake Union	☐ White	☐ Under 18	☑ Female
☐ Central	☐ North	☐ Black or African American	☑ 18-44	☐ Male
☐ Delridge	☐ Northeast	☐ American Indian or Alaska Native	☐ 45-64	☐ Transgender
☐ East District	☐ Southeast	☑ Asian	☐ 65 +	☐ Prefer not to identify
☐ Greater Duwamish	☐ Southwest	☐ Native Hawaiian or other Pacific Islander	☐ Prefer not to identify	
☑ King County (outside Seattle)		☐ Hispanic or Latino		
☐ Prefer not to identify		☐ Prefer not to identify		

APPENDIX E: ALL INDIVIDUAL COMMENTS RECEIVED

ALL COMMENTS RECEIVED ON ALPR AND PATROL

ID: 96

Submitted Through: Focus Group 2

Date: 11/20/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Safeguards / oversight & procedures are important. Otherwise good technology

---

ID: 95

Submitted Through: Focus Group 2

Date: 11/20/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

How far can citizens / private sector go before getting into private data – getting info that they shouldn't have - like using old accident data to prevent hiring.

ID: 94

Submitted Through: Focus Group 2

Date: 11/20/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Get better technology that will differentiate different state plates

---

ID: 93

Submitted Through: Focus Group 2

Date: 11/20/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Makes nervous – watching micro manipulation data used in China – reason for concern

---

ID: 92

Submitted Through: Focus Group 2

Date: 11/20/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Like it- can used in illegal activity. Easier to track down people using car for illegal activity

---

ID: 91

Submitted Through: Focus Group 2

Date: 11/20/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Remove guessing game officers have to go through – but do verify

---

ID: 90

Submitted Through: Focus Group 2

Date: 11/20/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Like being used in DV cases and in other investigations. Effective use of technology

---

ID: 89

Submitted Through: Focus Group 2

Date: 11/20/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Great – eased concern about potential abuse. Allows more efficiency in SPD

ID: 88

Submitted Through: Focus Group 2

Date: 11/20/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

In this area CFD, parking is a nightmare. Things helped when parking enforced within reason.

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 62

Submitted Through: Focus Group 1

Date: 11/8/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Police trained to work well with those who have disabilities and mental illness

---

ID: 57

Submitted Through: Focus Group 1

Date: 11/8/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Stole my plate, put a different plate on there, and replaced plate had no tabs and I had to pay for that.

ID: 55

Submitted Through: Focus Group 1

Date: 11/8/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Lots of information being collected and stored

What value do you think this technology brings to our city?

Getting your stolen car back

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

two systems synced together by numan beings could result in error

---

ID: 54

Submitted Through: Focus Group 1

Date: 11/8/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Not yet

What value do you think this technology brings to our city?

maybe save money

What worries you about how this is used?

none

What recommendations would you give policy makers at the City about this technology?

back up always with human oversight

Can you imagine another way to solve the problem this technology solves?

no

Do you have any other comments?

ID: 1

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

No

What value do you think this technology brings to our city?

Force multiplier for police

What worries you about how this is used?

Immigration enforcement

What recommendations would you give policy makers at the City about this technology?

add fixed LPR as well

Can you imagine another way to solve the problem this technology solves?

no

Do you have any other comments?

Keep up the great work and keep innovating

ID: 2

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

People may be misidentified in the case of a stolen vehicle

What value do you think this technology brings to our city?

What worries you about how this is used?

There may be potential for use in non-criminal investigations

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

An incident number should be required to pull ALPR data, not just a generic "reason"

ID: 6

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Scalability--this isn't a really scalable technology.

What value do you think this technology brings to our city?

ALPR brings order the city.

What worries you about how this is used?

The system may make mistakes

What recommendations would you give policy makers at the City about this technology?

Find a way to do auto-checking to reduce the need to call the system for verification

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Step forward to avoid profiling

ID: 8

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

The real value is in investigation/evidence of crime after a report is made.

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Deploy ALPR on a macro level - use the technology beyond just vehicles.

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Deploy static ALPR cameras throughout the city.

ID: 9

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Risk of misuse; potential access by Feds or others

What value do you think this technology brings to our city?

Important value to having technology to pull up information quickly and accurately in order to take timely action.

What worries you about how this is used?

Criminalizing people more, and has a greater impact getting people at work

What recommendations would you give policy makers at the City about this technology?

Make the data storage, process, testing and auditing process for these technologies more transparent.

Can you imagine another way to solve the problem this technology solves?

RFID tags on licenses or other non-photo method that accomplished the same thing

Do you have any other comments?

ID: 10

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Recording where people are as they go about daily life

What value do you think this technology brings to our city?

Increases effeciency.

What worries you about how this is used?

Doesn't account for situational or economic circumstance

What recommendations would you give policy makers at the City about this technology?

Clarify and ensure the technology is well-tested to prevent potential hacks.

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 11

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Privacy concerns in general.

What value do you think this technology brings to our city?

What worries you about how this is used?

More occurances and informaiton - more interaction could lead to more mistakes

What recommendations would you give policy makers at the City about this technology?

Provide a clear policy the data can't be used by police at home

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 12

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Potential expansion of ALPR use

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Provide clear policy for when data is exposed publicly (PDR) to ensure safety, 3rd party (plateholder) notified

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 13

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Where data is being stored. Is the data encrypted?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

release information on real results from the technology

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 14

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Control/use of the information in the audit

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 15

Submitted Through: Meeting 1

Date: 10/22/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Data protection in general, but also from public disclosure. For example, it becomes a safety issue if looking for someone, some vehicle

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 36

Submitted Through: Meeting 3

Date: 10/29/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

The Racial Equity Toolkit is not used in technology or policy around ALPR use

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

We need effective, rigorous, random, in-depth auditing process

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Doubtful that in 10 years of use, no inappropriate use has been noted by SPD staff. That says to me the audit process is ineffective

---

ID: 35

Submitted Through: Meeting 3

Date: 10/29/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

This technology could be sued for organized stalking activity

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 34

Submitted Through: Meeting 3

Date: 10/29/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

I am concerned about the misuse of data for purposes other than law enforcement or investigative purposes.

What value do you think this technology brings to our city?

What worries you about how this is used?

Misuse of time, energy, technology

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 33

Submitted Through: Meeting 3

Date: 10/29/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

I am concerned that surveillance is occuring in itself is concerning

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 32

Submitted Through: Meeting 3

Date: 10/29/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Concerned about collection and storage of information about or on innocent people or those not involved in criminality

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

In Parking enforcement autovu data is deleted in a day. PiPs is retained for 90 days

---

ID: 31

Submitted Through: Meeting 3

Date: 10/29/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

All techologies make errors. When ALPR and/or officer make a mistake on parking enforcement with a misread of a license plate and giev a ticket to a car legally parked using "pay by phone" app, how is this validated. How appealed if the wrong plate is recorded?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 30

Submitted Through: Meeting 3

Date: 10/29/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

yes

What value do you think this technology brings to our city?

Not much value unless it is directed to a specific vehicle involved in a crime, or, looking for a lost child or elderly person

What worries you about how this is used?

Just as with Det-Boxes and Stingray machines; law enforcement can absorb citizens cell phone information that are not criminals. Targeted individuals are stalked with these machines, and law enforcement is not made to divulge who are targeted by these machines

What recommendations would you give policy makers at the City about this technology?

Even though "Mary" the police represented insists that the police must demonstrate a "hit" when they find a suspects vehicle; what would prevent police from trolling any one's license plates thus absorbing private info?

Can you imagine another way to solve the problem this technology solves?

More oversight institutions apart from police departments - to check surveillance by SPD

Do you have any other comments?

ID: 29

Submitted Through: Meeting 3

Date: 10/29/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Police need to keep statistics on value and if this program and others work to help. Keep in mind privacy of public vs. criminals data storage etc.

ID: 50

Submitted Through: Meeting 4

Date: 10/30/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

More informed policy around data protection policy that involves policy makers and electeds and public

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 49

Submitted Through: Meeting 4

Date: 10/30/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Retention: delete "no match" records right away. State req. should reduece retention time

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 48

Submitted Through: Meeting 4

Date: 10/30/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Get act together to respond to PDR requests. Heavy metrics and transparency of them around usages and unintended applications

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 46

Submitted Through: Meeting 4

Date: 10/30/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Auditing transparency - use of algorithms is concern. Particularly around privacy, security, accuracy, and bias

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Data + Research transparency. Notify community if other uses contemplated as well as research being conducted

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 45

Submitted Through: Meeting 4

Date: 10/30/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Data retention and security - worried about misuse

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Ensure there is no mission creep. Other data captured and used for some other task

Can you imagine another way to solve the problem this technology solves?

Could community do this - open source? Crowd source??

Do you have any other comments?

Initial application benaign watch for expansion, transparency around data

---

ID: 44

Submitted Through: Meeting 4

Date: 10/30/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Concerns around data retention

What value do you think this technology brings to our city?

Faster return of vehicles even if higher cost

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Serious consequences for misuse of data or system

Can you imagine another way to solve the problem this technology solves?

Has efficacy but it's a powerful tool - choose between/tradeoffs between crime solving and civil liberties

Do you have any other comments?

Unintended consequences - being aware of cross referencing data

---

ID: 43

Submitted Through: Meeting 4

Date: 10/30/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Potential for misuse by govt employees to embarrassment of citizens

What value do you think this technology brings to our city?

Relieve officers of tedium of looking for stolen vehicles. Form of performing public service more efficiently

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Human beings needs to operate equipment and doing work

Can you imagine another way to solve the problem this technology solves?

Car GPS could be used instead of ALPR

Do you have any other comments?

Retention - used for what intended - not used beyond scope

ID: 42

Submitted Through: Meeting 4

Date: 10/30/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Are their safeguards in place for vulnerable populations when political climate changes. Trading privacy for security

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Quantify cost/benefits of ALPR. for example recovery time and recovery rate for stolen cars; a before and after comparison.

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 41

Submitted Through: Meeting 4

Date: 10/30/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Disparate impacts on communities of color that lose more privacy

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Delete immediately if no match to stolen vehicle list.

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 40

Submitted Through: Meeting 4

Date: 10/30/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

If records are kept longer than when fine is paid

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Do a better storytelling of benefits

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 39

Submitted Through: Meeting 4

Date: 10/30/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

If records are used to embarrass citizens

What value do you think this technology brings to our city?

Relieve patrol officers of the tedium of readig so many plates in seatch of a stolen vehicle. Their quest, after all, is a public service.

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Cost analysis before and after the technology - time and cost of recovery or solving crimes

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 10335611372

Submitted Through: Survey Monkey

Date: 11/8/2018 9:42:58 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Yes, I have extreme concerns about how ALPR is used in public places, particularly about how it is used by police. More so about how it is used by police who have a history of human rights violations so egregious that the U.S. government stepped in to force them to tone down those violations. And even more so about the potential use of it in coming years, as scope creeps and as the cost of deployment drops at the rate of advancement of computer technology.

What value do you think this technology brings to our city?

ALPR is valuable to police officers who wish to identify and catalog the whereabouts of everyone in view but 1) are unable to recognize those people by sight and make record of such due to limitations of human ability, and 2) are unable to stop and identify those those people due to constitutional protection against such unwarranted action. ALPR gives police superhuman abilities and a route around people's constitutional protection. Direct benefits to the public of police use of APLR include moderately improved efficiency of enforcement of on-street parking regulations and occasional discovery of stolen vehicles, suspects, fugitives, and missing persons, who would not otherwise have been recognized. Police can and do load ALPR devices with a list of vehicles of interest to them, of interest to partner agencies, or of interest to anyone who can put that license plate number on a watch list. This is likely used to alert patrol officers to stolen vehicles and to vehicles owned by suspects, fugitives, and missing persons. With a few mouse clicks, the same ALPR system could be used to instantly give patrol officers a heads-up about any vehicles in sight that are registered to people known to attack police, to people with any criminal record, to registered gun owners or holders of concealed weapons permits, to immigrants, or to any undesirable. ALPR allows patrol officers to pick people out of a crowd like never before. If enabling police to automatically observe and make record of the whereabouts of many thousands of people who are not suspected of any wrongdoing just in case it is useful against those people someday is a goal, then ALPR is invaluable in accomplishing it. Prior to their use of ALPR, SPD were completely unable to catalog the whereabouts of our vehicles, and thus of us, on the scale at which they do so now because of ALPR. ALPR also gives police a time machine of sorts; the ability to go back in time and find out where someone's vehicle has been and when it was there--not simply where and when a police officer remembered seeing that vehicle, as has always been the case, but every time and place that person's vehicle crossed paths with part of the police department's roving network of public surveillance devices. Later, a detective, an abusive spouse, or a hacker from across the globe can query the ALPR database to find out where someone's vehicle has been spotted, or where the vehicles of anyone in a group of any size has been spotted. This trove of personal data is available with just a few mouse clicks and a password guessed or read off a sticky pad--or a Public Records Act request, made through formal routes or quiet side-channels.

What worries you about how this is used?

I am very worried about devices in squad cars and elsewhere using ALPR to identify the likely-driver of every vehicle in view of those ALPR devices, then not only alerting someone who can take action if a vehicle for which police are currently searching is caught in the dragnet, but also making a record of the times and locations that vehicles *for which police have no reason to suspect related wrongdoing* were spotted by the device. SPD's own statistics indicate that somewhere in the area of 99.99% to 99.999% of the locational data they collect about us using ALPR corresponds to people of whom the device operator had no suspicion of wrongdoing. Police use ALPR a tiny portion of the time to alert a patrol officer that a vehicle of interest is in sight, but mostly to amass a database of the whereabouts of presumed-innocent people just in case that information will be useful against any of those people in the future. Instead of ignoring vehicles whose owners are *not* on a watch list, police, via ALPR, automatically identify and make record of when and where those vehicles were encountered. ALPR enables an officer to perform this dragnet search--performing a minimal investigation of every vehicle in view, probable cause or not--and to catalog in a central repository the whereabouts of vehicles owned by innocent people, all at superhman speed. It allows police to recognize and track us in ways undreamed of when we were first required to prominently display identifying numbers on our vehicles, ostensibly to prove that our vehicles are licensed for use on public roads. The long-term possibilities of our acceptance now of this public surveillance, particularly with ALPR policies and regulations crafted based on surveillance advocates' claims about how they currently use it, not on how we have analyzed that they actually use it, and not on how they are completely capable of using it today or tomorrow, secretly, in compliance with or in violation of any verbal assurances or written policies, are frightening.

What recommendations would you give policy makers at the City about this technology?

Please consider that this entire surveillance review process has been driven by pro-surveillance advocates and that nobody in the process assumed the role of privacy advocate. Nobody presented the pro-privacy side in opposition to advocates of public surveillance. Please consider that public input was driven by SPD presentations carefully crafted to highlight ALPR's more acceptable uses, to downplay less desirable uses, and to completely ignore its dangerous side-effects. Please consider that it is now trivial for computer systems to link a vehicle license plate to its owner, that the driver of a given non-commercial vehicle is very likely to be its registered owner, and thus that automated lookup of vehicle registration via license plate is, in essence, automated identification of nearly everyone who comes into view of an ALPR device. As these technology advances, it will be increasingly feasible to install such devices in more police cars, to provide them as software add-ons to dashboard camera and body camera systems, to mount them road-side or on overpasses, and to build them into traffic cameras, traffic signals, and "smart cities" street lights. ALPR devices, if used at all by our police, should be used sparingly for targeted searches, not as a no-holds-barred fishing expedition. If used, they should compare a plate number against a watch list, then take action if the plate is on the list, or ignore it and move on if not. Administration of ALPR watch lists should be very tightly constrained, with full audit trails, and when an investigation of someone concludes and he or she is removed from the list, he or she should be notified of the prior watch-listing. Enforcement of parking regulations should not serve as an excuse for general public surveillance--records of plate scans made to recognize over-time parking should under no circumstances be stored longer than they are useful for recognition of over-time parking. In crafting related policies and regulations, please focus not on how ALPR is likely used now, by people with the best of intentions, using a couple dozen ALPR devices, but how it could be used later, by people with very troubling intentions, using hundreds or thousands of devices--on every police car, in every body camera, at every entrance to "congestion zones," or on every traffic signal pole. Please do not settle for personal assurances from current SPD staff as protection against feature creep, but craft legislation prohibiting any but acceptable use. Even if we are to accept the dragnet searches--the requirement that we display machine-readable identification tags when traveling on public streets and that police will use those tags to identify each of us and look us up in order to identify the suspects and fugitives blending in among us--we should take extreme caution to prevent the use of data about innocent bystanders collected incidental to searches for those suspects and fugitives. Please consider the implications of a system that allows inexpensive devices to identify nearly everyone on the street. This is a dragnet search, akin to forcing everyone who walks on a public street to wear machine-readable identity tags, then using machines to identify everyone. That, in itself, is troubling. But for police to go beyond simply A) doing a "Papers, please!" style check of everyone they encounter so that they can find criminal suspects and other persons of interest, to B) also recording the times and locations that everyone *not* currently of interest was seen, is dangerous to our freedom. The results of automated license plate reads that do not indicate the need for further investigation (i.e., reads of plates that are not on any watch list) should not be stored--not for months, weeks, days, or hours. This is information about people that ALPR operators do not suspect of wrongdoing. Digital information has a way of living forever, even after we think we have purged the only copy of it. SPD have a history of fouling up digital storage--just a few years ago, they lost many thousands of digital in-car video recordings. People share passwords and write them on sticky-pads because they trust their colleagues. Default passwords sometimes go unchanged. Federal agencies and foreign hackers have a history of tapping into digital information that the most qualified of engineers believed to be secure. NSA have a stated goal of storing every bit of information about the public to which they can gain access. Commercial service providers have a history of failing to secure personal information they hold--even health care and financial credit information is regularly compromised. If Google cannot keep communications between their data centers secure, SPD surely cannot keep communications between their various ALPR readers, storage, and review systems secure. Please consider what uses of ALPR are

acceptable or inevitable, and regulate use tightly to allow such and nothing more. Please consider potential loopholes in said regulations. Please consider the potential actions of SPD staff who are assigned to co-locate with outside agencies. Please consider the department's ability to contract with service providers who will perform ALPR searches for them. Please imagine a day in the not-distant future, when shortly after you walk out your door or drive out of your garage, our government is recording where you go and with whom you likely associate, just in case it's useful against you someday. Please think about the roundup and internment of Japanese-Americans not too many years ago. Please think about ICE's immigrant round-ups today. Please think about the Muslim ban. Please think of the unaccountable blacklisting performed by DHS. Please think about Donald J. Trump and his DOJ appointees. If our police collect it, they will come.

Can you imagine another way to solve the problem this technology solves?

If the problem that automated license plate readers solve is defined as "read this license plate," then yes, I can imagine another way: Someone can read the plate. If the problem that ALPR solves is defined as "recognize vehicles that have been parked longer than allowed on a public street," then yes, I can imagine another way: Flashing indicators on parking meters, overdue stickers on windows, and chalk on a stick, as have been used effectively for decades. If, however, the problem is, "In a fraction of a second, read every license plate in view, query vehicle registration records to identify everyone driving the vehicles behind those plates, then enter into a database the time and precise location that each person was located and make it available for future use, then no, I can imagine nothing other than ALPR to solve the problem. ALPR is invaluable in accelerating us toward dystopia.

Do you have any other comments?

Police cataloging the historical locations of presumed-innocent people is completely inappropriate. Our police claim enthusiastically that they use these devices to catch murderers and rapists. This is likely true. Similarly, police almost certainly could catch more criminals if they were allowed to go door-to-door and search our homes without warrants. But, as with door-to-door searches of innocent people's homes, the risk of trolling our public streets to record the locations of innocent people outweighs the potential benefit. The ends do not justify the means. Criminals sometimes walking free is part of the cost of living in a free society. In the United States, unless we are suspected of wrongdoing, we are not required to identify ourselves to agents of our government proactively or even upon request. Vehicle license plates and registration records have become part of a system that facilitates the identification of people without our consent or even our knowledge. Until recently, risks associated with this "Papers, please!" loophole were limited by the ability of humans to read a plate, optionally query a database, and make a record of the time and location that the plate was read. Technological advancements including the automated reading of license plates, fast and wireless computer networking, and effectively limitless storage capacity have eliminated that natural limitation, increasing the stakes dramatically. To the degree that a license plate is linked to a specific person or set of persons, ALPR allows police to automatically and nearly-instantaneously identify everyone in view and maintain a near-flawless record of when and where those people were seen. Where we go and with whom we associate is personal information, and it is completely inappropriate for police to use the excuse that one every ten thousand vehicles they encounter contains a person of interest in order to capture and retain information about the whereabouts of the other 9,999 vehicles. When I show my face or drive my car in public while going about my personal business, this is not justification for our government to catalog my whereabouts in case it is useful against me someday. I accept that police department staff may observe, notice, and even take note of having seen me, but I should not have to subject myself to observance and recognition via a roving network of automated surveillance devices. When I cross paths with a police department vehicle, whether I am driving safely and lawfully down the street or parking at my home, a grocery store, women's health clinic, place of worship, or political

demonstration, I should not have to consider that a record has automatically been made of when and where we crossed paths. Our vehicles bear license plates to indicate that they are licensed for use on public roads, not to serve like a bar codes on our foreheads.

ID: 10333761515

Submitted Through: Survey Monkey

Date: 11/7/2018 5:47:53 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

1) Storing location/movement details of innocent citizens for the sole purpose of potentially using it against them in the future. If they have committed no crime (and aren't being investigated for such), then their whereabouts should not be tracked. 2) No technical controls in place requiring that usage of the system matches policy (that ALPR data is only used for "...active investigations, Scofflaw enforcement, and parking enforcement". 3) No protection from person A getting ALPR data for person B's vehicle (aka tracking person B's whereabouts) via public record request (whether that be used by angry neighbors, stalking of domestic violence survivors, employers stalking employees, canvassing for potential home invasion, etc).

What value do you think this technology brings to our city?

What worries you about how this is used?

1) The sheer volume of data maintained by SPD that is tracking innocent citizens, as collateral in case they maybe do something bad in the future. People who aren't being investigated or convicted of a crime should not be tracked by police. This negatively impacts the freedom to assemble. 2) Lack of protection against abuse of the data (especially by stalkers/abusers).

What recommendations would you give policy makers at the City about this technology?

1) ALPR data (not involved with an active investigation, Scofflaw, or parking enforcement) should not be retained for 90 days - instead at most 48 hours (or less). 90 days is too long to maintain tracking data of innocent people. 2) Only the vehicle's registered owner should be able to request ALPR data about it. (This is still imperfect regarding some domestic abuse situations, but I acknowledge the need for the public to be able to request and review their own records.) 3) Additional deployment of more ALPR cameras by SPD Patrol, should require another round of public engagement *before* deployment occurs.

Can you imagine another way to solve the problem this technology solves?

1) Significantly shorter data retention or 2) Manually running plates.

Do you have any other comments?

While I appreciate the time extension that was given for public comments, I do feel like the overall public review period was too short and the community meetings should be more spaced out to give people with competing schedules a chance to block off time so they can attend in person.

ID: 10328286779

Submitted Through: Survey Monkey

Date: 11/5/2018 9:24:45 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Yes, the ALPR technology is clearly mass/ bulk surveillance. ALPR tracks innocent Seattle citizens going about their daily activities.

What value do you think this technology brings to our city?

Little. According to Mary Perry, SPD Director of Transparency & Privacy, 2.4 million license plates were taken in 9 months with as little as 124 hits, an effectiveness ratio of less than 0.005%

What worries you about how this is used?

Location privacy is eroded thru warrantless search, there appears to be little oversight and little accountability.

What recommendations would you give policy makers at the City about this technology?

It should be abandoned.

Can you imagine another way to solve the problem this technology solves?

That is not the job of the public, to decide how the police do their job. The public has the expectation that their rights are protected.

Do you have any other comments?

During the public comment period, the police did everything they could to obscure the true nature of the technology's impact on society.

ID: 10328249243

Submitted Through: Survey Monkey

Date: 11/5/2018 8:45:32 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

Although the main justification for ALPR presented by the SPD is to find stolen cars, verbal reports from police officers indicate that most cars are found by running plates without the help of ALPR. Given that the intended benefit of this systems is not met, the side effect of constant city-wide surveillance seems unjustifiable.

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 10322852282

Submitted Through: Survey Monkey

Date: 11/2/2018 2:44:46 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Any type of a license plate reader is just asking to put into a database. We the people, do not want this.

What value do you think this technology brings to our city?

None, knowing the times of traffic means nothing. It doesn't change the fact that there IS traffic. We all have smart phones and know how long our commute will be roughly.

What worries you about how this is used?

Privacy.

What recommendations would you give policy makers at the City about this technology?

Just dont.

Can you imagine another way to solve the problem this technology solves?

Knowing the travel times isn't a problem, cause automatic plate readers doesn't STOP traffic.

Do you have any other comments?

ID: 10313731660

Submitted Through: Survey Monkey

Date: 10/30/2018 10:17:08 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

I've already submitted comments once, and attended a meeting on 29 Oct. After the meeting, I have even more concerns. Here's the write-up of concerns that I posted to my blog, which I submit here for inclusion. My first concern is that nowhere in the program description was there any description of their threat models. I asked SPD's Director of Transparency and Privacy what threat modeling had been done with respect to the ALPR technology and programs, and she did not think any had been done. If an organization hasn't modeled their threats, we have no idea if we're protecting against the right things if we're protecting anything at all. And given the tenor of the meeting, I suspect SPD isn't protecting against anything at all. The department is focused about 99.8% on the benefits it gives them in chasing down crimes, particularly stolen cars. Here's where me not being a security professional is apparent. I do not know how to do any formal threat modeling. But I tried too look at various categories of possibly malevolent actors and review the program description for ways it might be misused. Some of these came from other people at the meeting. SPD's use of the system for its intended purposes This is where the program is used by SPD for finding cars or investigating crimes but through bad policy the system infringes on the liberty of the people. In this category of concern, I asked the SPD representatives if the agency had used a racial equity toolkit (RET) to analyze the impact of the program on marginalized communities in Seattle. They had not yet. Looking at the process outlined in the description, most of the RET is completed after public feedback. Some of the first portions that they have indicated are affected are obviously wrong. For instance, to the question â€œWhich of the following inclusion criteria apply to this technology?â€ they left unchecked the following: The technology disparately impacts disadvantaged groups. There is a high likelihood that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service. The technology raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice. To the first unchecked item, SPD simply doesn't know because they haven't studied the information. And they later state â€œAn additional potential civil liberties concern is that the SPD would over-surveil vulnerable or historically targeted communities, deploying ALPR to diverse neighborhoods more often than to other areas of the City.â€ Additionally, we give heightened protection to political speech. But deploying ALPR cars around protests, rallies, and other such â€œfree speech activitiesâ€ SPD has the possibility of criminal pretexts being used as fishing expeditions against opponents. SPD would have 90 days to fish through location data. These are just a couple of possibilities that I can think of off the top of

my head. The technology obviously has reasonable concerns about impacts to freedom of speech. Out of policy use by SPD officers This is where SPD officers use the system for purposes outside what is allowed. Officers are required to undergo training and of course they are all sworn and background checked. The program administrator is supposed to approve all searches of stored read data, and the system automatically logs the officer, the terms searched for, the case number and the purpose for which the search is conducted. The SPD Inspector General (theoretically independent of SPD) can audit the system for misuse, as can the program administrator. When I asked SPD command staff how many instances of misuse of the system had been found during the 10 years the program has been in use, they answered â€œnone to our knowledgeâ€. It is unlikely in the extreme that not one officer has ever misused the system. Possibilities include officers tracking vehicles of girlfriends or rivals, locals that they want to keep tabs on, take bribes or favors to feed read hits to outside people, or simply get fed up with onerous requirements for logging and do things like re-use case numbers. An audit system that has uncovered no instances of misuse is either not recording the right information or is not being conducted thoroughly. Out of policy use by other agencies Agencies such as King County, the Washington State Patrol, the FBI or Immigration and Customs Enforcement (ICE) do not have direct access to the system. However, they may submit requests for information to SPD which send them responsive data. Such requests and responses are memorialized, but it's unclear how and whether that is part of the same audit trail. Additionally, SPD did not articulate how they vet such requests, particularly with respect to Seattle's policy of non-cooperation on immigration enforcement. ICE may be making direct requests for ALPR read data with nominally within policy reasons (e.g., for customs investigations) that are really for deportation reasons. Or they may be routing such requests through other agencies. Or there may be no issue at all. We have no way of knowing. This concern was brought to my attention by another attendee at the meeting. Misuse of the data by the public According to SPD, ALPR read data is subject to public records requests. There is nothing to stop me from submitting a request every 90 days for a CD of all ALPR read data, circumventing any protection we have by SPD erasing the data they hold after 90 days. While there may be restrictions on the legal use of such data, once it leaves SPD hands, we've lost effective control of it. Misuse of the data by the vendor According to the staff present, no security review of the software has ever been performed to make sure the software does what it's supposed to do by the vendor, Neology. The software is closed source as well. Are there backdoors for support? Are there security vulnerabilities that allow exfiltration of the data? Misuse of the data by IT The City of Seattle consolidated almost all IT within a central department. The technical staff are not sworn officers, though they are background checked. According to staff present, as well as some hints in the program description, ALPR read data is stored in a SQL system. Which suggests to me that the data is both unencrypted and can be reviewed outside of the audit system that is used by SPD personnel. Most of my privacy concerns could be mitigated by a policy of discarding all read data when it does not match a hit list and/or much stronger audit processes. That would not eliminate all concerns however. Additionally, I have some other concerns that I am giving a lower priority and not including here because this is already long and some of them verge on movie-plot threat type of issues.

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 10300692351

Submitted Through: Survey Monkey

Date: 10/24/2018 9:31:33 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

I am very concerned about how many people have access to this technology and their degree of impartiality, as well as where and how long this data will be stored. There seem to be far too many ways in which this data can be used-- even hacked-- outside of SPD intentions and outside of privacy laws.

What value do you think this technology brings to our city?

None, until the potential for privacy violations and discriminatory-even "hate"-purposes can be completely eliminated.

What worries you about how this is used?

I worry that innocent people will be targeted merely for their daily practices or appearance. I worry that a person with access to this data won't have the same "everybody is absolutely necessary to our society" beliefs that I have, within the written law

What recommendations would you give policy makers at the City about this technology?

Please let us know how you intend to safeguard the collection of this data so that no single person or unchecked group of people could use it for non-crime-related activities. Please let us know how you intend to dispose of this information so that it can't be hacked or accessed by folks who have goals motivated by prejudice.

Can you imagine another way to solve the problem this technology solves?

Provide more social, economic, and therapeutic means so that communities can come together and solve problems, heal divides, and support each other, so that crime is lessened. It works in other countries.

Do you have any other comments?

Thank you for listening.

ID: 10300624502

Submitted Through: Survey Monkey

Date: 10/24/2018 9:07:27 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

1) Concerned that the information obtained is used for purposes other than what is intended for and 2) That it adversely effects certain residents of Seattle more than others.

What value do you think this technology brings to our city?

Not sure. Maybe saves the city money.

What worries you about how this is used?

That the information gathered will be used for purposes other than its original purpose and that it will be seen as irrefutable in litigation settings because it uses AI

What recommendations would you give policy makers at the City about this technology?

Use it in a very limited way; have it always be reviewed by human beings; report back whom it is affecting adversely.

Can you imagine another way to solve the problem this technology solves?

Have more education in the community addressing the problem and then police officers gathering data to see how behaviors are changing.

Do you have any other comments?

ID: 10297128415

Submitted Through: Survey Monkey

Date: 10/23/2018 3:18:18 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Why are you not using more technology to fight crime?

What value do you think this technology brings to our city?

Spend less money on people doing what machines can do.

What worries you about how this is used?

Cost of storing records.

What recommendations would you give policy makers at the City about this technology?

Use more technology like this to save taxpayer money

Can you imagine another way to solve the problem this technology solves?

Hiring more people to patrol our city.

Do you have any other comments?

I'm tired of hearing that we don't use technology to run a technology city.

ID: 10296535556

Submitted Through: Survey Monkey

Date: 10/22/2018 6:49:12 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Yes

What value do you think this technology brings to our city?

Zero.

What worries you about how this is used?

1. There is no verification that Neology does not store or transmit ALPR data outside of SPD. The programs are proprietary and the program description does not indicate that outside experts have examined the source code to verify that Neology does not retain the data. 2. The software and hardware are closed source and no outside experts have verified that either are secure against hackers. 3. The data is described to be on a "secure server". Nothing in the program description details how the server is technologically secured. 4. Nothing in the program description details who authorizes people to view ALPR data. So far as I can tell from the description, once someone has completed the ACCESS training, they may self-select when and under what circumstances they will use it. Nothing indicates that supervisor permission is needed. Nothing appears to stop an officer from deciding to track a relative's vehicle, for instance. They are not supposed to, but the policy just says "don't". 5. The program description describes that the Neology software sets the 90 day limit and also that City IT

deletes the data after 90 days in a SQL back end. These are not consistent. 6. Nothing in the program description details how the data is secured in the SQL backend against exfiltration. 7. Nothing in the program description details how ALPR data is secured in transmission between patrol cars and the "secure server". 8. ALPR data is retained for 90 days according to the policy. For the purposes described in the program description, there is no need to retain ALPR data at all; once a license plate is determined not to match, the data should be discarded. 9. The only measures described for deleting improperly retained data is that it is against policy. Nothing describes how that policy is enforced. 10. The Seattle PD OIG can audit the system, but nothing in the policy describes scheduled or random audits. 11. Nothing in the program description describes how the in vehicle computers are secured against malware. The existence of a USB port and a vehicle left unattended for 30 seconds is enough for someone to insert malware into the system. 12. Individuals can contest erroneous information about them collected by the system, but the policy as described is that much of the information that could be used to challenge erroneous information is discarded after 90 days. For instance, data on the license plates read before and after a reading that triggers the hotlist is not retained after 90 days. 13. Section 7.3 says that there is only a privacy risk if the public requests ALPR data and if they know which license plates belong to which people. Owners and users of vehicles can be relatively easily inferred from location data alone. Even stripping out license plate numbers leaves a privacy risk. Knowing that a car has been parked outside two particular places is a privacy risk (e.g., recorded outside both a residential home and a strip club). 14. Nothing in the document describes the redaction policy for ALPR data when it is subject to PRA requests. 15. Nothing in the document describes the threat models Seattle PD has for considering the security of ALPR data. 16. The duties and procedures of the ALPR administrator are barely described. They have control of the system but the program document only describes what they *can* do, not what policy mandates that they do. 17. This surveillance technology has apparently been in use for some time. Nothing in the document describes past audits, past problems, past discipline related to misuse of the technology, etc. Nothing in the document describes when the technology was adopted or how its use and governance has changed because of issues with the system. These are all necessary.

What recommendations would you give policy makers at the City about this technology?

This system needs to be scrapped.

Can you imagine another way to solve the problem this technology solves?

There's no need for any of this to be automated. We got along just fine without it up until now.

Do you have any other comments?

Seattle PD has been not-so-curiously silent that these meetings are taking place or that they are considering adopting these technologies. Nothing on the twitter feed. Nothing on SPD blotter. It wasn't on the main SPD page last week. SDOT had to put it on their twitter, the day of the first meeting and only a few hours beforehand. Someone had to be following the city's Techtalk blog to see this earlier.

ID: 10296502069

Submitted Through: Survey Monkey

Date: 10/22/2018 6:25:56 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Yes

What value do you think this technology brings to our city?

Zero.

What worries you about how this is used?

1. There is no verification that Neology does not store or transmit ALPR data outside of SPD. The programs are proprietary and the program description does not indicate that outside experts have examined the source code to verify that Neology does not retain the data. 2. The software and hardware are closed source and no outside experts have verified that either are secure against hackers. 3. The data is described to be on a "secure server". Nothing in the program description details how the server is technologically secured. 4. Nothing in the program description details who authorizes people to view ALPR data. So far as I can tell from the description, once someone has completed the ACCESS training, they may self-select when and under what circumstances they will use it. Nothing indicates that supervisor permission is needed. Nothing appears to stop an officer from deciding to track a relative's vehicle, for instance. They are not supposed to, but the policy just says "don't". 5. The program description describes that the Neology software sets the 90 day limit and also that City IT deletes the data after 90 days in a SQL back end. These are not consistent. 6. Nothing in the program description details how the data is secured in the SQL backend against exfiltration. 7. Nothing in the program description details how ALPR data is secured in transmission between patrol cars and the "secure server". 8. ALPR data is retained for 90 days according to the policy. For the purposes described in the program description, there is no need to retain ALPR data at all; once a license plate is determined not to match, the data should be discarded. 9. The only measures described for deleting improperly retained data is that it is against policy. Nothing describes how that policy is enforced. 10. The Seattle PD OIG can audit the system, but nothing in the policy describes scheduled or random audits. 11. Nothing in the program description describes how the in vehicle computers are secured against malware. The existence of a USB port and a vehicle left unattended for 30 seconds is enough for someone to insert malware into the system. 12. Individuals can contest erroneous information about them collected by the system, but the policy as described is that much of the information that could be used to challenge erroneous information is discarded after 90 days. For instance, data on the license plates read before and after a reading that triggers the hotlist is not retained after 90 days. 13. Section 7.3 says that there is only a privacy risk if the public requests ALPR data and if they know which license plates belong to which people. Owners and users of vehicles can be relatively easily inferred from location data alone. Even stripping out license plate numbers leaves a privacy risk. Knowing that a car has been parked outside two particular places is a privacy risk (e.g., recorded outside both a residential home and a strip club). 14. Nothing in the document describes the redaction policy for ALPR data when it is subject to PRA requests. 15. Nothing in the document describes the threat models Seattle PD has for considering the security of ALPR data. 16. The duties and procedures of the ALPR administrator are barely described. They have control of the system but the program document only describes what they *can* do, not what policy mandates that they do. 17. This surveillance technology has apparently been in use for some time. Nothing in the document describes past audits, past problems, past discipline related to misuse of the technology, etc. Nothing in the document describes when the technology was adopted or how its use and governance has changed because of issues with the system. These are all necessary.

What recommendations would you give policy makers at the City about this technology?

This system needs to be scrapped.

Can you imagine another way to solve the problem this technology solves?

There's no need for any of this to be automated. We got along just fine without it up until now.

Do you have any other comments?

Seattle PD has been not-so-curiously silent that these meetings are taking place or that they are considering adopting these technologies. Nothing on the twitter feed. Nothing on SPD blotter. It wasn't on the main SPD page last week. SDOT had to put it on their twitter, the day of the first meeting and only a few hours beforehand. Someone had to be following the city's Techtalk blog to see this earlier.

ID: 10295310294

Submitted Through: Survey Monkey

Date: 10/22/2018 9:22:22 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Yes. I am concerned that it is not being deployed quickly and widely enough.

What value do you think this technology brings to our city?

Yes. I think it is clearly not being used enough. I frequently see cars with expired tags, people with out of state plates who have lived in Washington state for years, and there are many people driving without insurance or valid licenses. This technology could increase public safety and decrease insurance costs while increasing needed tax revenue to pay for transportation maintenance and improvements.

What worries you about how this is used?

Nothing. There is no expectation of privacy when driving or parking a car on a public road. I worry that by not using it effectively, people will needlessly be killed or injured while dangerous people continue to drive cars without insurance or with suspended licenses.

What recommendations would you give policy makers at the City about this technology?

Implement it quickly and effectively.

Can you imagine another way to solve the problem this technology solves?

Not in a cost or manpower efficient way.

Do you have any other comments?

No

ID: 10281786029

Submitted Through: Survey Monkey

Date: 10/15/2018 8:42:37 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

My concern stems from the Washington disclosure laws that compel police to disclose the collected data. The solution is simple. Don't eliminate the technology. Work with the Legislature to change the Public Records Act.

What value do you think this technology brings to our city?

The SIR sums it up. ALPR helps find stolen cars, enforce parking laws, find lost people, and solve serious crimes.

What worries you about how this is used?

No worries about how it is used by police. Law and policy apply to how police use it. It is absurd that state law makes the data available to the public. The City Council should focus on changing state disclosure law rather than endangering Seattle citizens by limiting police access to technology like this.

What recommendations would you give policy makers at the City about this technology?

Work with privacy advocates to persuade the legislature to protect ALPR data from public disclosure.

Can you imagine another way to solve the problem this technology solves?

Only if we tripled the number police officers on the street.

Do you have any other comments?

Transparency about what the government does is good but it shouldn't require disclosing ALPR data of innocent citizens.

ID: 10278400379

Submitted Through: Survey Monkey

Date: 10/14/2018 6:32:37 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

When did the Office of Inspector General (OIG) can conduct an audit of the system?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 10268043919

Submitted Through: Survey Monkey

Date: 10/9/2018 1:09:31 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

Yes.

What value do you think this technology brings to our city?

It allows aggregation of people's vehicles whereabouts and surveillance without warrant not cause. This makes governmental control of the population easier.

What worries you about how this is used?

It allows aggregation of people's vehicles whereabouts and surveillance without warrant not cause.

What recommendations would you give policy makers at the City about this technology?

Do not adopt this technology. Prohibit this technology from being used by non-governmental entities without first obtaining a permit.

Can you imagine another way to solve the problem this technology solves?

Do not aggregate the data. Do not store the data. Do not allow access to the data outside the vehicle the scanner is being used in.

Do you have any other comments?

ID: 10267989060

Submitted Through: Survey Monkey

Date: 10/9/2018 12:46:16 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Automated License Plate Reader (ALPR)

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

This technology establishes a precedent for breaching citizen privacy and does not benefit the city.

What worries you about how this is used?

I worry that this will contribute data to predictive policing.

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ALL COMMENTS RECEIVED ON GENERAL SURVEILLANCE

ID: 66

Submitted Through: Focus Group 1

Date: 11/8/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

no. Glad some surveillance is being used.

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 65

Submitted Through: Focus Group 1

Date: 11/8/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Technologies discussed are less dangerous then some other technologies in our personal lives

---

ID: 63

Submitted Through: Focus Group 1

Date: 11/8/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

not a lot of privacy anymore: google earth, maps, streetview

What value do you think this technology brings to our city?

What worries you about how this is used?

Google home is always listening. There is always someone listening to your conversations.

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Some of the images you can find online appear to be voyerism

ID: 61

Submitted Through: Focus Group 1

Date: 11/8/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Street sweepers coming in the middle of the night are ineffective, cars are parked and blocking areas

---

ID: 60

Submitted Through: Focus Group 1

Date: 11/8/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

Sometimes too much surveillance

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Curious about how much construction has to pay when blocking off half a block for parking.

ID: 56

Submitted Through: Mail

Date: 10/23/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Surveillance. I don't want it. Any of it. Just stop.

ID: 28

Submitted Through: Meeting 2

Date: 10/25/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Can you please do a better job telling the public about these meetings? Targeted Ads? KUOW - helped, Blogs, Newspaper - Poor turnout

---

ID: 27

Submitted Through: Meeting 2

Date: 10/25/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Most too technical and need to communicate better with public

---

ID: 26

Submitted Through: Meeting 2

Date: 10/25/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

Concerned about aggregation of technology and data collected

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

More transparent; less defnesive is how you gain trust

ID: 25

Submitted Through: Meeting 2

Date: 10/25/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

KC Parcel viewer information is too much. State listings of addresses of voters is a problem. Too much info has impact on DV victims - keeping them from voting

---

ID: 24

Submitted Through: Meeting 2

Date: 10/25/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Work and Human Rights Activist- Process too complicated. Can be benign but SPD doesn't make dark usage more clear. Info is too complex/data need better education for public on technologies.

ID: 23

Submitted Through: Meeting 2

Date: 10/25/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

No concerns as a professor. Traffic is getting worse - how do we make imporvements. How do we use data in other ways to improve our lives?

What value do you think this technology brings to our city?

Impressed by how City handles data - Check it and Chuck it

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Spent time on dark web and stunned by what they can do

ID: 53

Submitted Through: Meeting 4

Date: 10/30/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

People lose track of "public service" being performed. Misuse of data

---

ID: 52

Submitted Through: Meeting 4

Date: 10/30/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Hate to go "China route" tied to credit

ID: 51

Submitted Through: Meeting 4

Date: 10/30/2018

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

Restricted use: will it generate income? Mission creep. Report back to community

---

ID: 10334071978

Submitted Through: Survey Monkey

Date: 11/7/2018 9:41:13 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

Yes

What value do you think this technology brings to our city?

Minimal

What worries you about how this is used?

Very concerned about how red light enforcement cameras are racially unjust and frequently cause tickets to be issued to people of color.

What recommendations would you give policy makers at the City about this technology?

Remove red light cameras, if a particular intersection requires policing then assign officers to be posted there to create a presence that can be seen.

Can you imagine another way to solve the problem this technology solves?

Use officers in cars.

Do you have any other comments?

Red light cameras create an unjust, racially imbalanced burden on blacks, latinos and other marginalized groups. They should be eliminated from the city.

ID: 10328244312

Submitted Through: Survey Monkey

Date: 11/5/2018 8:41:00 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

We, the Critical Platform Studies Group, are a collective of researchers at the University of Washington Information School conducting a third-party ethnographic research study of the Seattle Surveillance Ordinance. In our ongoing research, we are conducting interviews with stakeholders on the processes leading to the revised Seattle Surveillance Ordinance. We have also compared the law to similar U.S. initiatives, and analyzed the functionality of each technology covered by Seattle's ordinance. Despite the salience of algorithmic processes in surveillance technologies, we are finding that the ordinance does not describe or address machine learning, artificial intelligence (AI), or algorithmic bias. We conclude that there is a pressing need for attention to algorithmic bias within disclosed surveillance technologies, for which we suggest additional elements be added to Seattle Surveillance Impact Reports, or by expanded stakeholder engagement in the RFP stage of the procurement process. Our preliminary findings that lead to these recommendations are as follows: *Expanded use of technologies triggers new surveillance review*: The Seattle ordinance models a strong process for submitting a given to technology to further review in the event its functionality or uses are expanded. *Law motivated by concern for marginalized groups*: The motivation for the Seattle Surveillance Ordinance was to protect groups that have historically been targeted by surveillance programs. Given that the implicit biases that have been demonstrated to exist in algorithmic systems invariably affect marginalized groups, it is critical to consider the algorithmic aspects and potential algorithmic biases in disclosed surveillance technologies. *Gap between perception and reality of current machine learning use*: Three municipal employees familiar with the Surveillance program stated that machine learning technologies are not used in technologies on the Master List. Contrary to these statements we found that at least two technologies on the Master List rely on machine algorithms---Automated License Plate Recognition (ALPR) and Booking Photo Comparison Software (BPCS). We found that at least two other technologies on the Master List rely on AI technology that could also be used long term in a way that implicates protected groups---i2 iBase and Maltego. The reliance on machine learning technologies likely introduces algorithmic bias, such as through "false positive" identifications. *Absence of algorithmic considerations in other surveillance ordinances*: None of the six municipal surveillance ordinances we surveyed included language for wrestling with algorithmic bias. *Opportunity to strengthen existing processes*: The Seattle Surveillance Impact Reports could include questions or prompts that would target and stimulate investigation into machine learning / AI facets or into algorithmic bias in disclosed surveillance technologies.

ID: 10326819811

Submitted Through: Survey Monkey

Date: 11/5/2018 9:14:43 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

Adaptive signal technology does not seem ready for a multimodal city where bikes/pedestrians need priority.

What value do you think this technology brings to our city?

It can potentially improve mobility and that has certainly been demonstrated for cars at least.

What worries you about how this is used?

It doesn't account for bikes or pedestrians or requires some sort of additional effort (like installing an app) to work for those groups.

What recommendations would you give policy makers at the City about this technology?

Are these technologies helping or hurting the vision zero goals?

Can you imagine another way to solve the problem this technology solves?

I would question whether cars being in gridlock is a problem that can be solved or simply a consequence of the culture that we are encouraging in a dense city.

Do you have any other comments?

ID: 10326707921

Submitted Through: Survey Monkey

Date: 11/5/2018 8:38:49 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

No

What value do you think this technology brings to our city?

As our population grows this is the only way to enforce laws as we don't have enough police to do it

What worries you about how this is used?

None. If you're abiding by the law you have nothing to fear

What recommendations would you give policy makers at the City about this technology?

Allow police to use it to their advantage to do their job to keep us all safe, but don't use it against them!

Can you imagine another way to solve the problem this technology solves?

Create an environment that would make police want to stay in Seattle and do the job they were hired to do.

Do you have any other comments?

See above

ID: 10324587536

Submitted Through: Survey Monkey

Date: 11/4/2018 3:55:12 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

License plate cameras in general, I'm supportive of, if they can be used at greater frequency to crack down on illegal parking and driving.

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Full steam ahead! Bus lane camera on every bus, so that operators can push a button to send video of an illegal bus lane violator or other moving/parking violations when they see one, to get folks to drive better.

Can you imagine another way to solve the problem this technology solves?

Literally no.

Do you have any other comments?

I have no worries about these technologies. Get bus cameras online ASAP.

ID: 10322210731

Submitted Through: Survey Monkey

Date: 11/2/2018 9:47:34 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

This is government overreach and Big Brother at it's finest. Surveillance technologies do not belong in a free society and are solely implemented to farm money from taxpayers for minor infractions, at "best".

What value do you think this technology brings to our city?

None; outside of the ticket-issuing racket.

What worries you about how this is used?

Law Enforcement will abuse this technology. As a prior victim of stalking at the hands of a Law Enforcement Officer, we don't need to give Police more surveillance tools which make it easier to harass citizens.

What recommendations would you give policy makers at the City about this technology?

Do not turn Seattle into Singapore, China, or the United Kingdom. America is The Land of the Free. We don't want to be under the Watchful Eye of Big Brother.

Can you imagine another way to solve the problem this technology solves?

Use your eyes and have officers enforce the law as needed.

Do you have any other comments?

Robots are not Sworn Officers of the Law. SPD should be writing tickets, not computers. This technology will likely be abused, it will violate privacy laws, and I don't trust the Government to keep secure such a Mass Surveillance system. The costs of securing and maintaining such a system will require massive amounts of artificial "ticketing". At best, this is a Perpetual Revenue Generator for City Hall; at worst, it's a Gross Violation of Our Civil Rights.

ID: 10315099454

Submitted Through: Survey Monkey

Date: 10/30/2018 7:57:58 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

No

What value do you think this technology brings to our city?

Hi it brings proof. It impacts crime before it occurs.

What worries you about how this is used?

Mone

What recommendations would you give policy makers at the City about this technology?

Where you see lots of camera you see less crime.

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 10314183202

Submitted Through: Survey Monkey

Date: 10/30/2018 12:34:32 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

The location of the cameras/where the police vans circulate can be racially discriminatory. The city should make sure that these are distributed equitably.

What recommendations would you give policy makers at the City about this technology?

If the city is already going to be placing these cameras, they should also use these cameras to enforce speeding violations. Cars are always driving dangerously fast in this city, and these cameras should also make people follow the law.

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 10312185174

Submitted Through: Survey Monkey

Date: 10/29/2018 7:45:04 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

Yes

What value do you think this technology brings to our city?

What worries you about how this is used?

Over-policing. Waste of tax money. City government probably isn't sufficiently organized or skilled to process and analyze the data collected. It will ultimately lead to more overly bureaucratic, under-skilled, departments hopelessly trying to learn how to use the equipment and manage a massive records collection. The City should think twice before tying their shoes together on this one. It won't turn out well. I suggest you save yourselves the headache and bad PR by abandoning any surveillance plans now.

What recommendations would you give policy makers at the City about this technology?

Fire whoever is responsible for trying to waste tax money on invasive surveillance equipment. Also, whoever wrote question #6 should take a course on writing unbiased survey questions because the question assumes that the proposed surveillance equipment in fact solves a problem but that is not an established truth.

Can you imagine another way to solve the problem this technology solves?

This is a loaded question. It does not solve a problem. It creates an IT nightmare, costs way too much to store the data, invasive surveillance, and bad PR. Eventually, someone involved will likely lose a future election as a result.

Do you have any other comments?

ID: 10312163737

Submitted Through: Survey Monkey

Date: 10/29/2018 7:35:08 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

Yes, I don't agree on public surveillance. This is America not China!

What value do you think this technology brings to our city?

I think it strips me from my right as a citizen and make me feel like the whole country is big huge jail

What worries you about how this is used?

How it's interpret and what people of color will have to go through to not been punished for small and trivial crimes.

What recommendations would you give policy makers at the City about this technology?

We're not ready, this is not London. Don't do it!

Can you imagine another way to solve the problem this technology solves?

I don't think it's solving a problem as much as it's creating one.

Do you have any other comments?

Don't do it!

ID: 10310577035

Submitted Through: Survey Monkey

Date: 10/29/2018 8:13:55 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

Yes, the police are not honest about how and when they use this technology which means they are violating the 4th amendment rights which is a federal offense. Are they held accountable? No, almost never.

What value do you think this technology brings to our city?

The percentage of crimes solved with these technologies is a very small amount. And violating 4th amendment rights is a normal act by police in many of those instances.

What worries you about how this is used?

I support the pursuit of justice to make our city safer but but lawful citizens and criminals all have rights which the police disregard because there is no price to pay. If you could cheat and got caught doing so but there was no consequences, why wouldn't you? Its examples like this in our leaders, public officials and public servants that have eroded society and the trust people in each other.

What recommendations would you give policy makers at the City about this technology?

Until we have good honest leaders at the top who oversee the ones who use these technologies and who have no bias about who is held accountable for violations of ANY kind, they should be sidelined.

Can you imagine another way to solve the problem this technology solves?

Good morals and the respect for your fellow humans. It starts with the people on top to set good examples. We as a society have gotten more numb to violence, dishonesty and corruption at the highest levels ,it has now sown itself into our way of life. If we see this kind of behavior from the people that are "roll models" or "leaders" then we adopt them as our own values.

Do you have any other comments?

Unfortunately, corruption is widespread in government agencies and public enterprises. Our political system promotes nepotism and wasting money. This has undermined our legal system and confidence in the functioning of the state. Communism is the corruption of a dream of justice.

ID: 10307049643

Submitted Through: Survey Monkey

Date: 10/26/2018 7:08:32 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

I need the red light cameras NOT to have flash equipment on them. These lights are too bright, and they flash without warning, blinding people on the sidewalks at intersections.

What value do you think this technology brings to our city?

Damn all. It may be that drivers get citations--but this does not compensate for the blinding of pedestrians, bicyclists, etc.

What worries you about how this is used?

I have several times been so bedazzled and startled that I might easily have stumbled into traffic, if I'd chanced to be closer to the curb.

What recommendations would you give policy makers at the City about this technology?

Get cameras that don't need so much light, if you INSIST on having such cameras.

Can you imagine another way to solve the problem this technology solves?

Since I don't think it solves anything, no.

Do you have any other comments?

Other cameras are intrusive and invasive--but they're not so immediately dangerous, generally.

ID: 10307028243

Submitted Through: Survey Monkey

Date: 10/26/2018 6:42:15 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

None of these technologies are novel, particularly compared to other parts of the world (Europe, Asia). However, the use of the automated parking enforcement technology specifically for the purpose of booting cars is of highly questionable value.

What value do you think this technology brings to our city?

Hopefully some efficiencies in reducing human effort required to perform basic data-gathering and enforcement. If the parking enforcement buggies can cover many more blocks in a day, or a police officer yanks someone out of a car that's actually stolen, great!

What worries you about how this is used?

Abuse of data access, lax enforcement of retention and removal-of-access policies, above SECURITY BREACH OF DATA that may be useful in some level of identification (car with plate X was seen at location Y at time Z). Be wary of social justice impacts, particularly of the auto-boot technology. Those who are the most vulnerable may be in more frequently trouble with the law (and absolutely unable to rectify fines) and would thus unable to reach services. It would be absolutely unacceptable if a vulnerable member of the population who may be living in a vehicle is booted and unable to access basic human services, or worse.

What recommendations would you give policy makers at the City about this technology?

Data security is of paramount importance -- if data cannot be handled safely by the right people at the right time with prompt removal processes for data and access, then none of this matters and the public trust is gone. If there are any questions about this whatsoever, do not proceed with adoption. After that is transparency. Be specific about what is gathered, down to individual data elements: publicly post the data schemas (but obviously not the data). E.g., when your license plate is recorded, it also gathers: date, time, location, and so on. Finally, policies about use must be clearly understood by the public and the civil servants the tech is entrusted too. "SPD may use tech [when] for [reason] in order to perform duty [elaborate]." "SDOT uses these cameras to perform analysis of [condition]". People care about access and retention policies in this day and age -- post them and perform routine audits no less than quarterly but ideally more often than that (again, posting results publicly).

Can you imagine another way to solve the problem this technology solves?

Drone-mounted cameras can be used to gather movement data for travel time analysis; this doesn't require the use or exposure of any identifying marks whatsoever. They may also be helpful for SFD response scenes to perform rapid large area surveys.

Do you have any other comments?

Addressing these topics with serious care and thoughtfulness raises chances of success. Be intentional about uses of these technologies and do not allow for hidden uses.

ID: 10307002973

Submitted Through: Survey Monkey

Date: 10/26/2018 6:13:10 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

Not particularly

What value do you think this technology brings to our city?

CCTV makes this city safer, particularly since we are so short of police officers.

What worries you about how this is used?

Nothing

What recommendations would you give policy makers at the City about this technology?

Beat policemen are better.

Can you imagine another way to solve the problem this technology solves?

Policemen/women who walk or ride bikes in the same neighborhood on a daily basis. We've all read English novels. Doesn't the bobby on his beat seem like the best way to protect a neighborhood, and make a neighborhood feel safe?

Do you have any other comments?

I've lived in Ballard for 35 years. In the last five years I've put grates on my windows, bought a wrought-iron screen door, locked the gate to the backyard. This is after the theft of my bicycle from my shed, shoes from my porch, etc. Opioids. The government is cracking down on doctors who overprescribe. How about cracking down on street drug dealers as well? If a bath tub is overflowing from two spigots going full blast, turning off only one of those spigots doesn't work. Gotta turn off both.

ID: 10306958976

Submitted Through: Survey Monkey

Date: 10/26/2018 5:25:35 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

I do have concerns. However, if there is public oversight of the surveillance technology used, both by elected officials and through releases of content recorded to the general public, then these concerns will be sufficiently addressed.

What value do you think this technology brings to our city?

I think this has the ability to automate many of the services currently done by the city. Further, it can provide hard evidence of events that occurred which human testimony cannot do.

What worries you about how this is used?

I am worried that these systems could be used by its operators to spy on people they know or to blackmail individuals both known and unknown to the operators. The accountability to elected officials and through releases to the public would prevent these things from happening.

What recommendations would you give policy makers at the City about this technology?

Make sure there is actual transparency and accountability to the general public and the press, and make sure this technology is about automation and providing evidence, not to keep tabs on people.

Can you imagine another way to solve the problem this technology solves?

no

Do you have any other comments?

ID: 10303980026

Submitted Through: Survey Monkey

Date: 10/25/2018 12:46:20 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

I have concerns about the validity of Seattle's privacy program after listening to Seattle's Chief Privacy Officer on KUOW today. Per Ordinance 125376, greykey (the ability for the Seattle Govt to unlock iphones without having the password) should have been reviewed by the Privacy Officer Armbruster, but it wasn't and she provided no explanation why. She offered no apology. This lacks transparency and accountability.

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 10300614662

Submitted Through: Survey Monkey

Date: 10/24/2018 9:04:59 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

yes

What value do you think this technology brings to our city?

On a world level, at the federal government level, and at the city level we move closer towards fascism and other forms of authoritarianism, expanded surveillance will give expanded power to authoritarian regimes such as ours.

What worries you about how this is used?

The list of technologies for surveillance should include all other 'law' inforcement agencies at work in our city such as ICE.

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

As I sat down on the Seattle Trolley on Jackson Street a drone flew up and held stationary and then titled slightly up. The blue lens of a camera flashed and the drone banked off. I'd like to know what other technologies are at use in our city, by ICE for instance as well as other 'law' agencies.

ID: 10299219171

Submitted Through: Survey Monkey

Date: 10/23/2018 7:14:36 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

in general I'm concerned about the collection, retention, aggregation, sharing, and mining of information collected thru surveillance technologies, particularly with regard to the risk for abuse by agencies like ICE or other yet-to-be created Federal agencies that do not represent the views of the Seattle area population.

What value do you think this technology brings to our city?

Emergency Scene cameras give medical professional an opportunity to prepare for treating emergencies and protect first responders from frivolous lawsuits. Hazmat cams gather information while allowing humans to remain at a safe distance. The rest of them essentially allow the city to more effectively collect revenue, except for ALPR, which scans licenses in search of stolen cars or vehicles sought for other reasons.

What worries you about how this is used?

ALPR is essentially a surveillance dragnet. Data is retained for 90 days even on vehicles that have nothing to do with anything.

What recommendations would you give policy makers at the City about this technology?

Do not retain any ALPR data except that which pertains to tagged vehicles. In general, always err on the side of not collecting data, not storing it, and not sharing it. Please. I work for Google.

Can you imagine another way to solve the problem this technology solves?

Fund transportation infrastructure so we don't have so many cars on the road running traffic lights and hitting pedestrians and cyclists and being driven by drunks.

Do you have any other comments?

Thank you for the opportunity to comment.

ID: 10298281561

Submitted Through: Survey Monkey

Date: 10/23/2018 11:18:38 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

It seems like all of these technologies are primarily focused on the movement of vehicles through Seattle instead of pedestrians and their own needs

What value do you think this technology brings to our city?

Giving the illusion of gathering useful, but inactionable, data.

What worries you about how this is used?

general privacy concerns about collecting so much data. There's no such thing as perfect security, to say the least.

What recommendations would you give policy makers at the City about this technology?

Use it to benefit the most vulnerable road users: pedestrians, including cyclists and other small transport methods/vehicles.

Can you imagine another way to solve the problem this technology solves?

Does it solve things? It's a bit early to say that.

Do you have any other comments?

Stop focusing on car throughput, and instead focus on people.

ID: 10298170617

Submitted Through: Survey Monkey

Date: 10/23/2018 10:37:29 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

Can you quantify the # of crime investigations, stolen cars recovered and $ amount of traffic violations recovered by using the ALPR/LPR technology.

What value do you think this technology brings to our city?

I am concerned that we are trading our privacy for a "sense" of security. How have surveillance technologies incrementally affected our security in Seattle.

What worries you about how this is used?

slippery slope -- see "The Last Enemy" film

What recommendations would you give policy makers at the City about this technology?

I'd like to see more police body cams; less surveillance;

Can you imagine another way to solve the problem this technology solves?

I have not been convinced except in the case of the Fire Department technology that we are actually better off -- I need to see numbers.

Do you have any other comments?

I would like to see year over year numbers comparing "before technology - after technology"

ID: 10296707285

Submitted Through: Survey Monkey

Date: 10/22/2018 9:13:04 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

The public ought to be made aware of all surveillance technologies being used. In the case of permanent fixed surveillance devices such as cameras, the public should be readily able to find information about where all such devices are installed.

What value do you think this technology brings to our city?

The provided examples of traffic monitoring seem useful. However, a full-blown security system similar to the widespread CCTV coverage in London seems overly pervasive.

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Minimize the number of surveillance devices implemented, and make their locations available for online viewing by the public at any time. No surveillance devices should be installed without informing the public.

Can you imagine another way to solve the problem this technology solves?

Security cameras should be limited to guarding private property or specific locations of concern, and not used to generally monitor all public areas at all times.

Do you have any other comments?

ID: 10296428154

Submitted Through: Survey Monkey

Date: 10/22/2018 5:35:21 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 10295649414

Submitted Through: Survey Monkey

Date: 10/22/2018 11:24:46 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

I don't want any surveillance. Any of it. Let us live privately and in peace. Just stop.

What value do you think this technology brings to our city?

I don't want any surveillance. Any of it. Let us live privately and in peace. Just stop.

What worries you about how this is used?

I don't want any surveillance. Any of it. Let us live privately and in peace. Just stop.

What recommendations would you give policy makers at the City about this technology?

I don't want any surveillance. Any of it. Let us live privately and in peace. Just stop.

Can you imagine another way to solve the problem this technology solves?

I don't want any surveillance. Any of it. Let us live privately and in peace. Just stop.

Do you have any other comments?

I don't want any surveillance. Any of it. Let us live privately and in peace. Just stop.

ID: 10295424650

Submitted Through: Survey Monkey

Date: 10/22/2018 10:02:24 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

SPD has proved over decades that it should BE constantly monitored, rather than be further enabled to abuse - the inseparable seduction of its under-controlled power.

What value do you think this technology brings to our city?

Surveillance tech further dehumanizes and commoditizes residents. A better SPD investment would be in outside beat walking and mingling with citizens.

What worries you about how this is used?

SPD is under Federal oversight due to its documented abuses. Its modus operandi are Trumpist (i.e. thrive only in the dark). We have witness where that tends.

What recommendations would you give policy makers at the City about this technology?

No Councilperson can adequately oversee or hold accountable her portfolio, let alone the Mishmash and Safe Communities octopus. Until proven effective governance by elected officials obtains, no greater powers should be distributed to SPD.

Can you imagine another way to solve the problem this technology solves?

The morality police in Iran and Saudi Arabia and the like in China demonstrate that everyday citizens are readily induced to spy and report on their neighbors. Although beyond the pale, a progressive version of neighborly support and assistance should be the direction Seattle pioneers to deal with the pressing problems of Mass Humanity.

Do you have any other comments?

One cannot "tech" to a humanitarian city, least of all through an insidiously equipped praetorian armed force. SPD elevates the interests of its minuscule membership above those of a citizenry whose dwarf it in all regards. City Council year-in/year-out approves the contracts cementing this folly. Seattle needs a formal goal of reducing its separate-but-armed constituency into the service element it should be, not the formidable power-center it is.

ID: 10295330166

Submitted Through: Survey Monkey

Date: 10/22/2018 9:29:06 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

Yes. We have crimes and shootings that occur in public areas where there is no reasonable expectation of privacy but we lack the info to respond effectively.

What value do you think this technology brings to our city?

By placing cameras in certain areas with frequent criminal activity we could both deter and aid in the arrest and prosecution of those responsible. The city is undergoing an epidemic of property crime and dumping of garbage in many areas. Cameras could help deter, aid in the arrest/fines and prosecution of those responsible.

What worries you about how this is used?

Very little. If used in public spaces there is no reasonable expectation of privacy. If there is concern about privacy or tracking, the data could be encrypted by default and then made available to police after an incident with a court order or approval of some oversight body.

What recommendations would you give policy makers at the City about this technology?

Hurry up and put cameras in place where it makes sense. If there are privacy concerns, implement some kind of a check on access but get moving.

Can you imagine another way to solve the problem this technology solves?

Not cost effectively.

Do you have any other comments?

ID: 10295152382

Submitted Through: Survey Monkey

Date: 10/22/2018 8:30:01 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

A person could be set up, I suppose. I just read that the journalist who was murdered in the embassy....well his ambushers had a double for him. Now whether this is true or not it could happen. Of course facial recognition might put a stop to imposters posing as someone else.

What value do you think this technology brings to our city?

Safety in public spaces is increased...although, it is sadly 'after the fact' that it is usually the most effective. I think that just the knowledge that you might be watched could deter criminal behavior or, for that matter, abuse by law enforcement. It works both ways. Also, if you had more speed detectors you could generate a lot of revenue with speeding tickets. I can't tell you the number of times I've had cars speed by me in neighborhoods where speed limits are 25 mph. I know police can't be everywhere...but cameras can be. People are much less respectful nowadays. I drive to neighborhoods all over Seattle 5 days a week as a caregiver and have people honking at me because I'm driving too slow for them. I wish I could take the Mayor along with me on some of my trips so she could see first hand how rude people can be.

What worries you about how this is used?

It will alleviate my worries about road rage....maybe make people feel safer walking about outside...especially those most vulnerable who stay cooped up in their homes too afraid to go outside.

What recommendations would you give policy makers at the City about this technology?

Please...more sir. I would love to see children outside playing...who aren't afraid of being outside playing...in quiet neighborhoods or parks. We need these cameras etc. if only to act as a babysitter in some respects.

Can you imagine another way to solve the problem this technology solves?

Change human nature....which is nearly impossible.

Do you have any other comments?

I'm sure there would be people who could try to use surveillance to watch women etc.....when I was younger I've had police pull me over I'm sure just to check me out...stupid weirdos....BUT there is a lot of good to be had with watching over the public for the public good

ID: 10291758143

Submitted Through: Survey Monkey

Date: 10/19/2018 2:19:06 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

No, I support surveillance cameras, even as I understand this is a tradeoff to privacy. But, CC TVs are widely accepted and extraordinarily helpful for law enforcement in other countries such as the UK.

What value do you think this technology brings to our city?

The ability to safeguard spaces and revisit victimizations.

What worries you about how this is used?

How long the data is kept. We should have a period of time that the data is kept after which it is destroyed.

What recommendations would you give policy makers at the City about this technology?

Adopt this widely.

Can you imagine another way to solve the problem this technology solves?

NO.

Do you have any other comments?

As a UW professor who studies law, I fully support better surveillance of our population--this includes police, citizens, and so on.

ID: 10287347565

Submitted Through: Survey Monkey

Date: 10/17/2018 9:55:10 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

No. Technology is ubiquitous; surveillance is everywhere. Technology plays a pivotal role in keeping our communities safe. The paranoia of some should be easily address by strong policies and auditing of use.

What value do you think this technology brings to our city?

Technology is critical to solving crime, deterring crime, and bringing criminals to justice, and providing closure to victims.

What worries you about how this is used?

I worry that it is not used enough. I live in the South End, yes, in a black community (I am black) and we have been pleading with the city (you, Councilmember Harrell) for cameras for years. The ACLU, and supposed "community activists", do not speak for the average among us who go to work, take our kids to school, and just want to live in a safe community.

What recommendations would you give policy makers at the City about this technology?

Lead. Do what you're paid to do. Protect the communities you serve, and allow - perhaps even enable - the police to keep our communities safe.

Can you imagine another way to solve the problem this technology solves?

A ridiculous question. If the city's not going to invest in a technological solution, why would the city invest in a lesser solution?

Do you have any other comments?

Please, do not hamstring our first responders anymore. Property crime is rampant. Auto theft is rampant. Our kids are being robbed on the street. And you want to TAKE AWAY tools to solve crime?? We want cameras - like we were promised, Councilmember Harrell. We want crimes solved, and deterred. Do not let absurdity rule the day.

ID: 10281389699

Submitted Through: Survey Monkey

Date: 10/15/2018 4:13:31 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

No

What value do you think this technology brings to our city?

Possible reduction in open street crimes

What worries you about how this is used?

May be comsidered not useful to detect crimes in low income communities.

What recommendations would you give policy makers at the City about this technology?

Use the technologies to cut down the kidnappers/rapist-- violent sex predators working and living in southend housing.

Can you imagine another way to solve the problem this technology solves?

Police patrols more often and seizure--not just showing up and leaving the scene.

Do you have any other comments?

The city seems to be over-run by kidnappers raping, I am getting sick to my stomach. Violent Sex Predators seem to be running the city via what I know.

ID: 10281279313

Submitted Through: Survey Monkey

Date: 10/15/2018 3:10:22 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 10273624842

Submitted Through: Survey Monkey

Date: 10/11/2018 1:35:22 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

What value do you think this technology brings to our city?

What worries you about how this is used?

What recommendations would you give policy makers at the City about this technology?

Can you imagine another way to solve the problem this technology solves?

Do you have any other comments?

ID: 10271359916

Submitted Through: Survey Monkey

Date: 10/10/2018 6:19:02 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

I think we need more. Especially at every bus stop.

What value do you think this technology brings to our city?

Hopefully catching criminals

What worries you about how this is used?

Nothing

What recommendations would you give policy makers at the City about this technology?

More cameras.

Can you imagine another way to solve the problem this technology solves?

No

Do you have any other comments?

ID: 10270768915

Submitted Through: Survey Monkey

Date: 10/10/2018 1:10:42 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

No

What value do you think this technology brings to our city?

I think it has great value in areas of high use, especially in areas where crime is historically reported. Both deterrent to crime and tool that helps law enforcement in the event crime has occurred.

What worries you about how this is used?

totally ok with it, as long as it's targeted in areas of heavy use, congested areas, high volume of people, areas with historically issues with crime, etc.

What recommendations would you give policy makers at the City about this technology?

Make sure law enforcement has real time access. Limit access to law enforcement type groups, don't get sidetracked as to possible other uses of the data.

Can you imagine another way to solve the problem this technology solves?

more police officers

Do you have any other comments?

Believe this is a cost effective way to help keep people safe.

ID: 10270556248

Submitted Through: Survey Monkey

Date: 10/10/2018 11:50:08 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

I do not want increased surveillance. License Plate Readers,

What value do you think this technology brings to our city?

None.

What worries you about how this is used?

Privacy and tracking concerns are rampant in an age where social media [LinkedIn] is almost required for a profession, a cell phone is required for jobs, and cars are required for jobs. StingRay [cell phone interceptor] has already been shown to be used unlawfully. I can only imagine a database version would be subject to equal lack of scrutiny.

What recommendations would you give policy makers at the City about this technology?

Vote no.

Can you imagine another way to solve the problem this technology solves?

Mountains out of molehills. Patrol HOV lanes.

Do you have any other comments?

Enforce HOV restrictions.

ID: 10270098107

Submitted Through: Survey Monkey

Date: 10/10/2018 9:10:36 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

ALPR/LPR: how is this technology used; if the data is being passively collected - how can the general public audit the back-end systems for sake of privacy (in the age of data breaches, this is a risk of *when* there is a breach and not *if*)

What value do you think this technology brings to our city?

Studies have shown that increased surveillance does not actually lead to reduced crime. More studies have also shown that community watch organisations do more to reduce crime than passive/active remote surveillance.

What worries you about how this is used?

Unclear duration of data usage, sharing and retention, and public request process to remove targeted data.

What recommendations would you give policy makers at the City about this technology?

Carefully evaluate vendors and their products to make sure the systems are hardened against breaches; evaluate whether the systems allow for public access to the data so that people can limit invasive surveillance.

Can you imagine another way to solve the problem this technology solves?

Better community education and watch programs. Try to find root causes of crimes and solve those causes. Surveillance is a short term gain with long term consequences and it doesn't address the problem of why crimes happen. Getting to the root cause may prove to be more productive (and in some cases, cost less public money)

Do you have any other comments?

ID: 10269149042

Submitted Through: Survey Monkey

Date: 10/10/2018 1:58:48 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

General Surveillance comment

Do you have concerns about this specific technology or how it is used?

With all of these technologies, my main concern is unnecessary storage and retention. For example, what if you're storing some kind of information on people's cars, which then is acquired by ICE to prosecute undocumented individuals in spite of our city's sanctuary status?

What value do you think this technology brings to our city?

I believe there is value in the diagnostic capabilities, for example finding out what kind of traffic levels there are on a street or sidewalk, finding out how many bus lane cheaters there are, or maybe finding a pattern of frequent dangerous behavior on a street. In the same vein, I'm extremely supportive of having cameras on buses that bus operators can use to report bus lane violations because I think the

level of bus lane violations we have is a serious impediment to our transportation system. I also appreciate that tech like this removes any prejudices that a police officer may have. Either you broke the law, or you didn't. I love that this tech will be used in parking enforcement. We need to enforce our traffic laws or nobody will care.

What worries you about how this is used?

Though it removes prejudice on the part of officers, I do also think this may be sub-optimal in some circumstances. Perhaps someone as speeding by only 1 mile per hour, which reasonably, we should let slide, but with cameras, we probably won't.

What recommendations would you give policy makers at the City about this technology?

Bus and bike lane camera enforcement, yes! You have no idea how many times some bus lane violators slow down a 60-person bus, or someone blocks the bike lane forcing me to make an unsafe movement. I'd also love to see box blocking or crosswalk blocking detection technology to prevent those things from happening because it seriously reduces the livability and safety of pedestrians and transit users. Don't have any facial recognition software though.

Can you imagine another way to solve the problem this technology solves?

I don't know how actionable this is, but maybe we could work with the judicial system to give the law a little bit of discretion on the prosecution of crimes, so for example if you're speeding by 1 mph, you don't get the same fine as someone speeding by 10 mph or 30 mph.

Do you have any other comments?

Please implement bus/bike lane enforcement cameras yesterday. I get there are challenges WRT privacy and whatnot, but if we're sensitive to these issues, we can make our city safer.

APPENDIX F: LETTERS FROM ORGANIZATIONS

Shankar Narayan
TECHNOLOGY AND LIBERTY PROJECT DIRECTOR

ACLU
AMERICAN CIVIL LIBERTIES UNION of WASHINGTON

October 24th, 2018

RE: ACLU-WA Comments Regarding Group 1 Surveillance Technologies

Dear Seattle IT:

On behalf of the ACLU of Washington, I write to offer the ACLU-WA's comments on the surveillance technologies included in Group 1 of the Seattle Surveillance Ordinance process. We are submitting these comments by mail because they do not conform to the specific format of the online comment form provided on the CTO's website, and because the technologies form groups in which some comments apply to multiple technologies.

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON
901 5TH AVENUE, STE 630
SEATTLE, WA 98164
T/206.624.2184
WWW.ACLU-WA.ORG

JEAN ROBINSON
BOARD PRESIDENT

KATHLEEN TAYLOR
EXECUTIVE DIRECTOR

These comments should be considered preliminary, given that the Surveillance Impact Reports for each technology leave a number of significant questions unanswered. Specific unanswered questions for each technology are noted in the comments relating to that technology, and it is our hope that those questions will be answered in the updated SIR provided to the City Council prior to its review of that technology.

The technologies in Group 1 are covered in the following order:

I. Automated License Plate Recognition (ALPR) Group

1. Automated License Plate Recognition (ALPR)(Patrol)(SPD)
2. Parking Enforcement Systems (Including ALPR)(SPD)
3. License Plate Readers (SDOT)

II. Camera Group

1. Emergency Scene Cameras (SFD)
2. Hazardous Materials (Hazmat) Camera (SFD)
3. Closed Circuit Television "Traffic Cameras" (SDOT)

I. ALPR Group

Automated License Plate Reader Systems (ALPRs) are powerful surveillance technologies that have the potential to significantly chill constitutionally protected activities by allowing the government to create a detailed picture of the movements—and therefore the lives—of a massive number of community members doing nothing more than going about their daily business. Indeed, at the first public meeting seeking comment on the SPD Patrol ALPRs, it was revealed that the ALPR system collected

1

37,000 license plates in a 24 hour period—which equates to over *13.5 million* scans over a full year. The overwhelming majority of these drivers are not suspected of any crime.

With this massive database of information, agencies can comprehensively track and plot the movements of individual cars over time, even when the driver has not broken any law. This enables agencies, including law enforcement, to undertake widespread, systematic surveillance on a level that was never possible before. Aggregate data stored for long periods of time becomes more invasive and revealing. Existing law in Seattle places no specific limits on the use of ALPR technology or data, meaning an agency can choose whether and how they want to retain data and track vehicle movements.

ALPR technology can be used to target drivers who visit sensitive places such as centers of religious worship, protests, union halls, immigration clinics, or health centers. Whole communities can be targeted based on their religious, ethnic, or associational makeup, and indeed, exactly that has happened elsewhere. In New York City, police officers drove unmarked vehicles equipped with license plate readers around local mosques in order to record each attendee as part of a massive program of suspicionless surveillance of the Muslim community. In the U.K., law enforcement agents installed over 200 cameras and license plate readers to target a predominantly Muslim community suburbs of Birmingham. ALPR data obtained from the Oakland Police Department showed that police there disproportionately deployed ALPR-mounted vehicles in low-income communities and communities of color. And the federal Immigration and Customs Enforcement agency has sought access to ALPR data in order to target immigrants for deportation. All of these concerns are magnified in light of a long history of the use of invasive surveillance technologies to target vulnerable communities (see, for example, Simone Browne's excellent, multidisciplinary book on the subject, *Dark Matters: On the Surveillance of Blackness*).

The foregoing concerns suggest the Council should ensure strong protections against the misuse of this technology, regardless of which agency is deploying it and for what purpose. Specific comments follow.

1. Automated License Plate Recognition (ALPR)(Patrol)(SPD)

The SIR relating to Patrol ALPRs raises a number of specific concerns around current policy and practice, and leaves open a number of significant questions. I attempt to capture these in sections below on concerns, questions, and recommendations.

a. Major Concerns

- *Inadequate Policies.* Policies cited in the SIR are vague, contradictory, and appear to impose no meaningful restrictions on the purposes for which ALPR data may be collected or used. Policy 16.170—the only apparent policy specific to ALPRs—for example, is very short, contains undefined terms, and focuses on training rather than use. Subsection 3 of the policy says that "ALPR Operation Shall be for Official Department Purposes" and that ALPR may be used "during routine patrol or any criminal investigation." This does not meaningfully restrict

the purposes for which ALPR may be used. And another part of the policy states that ALPR data may be accessed only when it relates to a specific criminal investigation—yet it is unclear how this relates to the enforcement of civil violations mentioned in both SPD SIRs. More generally, much of the practice described in the SIR does not appear to be reflected in any written policy at all (for example, the practice of manually verifying a hit visually is not reflected in policy).

- *Dragnet Use with No Justification.* While the SIR contains contradictory information on this point, it appears that ALPR cameras are always running, offering a vast dragnet of data collection. No legal standard is stated to justify this general, dragnet use. The Seattle Intelligence Ordinance is cited, but SPD seems to assume that dragnet surveillance is consistent with this Ordinance, without any specific policy (for example, are ALPR-equipped vehicles kept away from protests?).

- *Lengthy Retention Window with No Justification.* SPD retains ALPR data for 90 days, but examples given in the SIR of crimes solved using ALPRs largely appear to involve immediate matches against a hotlist. It is unclear what justifies this long retention window.

- *Data Sharing is Not Explicitly Limited by Policy or Statute.* The sharing of ALPR data with other agencies is of great concern, and SPD states a variety of situations in which such data may be shared (see SIR Section 6.1). But the policies cited do not make clear the criteria for such sharing, nor any inter-agency agreement that governs such sharing, nor why the data must be shared in the first place (see perfunctory answer to SIR Section 6.2). This issue of data sharing was raised in the enactment of the Surveillance Ordinance itself, and has only become more urgent under the current federal administration.

- *Inadequate Auditing.* The SIR appears to contradict itself on the subject of whether and how audits of inquiries to the system can be conducted (see SIR Sections 4.10 and 8.2, for example). As with any invasive surveillance system, a clear and regular audit trail to protect against abuse is important.

b. *Outstanding Questions*

I'm listing questions here that I hope will be answered in an updated SIR:

- To what degree are patrol and parking enforcement ALPR systems are separated, and do SPD policies on ALPR apply fully to the Parking Enforcement Systems? It appears the systems are merged at least to some extent, and in that case, the same strong protections against abuse should be applied to all systems.

- ALPR policy says there has to be a specific criminal investigation in order for ALPR data to be accessed. Does reasonable suspicion of a crime equate to a

specific criminal investigation? How is a specific criminal investigation documented?

- Under what agreements is data shared with outside agencies, and where "required by law," what specific laws require this sharing? To which systems outside SPD is data uploaded?

- How many plate images collected by the system every day? What is the hit rate on those images? Is there systematic data reflecting how many crimes each year are actually solved using ALPR data?

- How often do misreads occur? Are they systematically tracked?

c. *Recommendations*

These recommendations should be considered preliminary, pending answers to the questions above. But we urge the Council to ensure binding enforceable protections in ordinance that ensure the following minimum protections:

- Dragnet use and long retention of ALPR data should be outlawed. SPD must have reasonable suspicion that a crime has occurred before examining collected license plate reader data; they must not examine license plate reader data in order to generate reasonable suspicion. SPD should retain no information at all when a passing vehicle does not match a hot list (particularly given that such data is subject to public disclosure, including to federal agencies).

- People should be able to find out if plate data of vehicles registered to them are contained in SPD's ALPR database. They should also be able to access the data.

- There must be access controls on the ALPR databases, with only agents who have been trained in the policies governing such databases permitted access, and with every instance of access logged.

- SPD should not share any ALPR data with third parties without a written agreement ensuring that those third parties conform to the above retention and access rules, and should disclose to whom and under what circumstances the data are disclosed.

- Whenever a hit occurs, an officer, before taking any action, must confirm visually that a plate matches the number and state identified in the alert, confirm that the alert is still active by calling dispatch and, if the alert pertains to the registrant of the car and not the car itself, for example in a warrant situation, develop a reasonable belief that the vehicle's occupant(s) match any individual(s) identified in the alert.

- ALPRs should not be used for non-criminal enforcement purposes, other than parking enforcement.

- SPD should produce detailed records of ALPR scans, hits, and crimes solved specifically attributable to those hits, as well as an accounting of how ALPR use varies by neighborhood and demographic.

2. **Parking Enforcement Systems (Including ALPR)(SPD)**

Particularly given the partly merged nature of the parking enforcement and patrol ALPRs, including use of the parking enforcement ALPRs to check vehicle plates against hot lists, the concerns stated above with respect to SPD Patrol ALPRs apply equally to parking enforcement systems, and Council should ensure that the same minimum rules apply to them via ordinance—the intended primary use for parking enforcement does not in itself mitigate the concerns raised. In addition, the following outstanding questions should be answered in an updated SIR:

- It is unclear from the SIR how the Parking Enforcement ALPR systems integrate with the Patrol ALPR systems—it appears that some integration occurs at least in the case of the Scofflaw enforcement vans, that store collected data in the BOSS system. An updated ALPR should clarify specifically what rules apply to that data, and how they differ from rules applied to data collected by Patrol ALPR.

- A number of software and hardware providers are mentioned in Section 2.3 of the SIR—an updated SIR should clarify whether all contract directly with SPD itself, or with each other or a third party entity, to provide ALPR and related services.

- As with Patrol ALPR, statistics on numbers of scans, hits, and revenue from the systems would be helpful.

- Section 4.1 suggests pictures of the vehicle are being taken in addition to the plate—are these pictures stored, and if so, for how long?

- Concerns set forth in the section above relating to patrol ALPR regarding data access, clear standards for data sharing with third party entities and the purpose of such sharing, as well as auditing, all apply to these systems as well—and an updated SIR should clarify those standards.

3. **License Plate Readers (SDOT)**

The concerns stated above with respect to patrol ALPR largely apply to this set of ALPRs as well, with the additional concern of explicit sharing with a state entity. It is heartening that the SIR suggests that no license plate data is retained, but it is not clear whether that no-retention practice is reflected in policy. It is also unclear whether an explicit agreement exists with WSDOT ensuring deletion of the data and use only for the

purpose of calculating travel times. With that in mind, the following outstanding questions should be answered in an updated SIR:

- What explicit, written policies govern what SDOT and WSDOT can do with this ALPR data? Is there a written agreement with WSDOT requiring no personal data collection and deletion of all data?
- Under what circumstances might this data be used for law enforcement purposes? Is it possible for third parties to subpoena any data retained?
- What additional third parties get access to the data?

The Council should ensure by ordinance that the data collected is used only for the purpose of calculating travel times, that no data is retained, that no third party other than SDOT and WSDOT access the data at any time, and that a written agreement holds WSDOT to these restrictions.

II. Camera Group

Overall, concerns around this group of technologies largely focus on the use of these systems and the data collected by them for purposes other than those intended, over-collection and over-retention of data, and sharing of that data with third parties (such as federal law enforcement agencies). While the stated purposes of the cameras may be relatively innocuous, it is important to remember that images taken by such cameras, for example at emergency scenes, can compromise the privacy of individuals at vulnerable moments, and can be misused for the same kinds of targeting and profiling of particular communities detailed in Section I above. In addition, with the widespread and cheap availability of facial recognition technology, which can be applied after the fact to any image showing a face, it is all the more important that protections limiting the use of these tools to their intended purpose be enacted.

For all of these systems, the Council should adopt, via ordinance, clear and enforceable rules that ensure, at a minimum, the following:

- The purpose of camera use should be clearly defined, and its operation and data collected should be explicitly restricted to that purpose only.
- Data retention should be limited to the time needed to effectuate the purpose defined.
- Data sharing with third parties should be limited to those held to the same restrictions.
- Clear policies should govern operation, and all operators of the cameras should be trained in those policies.

Specific comments follow:

1. Emergency Scene Cameras (ESCs)(SFD)

The SIR for this technology states that no explicit internal policy exists at SFD that governs the use of ESCs, so a good start would be to create such a policy and include it in an updated SIR. This process should begin with an explicit list of specific uses for the ESCs, which are currently only set forth in general terms, and with apparent contradictions between sections of the SIR (for example, Section 1.0 describes three uses for the cameras, but Section 2.1 adds several more). In addition, the updated SIR should set forth any other internal internal policies and Washington laws governing use, retention, and disclosure of the data; where the data is stored; and which third parties, if any, have access to it, and for what purpose. (The SIR indicates data sharing with SPD, but the purpose is not clear.)

In turn, the Council should ensure via ordinance that no use is made of the images beyond the specific emergency, investigative, or training uses set forth, and that the data is deleted immediately upon completion of those purposes. Data sharing with third parties should be prohibited unless for those specific uses, and those third parties should be held to the same use and retention standards.

2. Hazardous Materials (Hazmat) Cameras (SFD)

As with ESCs, the SIR for Hazmat cameras indicates that no policy governing the use of this technology currently exists, with one limited exception for mechanism-of-injury recordings (see SIR Section 3.3). So similarly to ESCs, with this technology, an explicit policy that lists specific uses for the cameras should be created and included in an updated SIR. In addition, answers to questions such as who stores the data and which third parties have access to it should be made explicit. In particular, the SIR describes data sharing with law enforcement, but purposes of that disclosure are not made explicit (see SIR Section 4.7). In instances where a legal standard such as reasonable suspicion is applied, it should be clear what the standard is, who applies it, and how that application is documented. Overall, use of this technology should be limited to emergency response purposes, and any law enforcement use of the data should be restricted by ordinance.

3. Closed Circuit Television "Traffic Cameras" (SDOT)

As with the other two camera technologies, the crux of concern around these traffic cameras relates to limiting their use to specific purposes, enshrining in statute protections against invasion of privacy and general data collection, and limiting data sharing. It would be helpful to see the SDOT camera control guidelines referenced in the SIR, as well as to make clear in a policy applicable specifically to these cameras, what data will be deleted when (Section 5 appears to contain several different retention policies). Additional questions that an updated SIR should answer are as follows:

- The current SIR does not reference specific camera vendors and models—these would be helpful to have.

- Are there currently explicit guidelines on when recording occurs, and what's maintained? (See SIR Section 3.3 referencing recording for "compelling traffic operational needs"—the term is undefined.)

- Law enforcement use appears to be explicitly contemplated by the SIR, but the specific allowable uses are not defined—these should be made clear.

As with the other camera technologies, the Council should ensure clear purposes are defined in statute for these traffic cameras, that no use is made of the images for other purposes, that data is immediately deleted when the purpose is achieved, and that data sharing with third parties should be prohibited unless for those specific uses.

Thank you for your consideration, and we look forward to working with you on the process of ordinance implementation. Please feel free to contact me with questions or concerns.

Sincerely,

Shankar Narayan

cc: Seattle City Council and Executive

CASA LATINA
With Dignity and Opportunity

317 17TH AVENUE SOUTH, SEATTLE, WA 98144
TEL. 206.956.0779 FAX. 206.956.0780

October 29, 2018

My name is Marcos Martinez and I am the Executive Director at Casa Latina, a nonprofit organization based in Seattle that serves low income Latinx immigrant community through employment, education and community organizing.

The community that we serve at Casa Latina is particularly vulnerable to abuses by government agencies. Since the elections of 2016, our communities have been on edge due to the increased enforcement activities of agencies like ICE and Customs and Border Protection (CBP).

In addition, while government officials have pledged that the private information of individuals would be protected within agencies such as the State Department of Licensing, we have seen that those promises are not always borne out in reality. Breaches of community trust are very difficult to repair.

It is for these reasons that technologies such as the Automated License Plate Reader System cause concerns for our communities. The ACLU, in its comments on these technologies, has pointed out some major concerns regarding the policies that govern the use of the ALPR, including the lack of meaningful restrictions on the purposes for which ALPR data may be collected or used.

Limitations on data sharing are of particular concern, since this could affect immigrant community members who are subject to detention by immigration authorities but who are not the subject of any active criminal investigation by SPD. It's not clear that strong policies are in place to prohibit the sharing of data with ICE or CBP which would serve to aid those agencies in their efforts to detain immigrant community members.

Thank you for your consideration and I look forward to working with you to develop policies that protect the privacy of our most vulnerable communities.

Sincerely,

Marcos Martinez

www.casa-latina.org

DENSHŌ
The Japanese American Legacy Project

November 5, 2018

Dear Seattle IT:

I am writing to offer Densho's comments on the recently released Group 1 Surveillance Impact Reports (SIRs) under the Seattle Surveillance Ordinance review process. Densho is a community-based 501(c)(3) organization. For more than twenty years, we have been documenting the World War II incarceration of Japanese Americans to promote equity and social justice both in Seattle and across the country. The experiences of Japanese Americans are a somber lesson about the fragility of civil society in the face of intolerance and fear.

We have reason to cast a critical eye on infrastructure and systems created to monitor our citizenry. Some two decades before the beginning of WWII, the Japanese American community was targeted for mass surveillance in a coordinated effort involving the Federal Bureau of Investigation (FBI), the Office of Naval Intelligence (ONI), and the War Department's Military Intelligence Division, assisted by local law enforcement agencies. In the immediate aftermath of Pearl Harbor, US Census data was improperly used to develop exclusion area maps and lists of Japanese American citizens for registration. In the current political environment, we remember this history and are concerned about how a new breed of technologies may affect the rights of our friends and neighbors who belong to ethnic, religious and other vulnerable minority communities

These comments will cover the SIRs for the six Group 1 technologies in two primary sections. The first will address the Automated License Plate Reader (ALPR) sub-group, including SPD Patrol, Parking Enforcement, and SDOT. The second offers comments on the camera technology SIRs for SFD Emergency Scene Cameras, SFD Hazmat Cameras, SDOT Closed Circuit "Traffic Cameras"

Section 1: Automated License Plate Reader technologies

A. *General Concerns*

ALPR is a powerful technology that creates almost unprecedented abilities to surveil and track the movement of individuals across our city and region. It is already being utilized in ways that impact religious, ethnic and other minority communities. In the wake of the September 11 attacks, ALPR was used to monitor Muslim communities in New York, and more recently, US Immigration and Customs Enforcement has employed ALPR data through large aggregators such as Vigilant Solutions to target Latinx populations.

While ALPR is valuable to SPD (and SDOT) in their work, and – as discussed in the SIRs – there are generally benign and beneficial uses, the creation of a large pool of highly sensitive data presents a risk for misuse.

B. *SPD Patrol*

1416 South Jackson St. Seattle, WA 98144 Phone: 206 320.0095 Fax: 206 320.0098 www.densho.org

DENSHŌ
The Japanese American Legacy Project

1. Retention policy inconsistent with stated goals
   In the SIR, the primary goal of the ALPR program is stated as, "Property Recovery" – locating stolen vehicles, while the report cites, use, "[o]n occasion," of the stored data to assist criminal investigations, in particular, the location of Amber and Silver Alert subjects. If this is the case, this casts significant doubt on the need for a lengthy data retention period. The agency does not provide the analysis that led to the decision for the 90-day period anywhere in the SIR or, in response to questions during the public engagement meeting on October 30, 2018. This policy should be driven by careful consideration of the needs of the program, rather than

2. Third-party data sharing
   As stated in the SIR, data is shared with third-parties, including law enforcement and researchers, under a number of policies and inter-agency agreements. However, the criteria for permissible sharing is vague; these policies should be articulated in a clear, consistent and explicit fashion.
3. Lack of transparency and reporting
   Statistical data regarding the collection and use of the ALPR data should be made publicly available. The implementation of SPD's new RMS should include functionality for tracking and recording when ALPR data has been used in investigations and enforcement.
4. Governing policies
   Currently, the management and use of ALPR systems is guided principally by SPD Policy 16.170. SPD officials themselves admit that Policy 16.170 is inadequate and incomplete. ALPR is a novel, powerful technology that requires

C. *Parking Enforcement (SPD)*
   1. Co-mingling of Parking Enforcement and Patrol data
      The SIR describes the flow of data from the Scofflaw "boot vans" to the centralized Neology BOSS system, shared with Patrol. It is not clear whether this data is aggregated directly with the Patrol dataset. If so, this should be more explicitly stated, and the same policies and rules should apply.

D. *SDOT*
   1. Sharing of data with WSDOT and other third parties
      The SIR does not outline whether the data-sharing agreement with WSDOT includes provisions governing the sharing and use of SDOT-collected data.

Section 2: Camera technologies

The use of image and video technologies has obvious benefits in the efficiency and delivery of emergency services in crisis situations, as was articulated in the each of the SIRs covering this group. Densho's primary concern is the possibility that the infrastructure and the data collected may be subject to uses beyond the scope of the stated purposes. While it is highly unlikely that

1416 South Jackson St. Seattle, WA 98144 Phone: 206 320.0095 Fax: 206 320.0098 www.densho.org

DENSHŌ
The Japanese American Legacy Project

SFD and SDOT would utilize the systems in ways that directly impact privacy, unless the collection, retention and sharing of data is carefully regulated, there is potential for real harm to civil liberties in the hands of third parties. Coupled with facial recognition technology, camera data can be used in ways that SFD and SDOT may not have anticipated.

We appreciate the opportunity to share these concerns with you, and hope that this process may help to make our city a welcoming, safe and truly civil society.

Sincerely,

Geoff Froh
Deputy Director

1416 South Jackson St. Seattle, WA 98144 Phone: 206 320.0095 Fax: 206 320.0098 www.densho.org

APPENDIX G: EMAILS & LETTERS FROM THE PUBLIC

Letter submitted by individual constituent.

Surveillance.
I don't want it.
Any of it.
Just stop.

Letter submitted by individual constituent:

Kevin Orme
502 N 80th
Seattle, WA 98103
206-789-3891

November 4, 2018

Public Input Commentary – Seattle Surveillance Technology open Public Comment period – 10/22 through 11/5, 2018.

Opening Remarks:

1. Surveillance technology usage in the United States of America, regardless of use, purpose and policy, is completely and wholly within the basic tenets of the Bill of Rights, otherwise known as Amendments 1-10 to the US Constitution. There are no more fundamental laws in the United States than the Constitution and the amendments thereto.

As regards privacy, public surveillance/data capture technology and police oversight – these governing principles have to be considered in any and all policies and local procedures/laws created for our democratic society. Doing anything less is simply illegal and against our whole theory of government – it's that simple.

Specifically:

The First Amendment, including rights to freedom of speech, public assembly and the press.

The Fourth Amendment, including rights preventing unreasonable search, seizure and requiring warrants for same.

The Fifth Amendment, including rights against self-incrimination and deprivation of life, liberty and property without due process.

The Sixth Amendment, including the right to confront the accuser by the accused; defense counsel when accused of a crime and proper/complete informing of the accused concerning the nature and extent of criminal accusation if occurs.

And beyond the Bill of Rights, **the 14th Amendment, Section 1**, regarding rights of due process and federal laws also applying equally to the states (which means *cities* in those same states, of course)

2) The WA State Constitution:

In addition to the Bill of Rights and the US Constitution, the WA State Constitution is also instructive:

Article 1, Section 1 – all political power is inherent in the people, and governments …..are established to protect and maintain individual rights;

Article 1, Section 2 – the US Constitution is the supreme law of the land;

Article 1, Section 7 - Invasion of Private Affairs or Home Prohibited

Article 1, Section 32- "A frequent recurrence to fundamental principles is essential to the security of individual right and the perpetuity of free government."

3) Context for Seattle: The above means essentially:

You cannot simply 'surveil everything' in the hopes of finding a criminal (or even worse, someone you simply "don't agree with"). That is called 'guilty until proven innocent' and has been overturned time and time again in our system of laws by courts and legislators at every level. The Bill of Rights has protected the 4th Amendment concept of 'Innocent until Proven Guilty' and 24-7 surveillance of **any** sort flies in the face and openly defies this most basic law.

You cannot 'surveil' public assemblies, protests, or similar gatherings, most especially with facial recognition, phone network/bluetooth data capture or public video recordings and/or microphones without again, violating the above basic constitutional principles – otherwise known as "laws" (US and WA).

You cannot store data simply according to 'policy', or come up with what you believe adequate controls may or may not be, and then implement them without complete transparency and public input, including that of the City Attorney's office, elected officials and arguably most important, THE PUBLIC. I believe this effort you have begun to solicit feedback is a good start, but there's a long way to go and this is only the very beginning, rest assured.

Finally, you cannot pay lip service to these previous paragraphs by not actively doing them yourself, and then simply turn around and receive/use/retain the data anyway through other means – that is, you cannot obtain the data from the NSA's Fusion Center already located in downtown Seattle, or the FBI, or TSA, DHS, or increasingly rogue agencies like ICE – all of these still break the law, plain and simple.

Specific technologies being discussed in this public outreach:

1) SDOT LPR's.

Positive – the data is stated as being deleted immediately after a transit time calculation;
Positive – the data is stated as only being available to SDOT personnel after relay from WSDOT, with individual identifying license plates not part of that incoming data;
Positive – stated purpose – facilitate effective and efficient traffic management within the Seattle city limits.

SDOT LPR's - COMMENT for Submission/consideration:

a) It is unclear how long WSDOT is retaining this data for handoff to SDOT and Seattle generally – even if SDOT deletes it nearly immediately after a calculation/use, can they go back and re-retrieve it later? The answer should be NO, and simply that WSDOT is doing the same thing at minimum – deleting the data almost immediately after said calculation too (I recognize this latter is beyond SDOT's control, however, certainly as the biggest city in the state, Seattle would have major influence on these policies and procedures were you to weigh in and state clear policy positions).

b) It is also unclear what the statement 'travel time calculation' precisely means for these purposes. Is it just me driving through downtown and getting spotted if I go by any of these cameras/devices? Assuming the answer is yes, when is the 'timeout' – 1 minute if not seen by another camera? 5 minutes? When and how quickly does the 'calculation' occur (so that I know purportedly the data is then "immediately deleted" as you say?

c) It is also unclear if anyone else working for the City of Seattle has access to this WSDOT data (and if so, for how long, in what capacity, at what level of detail, etc.) – say, the SPD, City Attorney's office, or? So maybe SDOT isn't "surveilling" anyone within the normal meaning of the term given the safeguards noted in the policy PDF, but certainly the SPD have far different reasons for using this data, and most (if not all) of them are far removed from simple data calculations, and include direct data review to carry out those tasks?

Traffic Cameras (SDOT)

Positive – similar purposes to those above – namely efficient and effective traffic mgmt in real time, using systems and human operators (either in a data center or on the scene, e.g. tow truck, etc.) to make it happen.

SDOT Traffic Cams - COMMENT for Submission/consideration:

a) What are the 'SDOT Camera Control Protocol Guidelines' and are they public? If not, can they be and where can we review them? Have they ever been amended due to public input, potential past problems or abuses? When were they written and by whom with what expertise?

b) What are the 'specific cases' where footage is archived and for how long?

c) Has this data ever been subpoena'd by City personnel, or outside entities (e.g. ICE, NSA or similar)?

d) The 'protections' paragraph says archived footage isn't shared with any other City dept – but what about data that is 'in transit' between realtime capture and potential archiving later (whether only for 10 days or not)? How/when and in what circumstances might footage be temporarily retained or shared outside normal policy, and potentially 'evade' the otherwise typical 10-day delete policy as a result?

SPD – ALPR's

Positive – as stated by SPD with any such whiz-bang tech – 'preventing crime' ***SPD ALPR's: COMMENT***

for Submission/consideration:

a) Why 90 days? Why not something much more reasonable, like 15? Certainlyif the tech is sophisticated enough to create a 'hot list' as described here, **15 days – two working weeks in other words – is surely more than enough time for the data's intended purpose.**

b) Can we see examples of these 'auditable records' supposedly created by SPD when logging into ALPR/contacting dispatch? If you are making them 'auditable' for the purposes of ensuring restricted and limited use of the technology generally, then surely you don't mind if we see how that works at minimum so WE can know this (and believe you) too?

c) When does something become an 'active investigation' – and how long is the data retained, where stored and accessible by who then? What if the investigation is called off or invalidated by a court or city officer/city attorney – is the data immediately deleted, and an 'auditable record' of that activity created to prove it?

d) You say nothing about sharing the data with other entities (e.g. ICE, DHS, etc.) - do you? Are you planning to? Have you done so in the past? If so on any of these, under what circumstances and did they provide any sort of a warrant of any kind?

e) You stated there are eight SPD cars equipped with ALPR systems now, and that statement implies that this is the 'only' such ALPR system deployed 1) for these purposes, 2) with this specific technology citywide. Is this true? Are there stationary systems mounted elsewhere in the city that are networked (now or can be in the future) and if so, how many are there? Are there plans (either already in motion or for say, the next few years) to implement either more cars, add in stationary systems, or both? Certainly at minimum, just like with red light cameras, we deserve and demand publicly posted notice of any such stationary systems if they exist or are being deployed.

f) I have read the online 16.170-POL governing ALPR use http://www.seattle.gov/police-manual/title-16---patrol-operations/16170--automatic-license-plate-readers – and it's pretty sparse with only 4 short bullet points.
– more questions:

f1) what is ACCESS certification and how can we know more that it does what it's intended to do? Where is the training, who does it, is it a private entity creating coursework, etc.?

f2) how often are these standards updated (e.g. the policy is already 6 years old, dating from 2012 – certainly the technology is not falling behind in the same way);

f3) Who is in charge of TESU and what are their qualifications? Are they elected officials or behind the scenes?

f4) does the terminology 'part of an active investigation' = 'we got a hit on a license plate of X' – and X is a known criminal, there's a warrant out, or? Need way more information here, this is far too vague and un-specific when regards data management and control. I could be the most qualified TESU guy in the department and yet it doesn't mean I should be entitled to look at *any* data – especially without a legal warrant to do so? Where are the other controlling provisions?

Emergency Scene Cameras

Positive – improve and continue to enhance emergency preparedness and response effectiveness.

Emergency Cams: COMMENT for Submission/consideration:

a) where are the 'internal policies' and 'WA laws' governing storage of said photos and materials? The PDF is pretty vague.
b) Is live footage/drone image, sound and data capture being considered or already being used? As to data captured (audio, video, photo), storage management, retention and access policies – the Details, Please.
c) what about the same (live footage/audio/video) from vehicles or bodycams/etc.? Again, Details please.

Hazmat Cameras

Positive – largely identical to that of Emergency Incident Response, save the potential for nefarious/negligent actors to be involved

Hazmat Cams: COMMENT for Submission/consideration:

a) similar to with Emergency Cameras – essentially how long is the data stored, especially if no criminal activity is determined or the investigation concludes

b) anything beyond tablets used or planned to be used? This mentions tablets as the primary tech, but that doesn't foreclose plans for more (or by aggressive tech vendors already talking to you)?

c) what sort of data management training is provided to either HazMat or Emergency Responders, for that matter?

Parking Enforcement (SPD)

Positive – enforce parking and related laws, determine 'booting' situations ***SPD Parking Enforcement: COMMENT for Submission/consideration:***

a) there is nothing seen here about general data storage or retention parameters – Details, Please.

b) there is nothing here about whether this ALPR data is 'pooled' with ALPR datacollected from the eight so-equipped SPD cars mentioned earlier – and if so, whether governed by those parameters and restrictions too/not? Details, Please.

c) are these technologies governed by TESU as the others are? Barring possibly those controlled directly by the Seattle Municipal Court itself, separate from the SPD? Details, Please.

d) there is also no mention of the (likely older) Red Light Traffic Cam technology that has been in use in city locations for some years now, possibly over a decade. These aren't for SDOT use, these are for people running red lights, of course. All the relevant details (Data capture, retention, storage, access, certification, etc.) - all these apply here too – Details, Please.

Submitted 11/4/2018 by

Kevin Orme
502 N 80th
Seattle, WA 98103
206-789-3891

APPENDIX H: PUBLIC COMMENT ANALYSIS METHODOLOGY

OVERVIEW

The approach to comment analysis includes combination of qualitative and quantitative methods. A basic qualitative text analysis of the comments received, and a subsequent comparative analysis of results, were validated against quantitative results. Each comment was analyzed in the following ways, to observe trends and confirm conclusions:

1. Analyzed collectively, as a whole, with all other comments received
2. Analyzed by technology
3. Analyzed by technology and question

A summary of findings are included in Appendix B: Public Comment Demographics and Analysis. All comments received are included in Appendix E: All Individual Comments Received.

BACKGROUND ON METHODOLOGICAL FRAMEWORK

A modified Framework Methodology was used for qualitative analysis of the comments received, which "*…approaches [that] identify commonalities and differences in qualitative data, before focusing on relationships between different parts of the data, thereby seeking to draw descriptive and/or explanatory conclusions clustered around themes" (Gale, N.K., et.al, 2013).* Framework Methodology is a coding process which includes both inductive and deductive approaches to qualitative analysis.

The goal is to classify the subject data so that it can be meaningfully compared with other elements of the data and help inform decision-making. Framework Methodology is "not designed to be representative of a wider population, but purposive to capture diversity around a phenomenon" (*Gale, N.K., et.al, 2013).*

METHODOLOGY

STEP ONE: PREPARE DATA

1. Compile data received.
    I. Daily collection and maintenance of 2 primary datasets.
        A. Master dataset: a record of all raw comments received, questions generated at public meetings, and demographic information collected from all methods of submission.
        B. Comment analysis dataset: the dataset used for comment analysis that contains coded data and the qualitative codebook. The codebook contains the qualitative codes used for analysis and their definitions.
2. Clean the compiled data.
    I. Ensure data is as consistent and complete as possible. Remove special characters for machine readability and analysis.
    II. Comments submitted through SurveyMonkey for "General Surveillance" remained in the "General Surveillance" category for the analysis, regardless of content of the comment. Comments on surveillance generally, generated at public meetings, were categorized as such.
    III. Filter data by technology for inclusion in individual SIRs.

STEP TWO: CONDUCT QUALITATIVE ANALYSIS USING FRAMEWORK METHODOLOGY

1. Become familiar with the structure and content of the data. This occurred daily compilation and cleaning of the data in step one.
2. Individually and collaboratively code the comments received, and identify emergent themes.
    I. Begin with deductive coding by developing pre-defined codes derived from the prescribed survey and small group facilitator questions and responses.
    II. Use clean data, as outlined in Data Cleaning section above, to inductively code comments.
        A. Each coder individually reviews the comments and independently codes them.
        B. Coders compare and discuss codes, subcodes, and broad themes that emerge.
        C. Qualitative codes are added as a new field (or series of fields) into the Comments dataset to derive greater insight into themes, and provide increased opportunity for visualizing findings.
    III. Develop the analytical framework.
        A. Coders discuss codes, sub-codes, and broad themes that emerge, until codes are agreed upon by all parties.
        B. Codes are grouped into larger categories or themes.
        C. The codes are be documented and defined in the codebook.
    IV. Apply the framework to code the remainder of the comments received.
    V. Interpret the data by identifying differences and map relationships between codes and themes, using R and Tableau.

STEP THREE: CONDUCT QUANTITATIVE ANALYSIS

1. Identify frequency of qualitative codes for each technology overall, by questions, or by themes:
    I. Analyze results for single word codes.
    II. Analyze results for word pair codes (for context).
2. Identify the most commonly used words and word pairs (most common and least common) for all comments received.
    I. Compare results with qualitative code frequencies and use to validate codes.
    II. Create network graph to identify relationships and frequencies between words used in comments submitted. Use this graph to validate analysis and themes.
3. Extract CSVs of single word codes, word pair codes, and word pairs in text of the comments, as well as the corresponding frequencies for generating visualizations in Tableau.

STEP FOUR: SUMMARIZATION

1. Visualize themes and codes in Tableau. Use call out quotes to provide context and tone.
2. Included summary information and analysis in the appendices of each SIR.

APPENDIX I: POLICIES AND PROCEDURES GOVERNING ALPR

City of Seattle
Mayor Jenny A. Durkan

MAYORAL DIRECTIVE

Date: February 6, 2018

To: City of Seattle Department Directors

From: Mayor Jenny A. Durkan

Subject: City of Seattle Protocol on Federal Immigration Enforcement

---

Background on Seattle as a Welcoming City

We have pledged to be a Welcoming City that protects all residents. This is not only the morally right thing to do, it is essential to a fundamental City duty. The City has a duty to protect the public safety of all of its residents. Confidence and trust in law enforcement is critical to this duty. Such confidence and trust supports essential functions of law enforcement including reporting of crimes to officers, participation of witnesses in investigations, and enhancing respect for law enforcement in our communities. This support for the essential work of law enforcement makes everyone in a community safer.

Many people do not distinguish the various types and roles of law enforcement. Positive and negative interactions with any law enforcement can adhere to all law enforcement. Recent actions and pronouncements by federal authorities, particularly by Federal Immigration and Customs Enforcement (ICE), undermine the trust and confidence essential to law enforcement. Many residents, regardless of their immigration status, may be unwilling to report crimes or participate in investigations because of concerns about potential impacts on others in their families or communities. This erodes and undermines the community trust that is essential for the City to provide public safety.

To bolster and maintain the trust needed for public safety, all residents must know we will take the steps necessary to protect them. Recent reports regarding lapses by government, including by the Washington State Department of Licensing, show we must have robust protocols for all City departments.

As discussed below, we will be assessing all Departments to determine what information is collected and distributed, whether that information is necessary to collect, and the need for individual departmental protocols. Until such assessment is completed the following will be effective immediately:

To further Seattle as a Welcoming City for all residents, including immigrant and refugee residents and workers, City department directors are hereby directed to refer all requests from ICE authorities to the Mayor's Office Legal Counsel, including:

Office of the Mayor | 600 Fourth Avenue, P.O. Box 94749, Seattle, WA 98124 | 206-684-4000 | seattle.gov/mayor

- Access to non-public areas in City buildings and venues (i.e., areas not open to the public such as staff work areas that require card key access and other areas designated as "private" or "employee only");
- Actions seeking data or information (written or oral) about City employees, residents or workers.

In all cases, City employees are directed to ask ICE agents to wait to enter any non-public areas until the Mayor's Office Legal Counsel is contacted at (206) 471-0664. Counsel will review credentials, submission of written authority to conduct action, and determine whether to grant approval of access.

These protocols will work in conjunction with existing City ordinance and policy:

- **City employees are prohibited from asking about immigration status**. Often referred to as the City's "don't ask" law, Seattle Ordinance 121063, passed in 2003, instructs all City employees to refrain from inquiring about the immigration status of any person except police officers where officers have a reasonable suspicion that a person 1) has previously been deported from the United States; (2) is again present in the United States; and (3) is committing or has committed a felony criminal-law violation.

- **City employees will serve all residents and city services will be accessible to all residents, regardless of immigration status.** Seattle Resolution 31730, passed in 2017, reaffirms Ordinance 121063 and states that city agencies and law enforcement cannot withhold services based on ancestry, race, ethnicity, national origin, color, age, sex, sexual orientation, gender identity, marital status, physical or mental disability, religion, or immigration status. See, also, Seattle Resolution 30672, passed in 2004.

Assessment of City Systems

All City department directors will participate in an assessment of City policies and practices – including but not limited to employment, law enforcement, public safety, IT, and social service delivery. The purpose of the assessment is to assess City compliance with Seattle Municipal Code 4.18.15, and to gain a better understanding what information is collected by the City, whether collecting that information is necessary, and how the City's work interacts with federal immigration enforcement.

All department directors shall identify a department lead to assist in this assessment by February 13, 2018.

City Contractors

City departments will issue a letter to all contractors receiving General Fund dollars to clarify and inform about the protocols described above. A communication will be issued by City departments to their contractors by March 6, 2018.

County Policy

As a reminder, jails are in King County's jurisdiction and enforcing civil federal immigration violations are in the purview of the U.S. Department of Homeland Security, City department directors are reminded to comply with the City's policy to defer to King County on ICE detainer requests.

- **City employees will refer detainer requests from the U.S. Department of Homeland Security's Immigration and Customs Enforcement (ICE) to King County.** King County Ordinance 17886 passed in 2014 clarifies that the County will not honor ICE requests for notification or detention, unless accompanied by a judicial warrant.

Directive for Implementation

To achieve full Department participation in ensuring that responses to ICE requests are consistent with Seattle Ordinance 121063 and to assess departmental compliance with Seattle Ordinance 121063, I request all Departments identify a lead to the Mayor's Office by February 13, 2018.

Contact for Further Information

Thank you for your cooperation. If you have any questions, please contact Mayor's Office Legal Counsel, Ian Warner (206) 471.0664.

(3) Inserted in any envelope and/or publication the contents of which may be construed to be inappropriate for association with the Missing Children Penalty Mail Program.

(e) Each component shall provide the General Services Staff, Justice Management Division, with the name(s), telephone number(s) and mailing address(es) of each designated Missing Children Program Coordinator within 30 days of the effective date of this regulation.

(f) Each component shall submit a quarterly report to the General Services Staff, Justice Management Division, within 5 days after the close of each Fiscal Year quarter providing the specific information identified in § 19.5 concerning implementation and participation in the program.

PART 20—CRIMINAL JUSTICE INFORMATION SYSTEMS

Subpart A—General Provisions

Sec.
20.1 Purpose.
20.2 Authority.
20.3 Definitions.

Subpart B—State and Local Criminal History Record Information Systems

20.20 Applicability.
20.21 Preparation and submission of a Criminal History Record Information Plan.
20.22 Certification of compliance.
20.23 Documentation: Approval by OJARS.
20.24 State laws on privacy and security.
20.25 Penalties.

Subpart C—Federal Systems and Exchange of Criminal History Record Information

20.30 Applicability.
20.31 Responsibilities.
20.32 Includable offenses.
20.33 Dissemination of criminal history record information.
20.34 Individual's right to access criminal history record information.
20.35 Criminal Justice Information Services Advisory Policy Board.
20.36 Participation in the Interstate Identification Index System.
20.37 Responsibility for accuracy, completeness, currency, and integrity.
20.38 Sanction for noncompliance.

APPENDIX TO PART 20—COMMENTARY ON SELECTED SECTIONS OF THE REGULATIONS ON CRIMINAL HISTORY RECORD INFORMATION SYSTEMS

AUTHORITY: 28 U.S.C. 534; Pub. L. 92–544, 86 Stat. 1115; 42 U.S.C. 3711, *et seq.*, Pub. L. 99–169, 99 Stat. 1002, 1008–1011, as amended by Pub. L. 99–569, 100 Stat. 3190, 3196; Pub. L. 101–515, as amended by Pub. L. 104–99, set out in the notes to 28 U.S.C. 534.

SOURCE: Order No. 601–75, 40 FR 22114, May 20, 1975, unless otherwise noted.

Subpart A—General Provisions

SOURCE: 41 FR 11714, Mar. 19, 1976, unless otherwise noted.

§ 20.1 Purpose.

It is the purpose of these regulations to assure that criminal history record information wherever it appears is collected, stored, and disseminated in a manner to ensure the accuracy, completeness, currency, integrity, and security of such information and to protect individual privacy.

[Order No. 2258–99, 64 FR 52226, Sept. 28, 1999]

§ 20.2 Authority.

These regulations are issued pursuant to sections 501 and 524(b) of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Crime Control Act of 1973, Public Law 93–83, 87 Stat. 197, 42 U.S.C. 3701, *et seq.* (Act), 28 U.S.C. 534, and Public Law 92–544, 86 Stat. 1115.

§ 20.3 Definitions.

As used in these regulations:

(a) *Act* means the Omnibus Crime Control and Safe Streets Act, 42 U.S.C. 3701, *et seq.*, as amended.

(b) *Administration of criminal justice* means performance of any of the following activities: Detection, apprehension, detention, pretrial release, posttrial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal history record information.

(c) *Control Terminal Agency* means a duly authorized state, foreign, or international criminal justice agency with

direct access to the National Crime Information Center telecommunications network providing statewide (or equivalent) service to its criminal justice users with respect to the various systems managed by the FBI CJIS Division.

(d) *Criminal history record information* means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system.

(e) *Criminal history record information system* means a system including the equipment, facilities, procedures, agreements, and organizations thereof, for the collection, processing, preservation, or dissemination of criminal history record information.

(f) *Criminal history record repository* means the state agency designated by the governor or other appropriate executive official or the legislature to perform centralized recordkeeping functions for criminal history records and services in the state.

(g) *Criminal justice agency* means:

(1) Courts; and

(2) A governmental agency or any subunit thereof that performs the administration of criminal justice pursuant to a statute or executive order, and that allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspector General Offices are included.

(h) *Direct access* means having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of or intervention by any other party or agency.

(i) *Disposition* means information disclosing that criminal proceedings have been concluded and the nature of the termination, including information disclosing that the police have elected not to refer a matter to a prosecutor or that a prosecutor has elected not to commence criminal proceedings; or disclosing that proceedings have been indefinitely postponed and the reason for such postponement. Dispositions shall include, but shall not be limited to, acquittal, acquittal by reason of insanity, acquittal by reason of mental incompetence, case continued without finding, charge dismissed, charge dismissed due to insanity, charge dismissed due to mental incompetency, charge still pending due to insanity, charge still pending due to mental incompetence, guilty plea, nolle prosequi, no paper, nolo contendere plea, convicted, youthful offender determination, deceased, deferred disposition, dismissed-civil action, found insane, found mentally incompetent, pardoned, probation before conviction, sentence commuted, adjudication withheld, mistrial-defendant discharged, executive clemency, placed on probation, paroled, or released from correctional supervision.

(j) *Executive order* means an order of the President of the United States or the Chief Executive of a state that has the force of law and that is published in a manner permitting regular public access.

(k) *Federal Service Coordinator* means a non-Control Terminal Agency that has a direct telecommunications line to the National Crime Information Center network.

(l) *Fingerprint Identification Records System* or "FIRS" means the following FBI records: Criminal fingerprints and/or related criminal justice information submitted by authorized agencies having criminal justice responsibilities; civil fingerprints submitted by federal agencies and civil fingerprints submitted by persons desiring to have their fingerprints placed on record for personal identification purposes; identification records, sometimes referred to as "rap sheets," which are compilations of criminal history record information pertaining to individuals who have criminal fingerprints maintained in the FIRS; and a name index pertaining to all individuals whose fingerprints are maintained in the FIRS. See the FIRS Privacy Act System Notice periodically published in the FEDERAL REGISTER for further details.

(m) *Interstate Identification Index System* or "III System" means the cooperative federal-state system for the exchange of criminal history records, and includes the National Identification Index, the National Fingerprint File, and, to the extent of their participation in such system, the criminal history record repositories of the states and the FBI.

(n) *National Crime Information Center* or "NCIC" means the computerized information system, which includes telecommunications lines and any message switching facilities that are authorized by law, regulation, or policy approved by the Attorney General of the United States to link local, state, tribal, federal, foreign, and international criminal justice agencies for the purpose of exchanging NCIC related information. The NCIC includes, but is not limited to, information in the III System. See the NCIC Privacy Act System Notice periodically published in the FEDERAL REGISTER for further details.

(o) *National Fingerprint File* or "NFF" means a database of fingerprints, or other uniquely personal identifying information, relating to an arrested or charged individual maintained by the FBI to provide positive identification of record subjects indexed in the III System.

(p) *National Identification Index* or "NII" means an index maintained by the FBI consisting of names, identifying numbers, and other descriptive information relating to record subjects about whom there are criminal history records in the III System.

(q) *Nonconviction data* means arrest information without disposition if an interval of one year has elapsed from the date of arrest and no active prosecution of the charge is pending; information disclosing that the police have elected not to refer a matter to a prosecutor, that a prosecutor has elected not to commence criminal proceedings, or that proceedings have been indefinitely postponed; and information that there has been an acquittal or a dismissal.

(r) *State* means any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

(s) *Statute* means an Act of Congress or of a state legislature or a provision of the Constitution of the United States or of a state.

[Order No. 2258–99, 64 FR 52226, Sept. 28, 1999]

Subpart B—State and Local Criminal History Record Information Systems

SOURCE: 41 FR 11715, Mar. 19, 1976, unless otherwise noted.

§ 20.20 Applicability.

(a) The regulations in this subpart apply to all State and local agencies and individuals collecting, storing, or disseminating criminal history record information processed by manual or automated operations where such collection, storage, or dissemination has been funded in whole or in part with funds made available by the Law Enforcement Assistance Administration subsequent to July 1, 1973, pursuant to title I of the Act. Use of information obtained from the FBI Identification Division or the FBI/NCIC system shall also be subject to limitations contained in subpart C.

(b) The regulations in this subpart shall not apply to criminal history record information contained in:

(1) Posters, announcements, or lists for identifying or apprehending fugitives or wanted persons;

(2) Original records of entry such as police blotters maintained by criminal justice agencies, compiled chronologically and required by law or long standing custom to be made public, if such records are organized on a chronological basis;

(3) Court records of public judicial proceedings;

(4) Published court or administrative opinions or public judicial, administrative or legislative proceedings;

(5) Records of traffic offenses maintained by State departments of transportation, motor vehicles or the equivalent thereof for the purpose of regulating the issuance, suspension, revocation, or renewal of driver's, pilot's or other operators' licenses;

(6) Announcements of executive clemency.

(c) Nothing in these regulations prevents a criminal justice agency from disclosing to the public criminal history record information related to the offense for which an individual is currently within the criminal justice system. Nor is a criminal justice agency prohibited from confirming prior criminal history record information to members of the news media or any other person, upon specific inquiry as to whether a named individual was arrested, detained, indicted, or whether an information or other formal charge was filed, on a specified date, if the arrest record information or criminal record information disclosed is based on data excluded by paragraph (b) of this section. The regulations do not prohibit the dissemination of criminal history record information for purposes of international travel, such as issuing visas and granting of citizenship.

§20.21 Preparation and submission of a Criminal History Record Information Plan.

A plan shall be submitted to OJARS by each State on March 16, 1976, to set forth all operational procedures, except those portions relating to dissemination and security. A supplemental plan covering these portions shall be submitted no later than 90 days after promulgation of these amended regulations. The plan shall set forth operational procedures to—

(a) *Completeness and accuracy.* Insure that criminal history record information is complete and accurate.

(1) Complete records should be maintained at a central State repository. To be complete, a record maintained at a central State repository which contains information that an individual has been arrested, and which is available for dissemination, must contain information of any dispositions occurring within the State within 90 days after the disposition has occurred. The above shall apply to all arrests occurring subsequent to the effective date of these regulations. Procedures shall be established for criminal justice agencies to query the central repository prior to dissemination of any criminal history record information unless it can be assured that the most up-to-date disposition data is being used. Inquiries of a central State repository shall be made prior to any dissemination except in those cases where time is of the essence and the repository is technically incapable of responding within the necessary time period.

(2) To be accurate means that no record containing criminal history record information shall contain erroneous information. To accomplish this end, criminal justice agencies shall institute a process of data collection, entry, storage, and systematic audit that will minimize the possibility of recording and storing inaccurate information and upon finding inaccurate information of a material nature, shall notify all criminal justice agencies known to have received such information.

(b) *Limitations on dissemination.* Insure that dissemination of nonconviction data has been limited, whether directly or through any intermediary only to:

(1) Criminal justice agencies, for purposes of the administration of criminal justice and criminal justice agency employment;

(2) Individuals and agencies for any purpose authorized by statute, ordinance, executive order, or court rule, decision, or order, as construed by appropriate State or local officials or agencies;

(3) Individuals and agencies pursuant to a specific agreement with a criminal justice agency to provide services required for the administration of criminal justice pursuant to that agreement. The agreement shall specifically authorize access to data, limit the use of data to purposes for which given, insure the security and confidentiality of the data consistent with these regulations, and provide sanctions for violation thereof;

(4) Individuals and agencies for the express purpose of research, evaluative, or statistical activities pursuant to an agreement with a criminal justice agency. The agreement shall specifically authorize access to data, limit the use of data to research, evaluative, or statistical purposes, insure the confidentiality and security of the data consistent with these regulations and with section 524(a) of the Act and any regulations implementing section

524(a), and provide sanctions for the violation thereof. These dissemination limitations do not apply to conviction data.

(c) *General policies on use and dissemination.* (1) Use of criminal history record information disseminated to noncriminal justice agencies shall be limited to the purpose for which it was given.

(2) No agency or individual shall confirm the existence or nonexistence of criminal history record information to any person or agency that would not be eligible to receive the information itself.

(3) Subsection (b) does not mandate dissemination of criminal history record information to any agency or individual. States and local governments will determine the purposes for which dissemination of criminal history record information is authorized by State law, executive order, local ordinance, court rule, decision or order.

(d) *Juvenile records.* Insure that dissemination of records concerning proceedings relating to the adjudication of a juvenile as delinquent or in need or supervision (or the equivalent) to noncriminal justice agencies is prohibited, unless a statute, court order, rule or court decision specifically authorizes dissemination of juvenile records, except to the same extent as criminal history records may be disseminated as provided in paragraph (b) (3) and (4) of this section.

(e) *Audit.* Insure that annual audits of a representative sample of State and local criminal justice agencies chosen on a random basis shall be conducted by the State to verify adherence to these regulations and that appropriate records shall be retained to facilitate such audits. Such records shall include, but are not limited to, the names of all persons or agencies to whom information is disseminated and the date upon which such information is disseminated. The reporting of a criminal justice transaction to a State, local or Federal repository is not a dissemination of information.

(f) *Security.* Wherever criminal history record information is collected, stored, or disseminated, each State shall insure that the following requirements are satisfied by security standards established by State legislation, or in the absence of such legislation, by regulations approved or issued by the Governor of the State.

(1) Where computerized data processing is employed, effective and technologically advanced software and hardware designs are instituted to prevent unauthorized access to such information.

(2) Access to criminal history record information system facilities, systems operating environments, data file contents whether while in use or when stored in a media library, and system documentation is restricted to authorized organizations and personnel.

(3)(i) Computer operations, whether dedicated or shared, which support criminal justice information systems, operate in accordance with procedures developed or approved by the participating criminal justice agencies that assure that:

(*a*) Criminal history record information is stored by the computer in such manner that it cannot be modified, destroyed, accessed, changed, purged, or overlaid in any fashion by non-criminal justice terminals.

(*b*) Operation programs are used that will prohibit inquiry, record updates, or destruction of records, from any terminal other than criminal justice system terminals which are so designated.

(*c*) The destruction of records is limited to designated terminals under the direct control of the criminal justice agency responsible for creating or storing the criminal history record information.

(*d*) Operational programs are used to detect and store for the output of designated criminal justice agency employees all unauthorized attempts to penetrate any criminal history record information system, program or file.

(*e*) The programs specified in paragraphs (f)(3)(i) (*b*) and (*d*) of this section are known only to criminal justice agency employees responsible for criminal history record information system control or individuals and agencies pursuant to a specific agreement with the criminal justice agency to provide such programs and the program(s) are kept continuously under maximum security conditions.

(*f*) Procedures are instituted to assure that an individual or agency authorized direct access is responsible for (*1*) the physical security of criminal history record information under its control or in its custody and (*2*) the protection of such information from unauthorized access, disclosure or dissemination.

(*g*) Procedures are instituted to protect any central repository of criminal history record information from unauthorized access, theft, sabotage, fire, flood, wind, or other natural or manmade disasters.

(ii) A criminal justice agency shall have the right to audit, monitor and inspect procedures established above.

(4) The criminal justice agency will:

(i) Screen and have the right to reject for employment, based on good cause, all personnel to be authorized to have direct access to criminal history record information.

(ii) Have the right to initiate or cause to be initiated administrative action leading to the transfer or removal of personnel authorized to have direct access to such information where such personnel violate the provisions of these regulations or other security requirements established for the collection, storage, or dissemination of criminal history record information.

(iii) Institute procedures, where computer processing is not utilized, to assure that an individual or agency authorized direct access is responsible for

(*a*) The physical security of criminal history record information under its control or in its custody and

(*b*) The protection of such information from unauthorized access, disclosure, or dissemination.

(iv) Institute procedures, where computer processing is not utilized, to protect any central repository of criminal history record information from unauthorized access, theft, sabotage, fire, flood, wind, or other natural or manmade disasters.

(v) Provide that direct access to criminal history record information shall be available only to authorized officers or employees of a criminal justice agency and, as necessary, other authorized personnel essential to the proper operation of the criminal history record information system.

(5) Each employee working with or having access to criminal history record information shall be made familiar with the substance and intent of these regulations.

(g) *Access and review*. Insure the individual's right to access and review of criminal history information for purposes of accuracy and completeness by instituting procedures so that—

(1) Any individual shall, upon satisfactory verification of his identity, be entitled to review without undue burden to either the criminal justice agency or the individual, any criminal history record information maintained about the individual and obtain a copy thereof when necessary for the purpose of challenge or correction;

(2) Administrative review and necessary correction of any claim by the individual to whom the information relates that the information is inaccurate or incomplete is provided;

(3) The State shall establish and implement procedures for administrative appeal where a criminal justice agency refuses to correct challenged information to the satisfaction of the individual to whom the information relates;

(4) Upon request, an individual whose record has been corrected shall be given the names of all non-criminal justice agencies to whom the data has been given;

(5) The correcting agency shall notify all criminal justice recipients of corrected information; and

(6) The individual's right to access and review of criminal history record information shall not extend to data contained in intelligence, investigatory, or other related files and shall not be construed to include any other information than that defined by §20.3(b).

[41 FR 11715, Mar. 19, 1976, as amended at 42 FR 61595, Dec. 6, 1977]

§20.22 Certification of compliance.

(a) Each State to which these regulations are applicable shall with the submission of its plan provide a certification that to the maximum extent feasible action has been taken to comply with the procedures set forth in the plan. Maximum extent feasible, in this subsection, means actions which can be

taken to comply with the procedures set forth in the plan that do not require additional legislative authority or involve unreasonable cost or do not exceed existing technical ability.

(b) The certification shall include—

(1) An outline of the action which has been instituted. At a minimum, the requirements of access and review under § 20.21(g) must be completely operational;

(2) A description of any legislation or executive order, or attempts to obtain such authority that has been instituted to comply with these regulations;

(3) A description of the steps taken to overcome any fiscal, technical, and administrative barriers to the development of complete and accurate criminal history record information;

(4) A description of existing system capability and steps being taken to upgrade such capability to meet the requirements of these regulations; and

(5) A listing setting forth categories of non-criminal justice dissemination. See § 20.21(b).

§ 20.23 Documentation: Approval by OJARS.

Within 90 days of the receipt of the plan, OJARS shall approve or disapprove the adequacy of the provisions of the plan and certification. Evaluation of the plan by OJARS will be based upon whether the procedures set forth will accomplish the required objectives. The evaluation of the certification(s) will be based upon whether a good faith effort has been shown to initiate and/or further compliance with the plan and regulations. All procedures in the approved plan must be fully operational and implemented by March 1, 1978. A final certification shall be submitted on March 1, 1978.

Where a State finds it is unable to provide final certification that all required procedures as set forth in § 20.21 will be operational by March 1, 1978, a further extension of the deadline will be granted by OJARS upon a showing that the State has made a good faith effort to implement these regulations to the maximum extent feasible. Documentation justifying the request for the extension including a proposed timetable for full compliance must be submitted to OJARS by March 1, 1978. Where a State submits a request for an extension, the implementation date will be extended an additional 90 days while OJARS reviews the documentation for approval or disapproval. To be approved, such revised schedule must be consistent with the timetable and procedures set out below:

(a) July 31, 1978—Submission of certificate of compliance with:

(1) Individual access, challenge, and review requirements;

(2) Administrative security;

(3) Physical security to the maximum extent feasible.

(b) Thirty days after the end of a State's next legislative session—Submission to OJARS of a description of State policy on dissemination of criminal history record information.

(c) Six months after the end of a State's legislative session—Submission to OJARS of a brief and concise description of standards and operating procedures to be followed by all criminal justice agencies covered by OJARS regulations in complying with the State policy on dissemination.

(d) Eighteen months after the end of a State's legislative session—Submission to OJARS of a certificate attesting to the conduct of an audit of the State central repository and of a random number of other criminal justice agencies in compliance with OJARS regulations.

[41 FR 11715, Mar. 19, 1976, as amended at 42 FR 61596, Dec. 6, 1977]

§ 20.24 State laws on privacy and security.

Where a State originating criminal history record information provides for sealing or purging thereof, nothing in these regulations shall be construed to prevent any other State receiving such information, upon notification, from complying with the originating State's sealing or purging requirements.

§ 20.25 Penalties.

Any agency or individual violating subpart B of these regulations shall be subject to a civil penalty not to exceed $10,000 for a violation occurring before September 29, 1999, and not to exceed $11,000 for a violation occurring on after September 29, 1999. In addition,

OJARS may initiate fund cut-off procedures against recipients of OJARS assistance.

[41 FR 11715, Mar. 19, 1976, as amended by Order No. 2249-99, 64 FR 47102, Aug. 30, 1999]

Subpart C—Federal Systems and Exchange of Criminal History Record Information

SOURCE: Order No. 2258-99, 64 FR 52227, Sept. 28, 1999, unless otherwise noted.

§20.30 Applicability.

The provisions of this subpart of the regulations apply to the III System and the FIRS, and to duly authorized local, state, tribal, federal, foreign, and international criminal justice agencies to the extent that they utilize the services of the III System or the FIRS. This subpart is applicable to both manual and automated criminal history records.

§20.31 Responsibilities.

(a) The Federal Bureau of Investigation (FBI) shall manage the NCIC.

(b) The FBI shall manage the FIRS to support identification and criminal history record information functions for local, state, tribal, and federal criminal justice agencies, and for noncriminal justice agencies and other entities where authorized by federal statute, state statute pursuant to Public Law 92-544, 86 Stat. 1115, Presidential executive order, or regulation or order of the Attorney General of the United States.

(c) The FBI CJIS Division may manage or utilize additional telecommunication facilities for the exchange of fingerprints, criminal history record related information, and other criminal justice information.

(d) The FBI CJIS Division shall maintain the master fingerprint files on all offenders included in the III System and the FIRS for the purposes of determining first offender status; to identify those offenders who are unknown in states where they become criminally active but are known in other states through prior criminal history records; and to provide identification assistance in disasters and for other humanitarian purposes.

(e) The FBI may routinely establish and collect fees for noncriminal justice fingerprint-based and other identification services as authorized by Federal law. These fees apply to Federal, State and any other authorized entities requesting fingerprint identification records and name checks for noncriminal justice purposes.

(1) The Director of the FBI shall review the amount of the fee periodically, but not less than every four years, to determine the current cost of processing fingerprint identification records and name checks for noncriminal justice purposes.

(2) Fee amounts and any revisions thereto shall be determined by current costs, using a method of analysis consistent with widely accepted accounting principles and practices, and calculated in accordance with the provisions of 31 U.S.C. 9701 and other Federal law as applicable.

(3) Fee amounts and any revisions thereto shall be published as a notice in the FEDERAL REGISTER.

(f) The FBI will collect a fee for providing noncriminal name-based background checks of the FBI Central Records System through the National Name Check Program pursuant to the authority in Pub. L. 101-515 and in accordance with paragraphs (e)(1), (2) and (3) of this section.

[41 FR 11715, Mar. 19, 1976, as amended at 75 FR 18755, Apr. 13, 2010; 75 FR 24798, May 6, 2010]

§20.32 Includable offenses.

(a) Criminal history record information maintained in the III System and the FIRS shall include serious and/or significant adult and juvenile offenses.

(b) The FIRS excludes arrests and court actions concerning nonserious offenses, e.g., drunkenness, vagrancy, disturbing the peace, curfew violation, loitering, false fire alarm, non-specific charges of suspicion or investigation, and traffic violations (except data will be included on arrests for vehicular manslaughter, driving under the influence of drugs or liquor, and hit and run), when unaccompanied by a §20.32(a) offense. These exclusions may not be applicable to criminal history records maintained in state criminal

history record repositories, including those states participating in the NFF.

(c) The exclusions enumerated above shall not apply to federal manual criminal history record information collected, maintained, and compiled by the FBI prior to the effective date of this subpart.

§ 20.33 Dissemination of criminal history record information.

(a) Criminal history record information contained in the III System and the FIRS may be made available:

(1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies;

(2) To federal agencies authorized to receive it pursuant to federal statute or Executive order;

(3) For use in connection with licensing or employment, pursuant to Public Law 92–544, 86 Stat. 1115, or other federal legislation, and for other uses for which dissemination is authorized by federal law. Refer to § 50.12 of this chapter for dissemination guidelines relating to requests processed under this paragraph;

(4) For issuance of press releases and publicity designed to effect the apprehension of wanted persons in connection with serious or significant offenses;

(5) To criminal justice agencies for the conduct of background checks under the National Instant Criminal Background Check System (NICS);

(6) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/ information services for criminal justice agencies; and

(7) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

(b) The exchange of criminal history record information authorized by paragraph (a) of this section is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or service providers identified in paragraphs (a)(6) and (a)(7) of this section.

(c) Nothing in these regulations prevents a criminal justice agency from disclosing to the public factual information concerning the status of an investigation, the apprehension, arrest, release, or prosecution of an individual, the adjudication of charges, or the correctional status of an individual, which is reasonably contemporaneous with the event to which the information relates.

(d) Criminal history records received from the III System or the FIRS shall be used only for the purpose requested and a current record should be requested when needed for a subsequent authorized use.

§ 20.34 Individual's right to access criminal history record information.

The procedures by which an individual may obtain a copy of his or her identification record from the FBI to review and request any change, correction, or update are set forth in §§ 16.30–16.34 of this chapter. The procedures by which an individual may obtain a copy of his or her identification record from a state or local criminal justice agency are set forth in § 20.34 of the appendix to this part.

§ 20.35 Criminal Justice Information Services Advisory Policy Board.

(a) There is established a CJIS Advisory Policy Board, the purpose of which is to recommend to the FBI Director general policy with respect to the philosophy, concept, and operational principles of various criminal justice information systems managed by the FBI's CJIS Division.

(b) The Board includes representatives from state and local criminal justice agencies; members of the judicial, prosecutorial, and correctional segments of the criminal justice community; a representative of federal agencies participating in the CJIS systems; and representatives of criminal justice professional associations.

(c) All members of the Board will be appointed by the FBI Director.

(d) The Board functions solely as an advisory body in compliance with the provisions of the Federal Advisory Committee Act, Title 5, United States Code, Appendix 2.

§ 20.36 Participation in the Interstate Identification Index System.

(a) In order to acquire and retain direct access to the III System, each Control Terminal Agency and Federal Service Coordinator shall execute a CJIS User Agreement (or its functional equivalent) with the Assistant Director in Charge of the CJIS Division, FBI, to abide by all present rules, policies, and procedures of the NCIC, as well as any rules, policies, and procedures hereinafter recommended by the CJIS Advisory Policy Board and adopted by the FBI Director.

(b) Entry or updating of criminal history record information in the III System will be accepted only from state or federal agencies authorized by the FBI. Terminal devices in other agencies will be limited to inquiries.

§ 20.37 Responsibility for accuracy, completeness, currency, and integrity.

It shall be the responsibility of each criminal justice agency contributing data to the III System and the FIRS to assure that information on individuals is kept complete, accurate, and current so that all such records shall contain to the maximum extent feasible dispositions for all arrest data included therein. Dispositions should be submitted by criminal justice agencies within 120 days after the disposition has occurred.

§ 20.38 Sanction for noncompliance.

Access to systems managed or maintained by the FBI is subject to cancellation in regard to any agency or entity that fails to comply with the provisions of subpart C of this part.

APPENDIX TO PART 20—COMMENTARY ON SELECTED SECTIONS OF THE REGULATIONS ON CRIMINAL HISTORY RECORD INFORMATION SYSTEMS

Subpart A–§ 20.3(d). The definition of criminal history record information is intended to include the basic offender-based transaction statistics/III System (OBTS/III) data elements. If notations of an arrest, disposition, or other formal criminal justice transaction occurs in records other than the traditional "rap sheet," such as arrest reports, any criminal history record information contained in such reports comes under the definition of this subsection.

The definition, however, does not extend to other information contained in criminal justice agency reports. Intelligence or investigative information (e.g., suspected criminal activity, associates, hangouts, financial information, and ownership of property and vehicles) is not included in the definition of criminal history information.

§ 20.3(g). The definitions of criminal justice agency and administration of criminal justice in § 20.3(b) of this part must be considered together. Included as criminal justice agencies would be traditional police, courts, and corrections agencies, as well as subunits of noncriminal justice agencies that perform the administration of criminal justice pursuant to a federal or state statute or executive order and allocate a substantial portion of their budgets to the administration of criminal justice. The above subunits of noncriminal justice agencies would include, for example, the Office of Investigation of the Food and Drug Administration, which has as its principal function the detection and apprehension of persons violating criminal provisions of the Federal Food, Drug and Cosmetic Act. Also included under the definition of criminal justice agency are umbrella-type administrative agencies supplying criminal history information services, such as New York's Division of Criminal Justice Services.

§ 20.3(i). Disposition is a key concept in section 524(b) of the Act and in §§ 20.21(a)(1) and 20.21(b) of this part. It therefore is defined in some detail. The specific dispositions listed in this subsection are examples only and are not to be construed as excluding other, unspecified transactions concluding criminal proceedings within a particular agency.

§ 20.3(q). The different kinds of acquittals and dismissals delineated in § 20.3(i) are all considered examples of nonconviction data.

Subpart B—§ 20.20(a). These regulations apply to criminal justice agencies receiving funds under the Omnibus Crime Control and Safe Streets Act for manual or automated

systems subsequent to July 1, 1973. In the hearings on the regulations, a number of those testifying challenged LEAA's authority to promulgate regulations for manual systems by contending that section 524(b) of the Act governs criminal history information contained in automated systems.

The intent of section 524(b), however, would be subverted by only regulating automated systems. Any agency that wished to circumvent the regulations would be able to create duplicate manual files for purposes contrary to the letter and spirit of the regulations.

Regulation of manual systems, therefore, is authorized by section 524(b) when coupled with section 501 of the Act which authorizes the Administration to establish rules and regulations "necessary to the exercise of its functions * * *."

The Act clearly applies to all criminal history record information collected, stored, or disseminated with LEAA support subsequent to July 1, 1973.

Limitations as contained in subpart C also apply to information obtained from the FBI Identification Division or the FBI/NCIC System.

§ 20.20 (b) and (c). Section 20.20 (b) and (c) exempts from regulations certain types of records vital to the apprehension of fugitives, freedom of the press, and the public's right to know. Court records of public judicial proceedings are also exempt from the provisions of the regulations.

Section 20.20(b)(2) attempts to deal with the problem of computerized police blotters. In some local jurisdictions, it is apparently possible for private individuals and/or newsmen upon submission of a specific name to obtain through a computer search of the blotter a history of a person's arrests. Such files create a partial criminal history data bank potentially damaging to individual privacy, especially since they do not contain final dispositions. By requiring that such records be accessed solely on a chronological basis, the regulations limit inquiries to specific time periods and discourage general fishing expeditions into a person's private life.

Subsection 20.20(c) recognizes that announcements of ongoing developments in the criminal justice process should not be precluded from public disclosure. Thus, announcements of arrest, convictions, new developments in the course of an investigation may be made. It is also permissible for a criminal justice agency to confirm certain matters of public record information upon specific inquiry. Thus, if a question is raised: "Was X arrested by your agency on January 3, 1975" and this can be confirmed or denied by looking at one of the records enumerated in subsection (b) above, then the criminal justice agency may respond to the inquiry. Conviction data as stated in § 20.21(b) may be disseminated without limitation.

§ 20.21. The regulations deliberately refrain from specifying who within a State should be responsible for preparing the plan. This specific determination should be made by the Governor. The State has 90 days from the publication of these revised regulations to submit the portion of the plan covering §§ 20.21(b) and 20.21(f).

§ 20.21(a)(1). Section 524(b) of the Act requires that LEAA insure criminal history information be current and that, to the maximum extent feasible, it contain disposition as well as current data.

It is, however, economically and administratively impractical to maintain complete criminal histories at the local level. Arrangements for local police departments to keep track of dispositions by agencies outside of the local jurisdictions generally do not exist. It would, moreover, be bad public policy to encourage such arrangements since it would result in an expensive duplication of files.

The alternatives to locally kept criminal histories are records maintained by a central State repository. A central State repository is a State agency having the function pursuant to a statute or executive order of maintaining comprehensive statewide criminal history record information files. Ultimately, through automatic data processing the State level will have the capability to handle all requests for in-State criminal history information.

Section 20.20(a)(1) is written with a centralized State criminal history repository in mind. The first sentence of the subsection states that complete records should be retained at a central State repository. The word "should" is permissive; it suggests but does not mandate a central State repository.

The regulations do require that States establish procedures for State and local criminal justice agencies to query central State repositories wherever they exist. Such procedures are intended to insure that the most current criminal justice information is used.

As a minimum, criminal justice agencies subject to these regulations must make inquiries of central State repositories whenever the repository is capable of meeting the user's request within a reasonable time. Presently, comprehensive records of an individual's transactions within a State are maintained in manual files at the State level, if at all. It is probably unrealistic to expect manual systems to be able immediately to meet many rapid-access needs of police and prosecutors. On the other hand, queries of the State central repository for most noncriminal justice purposes probably can and should be made prior to dissemination of criminal history record information.

§ 20.21(b). The limitations on dissemination in this subsection are essential to fulfill the

mandate of section 524(b) of the Act which requires the Administration to assure that the "privacy of all information is adequately provided for and that information shall only be used for law enforcement and criminal justice and other lawful purposes." The categories for dissemination established in this section reflect suggestions by hearing witnesses and respondents submitting written commentary.

The regulations distinguish between conviction and nonconviction information insofar as dissemination is concerned. Conviction information is currently made available without limitation in many jurisdictions. Under these regulations, conviction data and pending charges could continue to be disseminated routinely. No statute, ordinance, executive order, or court rule is necessary in order to authorize dissemination of conviction data. However, nothing in the regulations shall be construed to negate a State law limiting such dissemination.

After December 31, 1977, dissemination of nonconviction data would be allowed, if authorized by a statute, ordinance, executive order, or court rule, decision, or order. The December 31, 1977, deadline allows the States time to review and determine the kinds of dissemination for non-criminal justice purposes to be authorized. When a State enacts comprehensive legislation in this area, such legislation will govern dissemination by local jurisdictions within the State. It is possible for a public record law which has been construed by the State to authorize access to the public of all State records, including criminal history record information, to be considered as statutory authority under this subsection. Federal legislation and executive orders can also authorize dissemination and would be relevant authority.

For example, Civil Service suitability investigations are conducted under Executive Order 10450. This is the authority for most investigations conducted by the Commission. Section 3(a) of 10450 prescribes the minimum scope of investigation and requires a check of FBI fingerprint files and written inquiries to appropriate law enforcement agencies.

§ 20.21(b)(3). This subsection would permit private agencies such as the Vera Institute to receive criminal histories where they perform a necessary administration of justice function such as pretrial release. Private consulting firms which commonly assist criminal justice agencies in information systems development would also be included here.

§ 20.21(b)(4). Under this subsection, any good faith researchers including private individuals would be permitted to use criminal history record information for research purposes. As with the agencies designated in § 20.21(b)(3) researchers would be bound by an agreement with the disseminating criminal justice agency and would, of course, be subject to the sanctions of the Act.

The drafters of the regulations expressly rejected a suggestion which would have limited access for research purposes to certified research organizations. Specifically "certification" criteria would have been extremely difficult to draft and would have inevitably led to unnecessary restrictions on legitimate research.

Section 524(a) of the Act which forms part of the requirements of this section states:

"Except as provided by Federal law other than this title, no officer or employee of the Federal Government, nor any recipient of assistance under the provisions of this title shall use or reveal any research or statistical information furnished under this title by any person and identifiable to any specific private person for any purpose other than the purpose for which it was obtained in accordance with this title. Copies of such information shall be immune from legal process, and shall not, without the consent of the person furnishing such information, be admitted as evidence or used for any purpose in any action suit, or other judicial or administrative proceedings."

LEAA anticipates issuing regulations, pursuant to section 524(a) as soon as possible.

§ 20.21(c)(2). Presently some employers are circumventing State and local dissemination restrictions by requesting applicants to obtain an official certification of no criminal record. An employer's request under the above circumstances gives the applicant the unenviable choice of invasion of his privacy or loss of possible job opportunities. Under this subsection routine certifications of no record would no longer be permitted. In extraordinary circumstances, however, an individual could obtain a court order permitting such a certification.

§ 20.21(c)(3). The language of this subsection leaves to the States the question of who among the agencies and individuals listed in § 20.21(b) shall actually receive criminal records. Under these regulations a State could place a total ban on dissemination if it so wished. The State could, on the other hand, enact laws authorizing any member of the private sector to have access to non-conviction data.

§ 20.21(d). Non-criminal justice agencies will not be able to receive records of juveniles unless the language of a statute or court order, rule, or court decision specifies that juvenile records shall be available for dissemination. Perhaps the most controversial part of this subsection is that it denies access to records of juveniles by Federal agencies conducting background investigations for eligibility to classified information under existing legal authority.

§ 20.21(e) Since it would be too costly to audit each criminal justice agency in most

States (Wisconsin, for example, has 1075 criminal justice agencies) random audits of a "representative sample" of agencies are the next best alternative. The term "representative sample" is used to insure that audits do not simply focus on certain types of agencies. Although this subsection requires that there be records kept with the names of all persons or agencies to whom information is disseminated, criminal justice agencies are not required to maintain dissemination logs for "no record" responses.

§ 20.21(f). Requirements are set forth which the States must meet in order to assure that criminal history record information is adequately protected. Automated systems may operate in shared environments and the regulations require certain minimum assurances.

§ 20.21(g)(1). A "challenge" under this section is an oral or written contention by an individual that his record is inaccurate or incomplete; it would require him to give a correct version of his record and explain why he believes his version to be correct. While an individual should have access to his record for review, a copy of the record should ordinarily only be given when it is clearly established that it is necessary for the purpose of challenge.

The drafters of the subsection expressly rejected a suggestion that would have called for a satisfactory verification of identity by fingerprint comparison. It was felt that States ought to be free to determine other means of identity verification.

§ 20.21(g)(5). Not every agency will have done this in the past, but henceforth adequate records including those required under 20.21(e) must be kept so that notification can be made.

§ 20.21(g)(6). This section emphasizes that the right to access and review extends only to criminal history record information and does not include other information such as intelligence or treatment data.

§ 20.22(a). The purpose for the certification requirement is to indicate the extent of compliance with these regulations. The term "maximum extent feasible" acknowledges that there are some areas such as the completeness requirement which create complex legislative and financial problems.

NOTE: In preparing the plans required by these regulations, States should look for guidance to the following documents: National Advisory Commission on Criminal Justice Standards and Goals, Report on the Criminal Justice System; Project SEARCH: Security and Privacy Considerations in Criminal History Information Systems, Technical Reports No. 2 and No. 13; Project SEARCH: A Model State Act for Criminal Offender Record Information, Technical Memorandum No. 3; and Project SEARCH: Model Administrative Regulations for Criminal Offender Record Information, Technical Memorandum No. 4.

Subpart C–§ 20.31. This section defines the criminal history record information system managed by the Federal Bureau of Investigation. Each state having a record in the III System must have fingerprints on file in the FBI CJIS Division to support the III System record concerning the individual.

Paragraph (b) is not intended to limit the identification services presently performed by the FBI for local, state, tribal, and federal agencies.

§ 20.32. The grandfather clause contained in paragraph (c) of this section is designed, from a practical standpoint, to eliminate the necessity of deleting from the FBI's massive files the non-includable offenses that were stored prior to February, 1973. In the event a person is charged in court with a serious or significant offense arising out of an arrest involving a non-includable offense, the non-includable offense will also appear in the arrest segment of the III System record.

§ 20.33(a)(3). This paragraph incorporates provisions cited in 28 CFR 50.12 regarding dissemination of identification records outside the federal government for noncriminal justice purposes.

§ 20.33(a)(6). Noncriminal justice governmental agencies are sometimes tasked to perform criminal justice dispatching functions or data processing/information services for criminal justice agencies as part, albeit not a principal part, of their responsibilities. Although such inter-governmental delegated tasks involve the administration of criminal justice, performance of those tasks does not convert an otherwise non-criminal justice agency to a criminal justice agency. This regulation authorizes this type of delegation if it is effected pursuant to executive order, statute, regulation, or interagency agreement. In this context, the noncriminal justice agency is servicing the criminal justice agency by performing an administration of criminal justice function and is permitted access to criminal history record information to accomplish that limited function. An example of such delegation would be the Pennsylvania Department of Administration's Bureau of Consolidated Computer Services, which performs data processing for several state agencies, including the Pennsylvania State Police. Privatization of the data processing/information services or dispatching function by the noncriminal justice governmental agency can be accomplished pursuant to § 20.33(a)(7) of this part.

§ 20.34. The procedures by which an individual may obtain a copy of his manual identification record are set forth in 28 CFR 16.30–16.34.

The procedures by which an individual may obtain a copy of his III System record are as follows: If an individual has a criminal record supported by fingerprints and that

record has been entered in the III System, it is available to that individual for review, upon presentation of appropriate identification, and in accordance with applicable state and federal administrative and statutory regulations. Appropriate identification includes being fingerprinted for the purpose of insuring that he is the individual that he purports to be. The record on file will then be verified as his through comparison of fingerprints.

Procedure. 1. All requests for review must be made by the subject of the record through a law enforcement agency which has access to the III System. That agency within statutory or regulatory limits can require additional identification to assist in securing a positive identification.

2. If the cooperating law enforcement agency can make an identification with fingerprints previously taken which are on file locally and if the FBI identification number of the individual's record is available to that agency, it can make an on-line inquiry through NCIC to obtain his III System record or, if it does not have suitable equipment to obtain an on-line response, obtain the record from Clarksburg, West Virginia, by mail. The individual will then be afforded the opportunity to see that record.

3. Should the cooperating law enforcement agency not have the individual's fingerprints on file locally, it is necessary for that agency to relate his prints to an existing record by having his identification prints compared with those already on file in the FBI, or, possibly, in the state's central identification agency.

4. The subject of the requested record shall request the appropriate arresting agency, court, or correctional agency to initiate action necessary to correct any stated inaccuracy in his record or provide the information needed to make the record complete.

§20.36. This section refers to the requirements for obtaining direct access to the III System.

§20.37. The 120-day requirement in this section allows 30 days more than the similar provision in subpart B in order to allow for processing time that may be needed by the states before forwarding the disposition to the FBI.

[Order No. 662-76, 41 FR 34949, Aug. 18, 1976, as amended by Order No. 1438-90, 55 FR 32075, Aug. 7, 1990; Order No. 2258-99, 64 FR 52229, Sept. 28, 1999]

PART 21—WITNESS FEES

Sec.

21.1 Definitions.
21.2 Employees of the United States serving as witnesses.
21.3 Aliens.
21.4 Fees and allowances of fact witnesses.
21.5 Use of table of distances.
21.6 Proceedings *in forma pauperis.*
21.7 Certification of witness attendance.

AUTHORITY: 28 U.S.C. 509, 510, 1821-1825, 5 U.S.C. 301.

SOURCE: 51 FR 16171, May 1, 1986, unless otherwise noted.

§21.1 Definitions.

(a) *Agency proceeding.* An agency process as defined by 5 U.S.C. 551 (5), (7) and (9).

(b) *Alien.* Any person who is not a citizen or national of the United States.

(c) *Judicial proceeding.* Any action or suit, including any condemnation, preliminary, informational or other proceeding of a judicial nature. Examples of the latter include, but are not limited to, hearings and conferences before a committing court, magistrate, or commission, grand jury proceedings, pre-trial conferences, depositions, and coroners' inquests. It does not include information or investigative proceedings conducted by a prosecuting attorney for the purpose of determining whether an information or charge should be made in a particular case. The judicial proceeding may be in the District of Columbia, a State, or a territory or possession of the United States including the Commonwealth of Puerto Rico or the Trust Territory of the Pacific Islands.

(d) *Pre-trial conference.* A conference between the Government Attorney and a witness to discuss the witness' testimony. The conference must take place after a trial, hearing or grand jury proceeding has been scheduled but prior to the witness' actual appearance at the proceeding.

(e) *Residence.* The term *residence* is not limited to the legal residence, but includes any place at which the witness is actually residing and at which the subpoena or summons is served. If the residence of the witness at the time of appearance is different from the place of subpoena or summons, the new place of residence shall be considered the witness' residence for computation of the transportation allowance; but, if the witness is on a business or vacation trip at the time of appearance, the witness shall be paid for travel from the place of service if this does not result

2016
RSJI COMMUNITY SURVEY

SEATTLE OFFICE FOR CIVIL RIGHTS

APRIL 2017

Acknowledgements

The RSJI Community Survey is the result of collaboration among researchers, community leaders and the City of Seattle who worked together as part of a Race and Social Justice Community Survey Steering Committee. We thank the Steering Committee for guiding the development of the survey questions and outreach.

Thank you to Gabriela Quintana for overall project coordination, including managing outreach. Outreach also was made possible through the support of our Community Survey Partners, City employees, and students from the University of Washington. Special thanks to Sarah Leyrer, Margaret Weihs, Brian Cedeno, Kelsey McGuire, Hillary Jaregui, Cornetta Mosley, Tucker Richards, Kathryn Peebles, Junyi Zhang, Violet Lavatai, Darcy White and Fadumo Nurdin.

Thank you to Pacific Market Research for fielding the phone survey.

Special thanks to Chris Hess at the University of Washington Sociology Department for providing data analysis and an early draft that laid the foundation for the final report.

2016 Race and Social Justice Initiative
Community Survey
Steering Committee Members

Derrick Belgarde, Chief Seattle Club

Kyle Crowder, University of Washington

Ben Danielson, Odessa Brown Medical Center

Patricia Hayden, Seattle Human Services Coalition

Marcos Martinez, Entre Hermanos

Xochitl Maykovich, Washington Community Action Network

India Ornelas, University of Washington

Rebecca Saldaña, Puget Sound Sage

Michael Ramos, Church Council of Greater Seattle

Jenny Romich, University of Washington

Rich Stolz, OneAmerica

Executive Summary

The Seattle Race and Social Justice Initiative (RSJI) is the City of Seattle's commitment to ending racial disparities and achieving racial equity in Seattle. In 2014, the City affirmed and expanded RSJI via an Executive Order requiring City staff to assess progress made on racial equity. It also called on the Race and Social Justice Initiative to deepen the City's support for community-led racial justice work through projects and programs that increase the City's accountability to the community. The RSJI Community Survey is a key part of assessing the impact of our collective efforts for racial equity.

The RSJI Community Survey, first fielded in 2013, measures the perspectives of those who live, work, and go to school in Seattle, including satisfaction with City services, neighborhood quality, housing affordability, feelings about the state of racial equity in the city, and the role of government in addressing racial inequities. The 2016 survey provides updated information on the state of racial equity in Seattle.

Key Findings

1 **Ending racial inequity is a responsibility of government.**

Seattle respondents feel strongly that government should prioritize ending the racial equity gaps that impact our communities. Nearly all respondents (96%) said government should prioritize addressing racial inequities.

2 **To achieve equity, resources must be allocated based on need.**

Eighty-seven percent of all respondents agreed when asked whether a greater portion of resources should go to those most in need.

3 **Economic prosperity is not felt by all -- Seattle's Black community experiences a disproportionate lack of opportunity.**

More than half (53%) of all Black/African American survey respondents said they are *not* experiencing economic opportunities; Black/African American women cite the highest rates of economic exclusion.

4 **Environmental inequities persist by race and gender.**

People of color and transgender respondents were more likely to say their neighborhoods are unhealthy places to live; close to half of all American Indian/Alaska Native respondents do not feel they have benefited from Seattle's environmental progress.

5 **Communities of color do not feel they experience equal treatment by the City's criminal justice system.**

The number of people across the board reporting greater confidence in the police has increased since the last survey, but communities of color continue to have less confidence in the police than White

respondents do. More than half of all African American/Black respondents (56.1%), and nearly half of all Multiracial respondents (47.3%) and American Indian/Alaska Native (47%) respondents have little to no confidence in the police to do a good job enforcing the law.

There is a strong lack of confidence in the courts to treat people of color and Whites equally, with nearly 70% of people of color reporting a lack of confidence.

6 **Communities of color and other vulnerable groups struggle to remain in our high-cost city.**

Thirty-four percent (34.4%) of those surveyed responded that they or someone in their family have moved out of Seattle in the past two years due to the rising cost of housing. American Indian/Alaska Native, Black/African American, Multiracial, and Latino respondents were most likely to say so than other groups.

Every racial group rated the number one reason they personally had moved out of Seattle to be the need to find lower rent or a less expensive house to maintain. At the same time, people of color cited other economic reasons (such as foreclosure or eviction) more often than White respondents.

7 **Seattle Public Schools struggle to make the grade with communities of color.**

Despite some mixed opinions regarding performance and preparation of students for the future, Seattle respondents were united in support of ending punitive discipline measures and improving schools and after-school programs to promote racial equity. Differences in perceptions of Seattle Public Schools (SPS) emerged along racial lines. The web survey showed that while 44.5% of young people ages 15-25 rated SPS favorably, youth of color were less likely to rate Seattle Public Schools favorably compared to their White counterparts.

8 **City efforts to be inclusive are making some inroads, but more work needs to be done.**

In both phone and web surveys, we saw a decline in the number of people who felt their participation in City processes was valued. Despite this overall decline, the web survey found communities of color and lesbian, gay and bisexual respondents felt their participation was valued at a greater rate than reported in 2013. This did not hold for transgender respondents who were less likely to say their participation was valued compared to 2013.

9 **Progress towards racial equity is not being felt by all. Urgency and action is necessary to make a difference in people's lives.**

Both phone and web surveys revealed a decline in the percentage of people agreeing that Seattle is making progress at eliminating racial inequity. Seventy-two percent of phone and 43% of web respondents agree that Seattle is making progress. This is a decline by a margin of 7% points in the web survey and a margin of 14% in the web survey. When disaggregated by race, the percent stayed consistent for communities of color compared to 2013, while an increasing number of White respondents do not believe the City is making progress.

Conclusion

Seattle remains a City with much work to do to achieve racial equity. The Race and Social Justice Initiative is tasked with leading municipal government's efforts to put our value of racial equity into action. The 2013 survey provided us with baseline data on the experiences of people who live, work, and go to school in Seattle. The 2016 survey reveals sobering information that the City cannot afford to ignore: despite our efforts to address inequities, **we continue to see disparate outcomes** for our communities by race and other factors. If we are going to truly see a difference in people's lives, we must invest in community-driven strategies that hold us accountable to those most impacted by structural racism and other biases. We can and we must do better.

Methodology

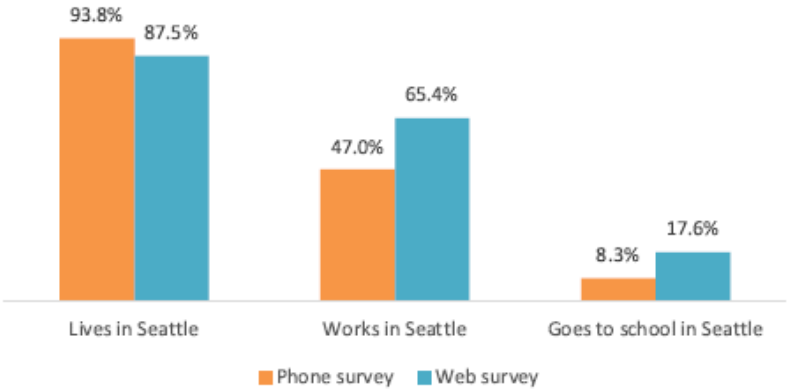
The Race and Social Justice Community Survey was developed in partnership with a steering committee comprised of researchers from the University of Washington, community based organizations and local government. Steering Committee members guided question development and outreach.

Survey data was collected via phone and internet. The phone survey included 400 respondents and the web survey included 1,295 for a total of 1,695 respondents. Phone and web surveys differed in a few key ways: the phone survey was fielded using random digit dialing (with a 60/40 split between landline and wireless phones), while the web survey was composed of self-selected respondents. Outreach efforts for the web survey were conducted by City staff and a team of student volunteers from the University of Washington who asked community partners to send the survey link to their clients and members, visited homeless shelters and community centers and posted the survey link at libraries.

Who we heard from

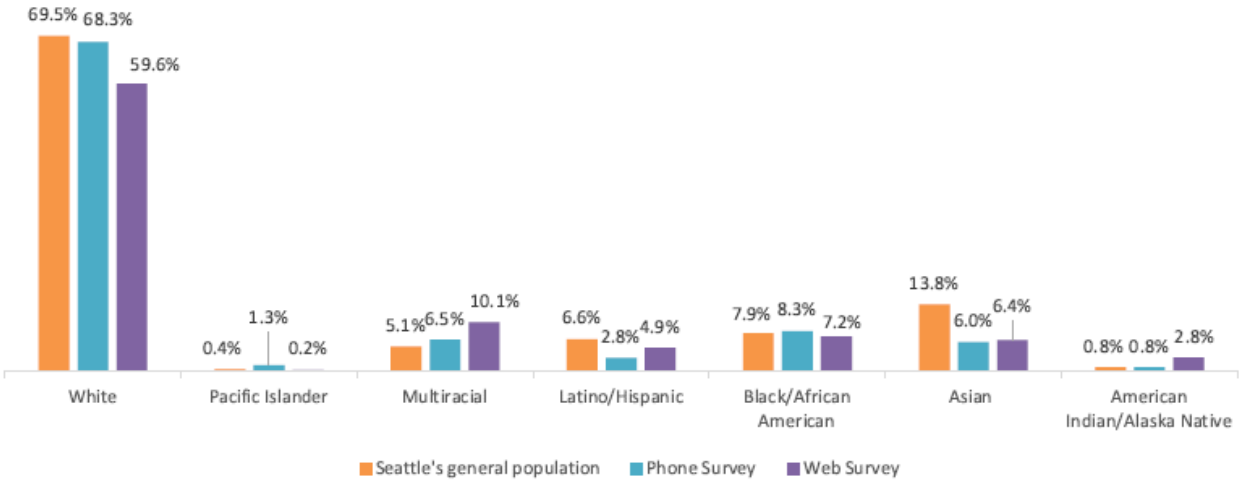
The survey was open to anyone who lives, works, or goes to school in Seattle. Nearly all respondents live in Seattle and nearly half of all phone respondents and more than half of all web respondents work in Seattle. Eighteen percent of those surveyed by web go to school in Seattle, slightly more than twice the rate of those surveyed by phone [Figure 1].

Figure 1. Percent of respondents by survey type who live, work and go to school in Seattle



In terms of race, the phone survey most closely matched the demographics of Seattle for White respondents, Black/African American respondents, Multiracial respondents, and American Indian/Alaska Native respondents. Both surveys received an under representation of Latino and Asian/Pacific Islander respondents compared to their percent of the overall population [Figure 2].

Figure 2. Comparison of survey respondents to overall Seattle population by race



*Note: Survey only fielded to those over the age of 15. Seattle general population data above includes those under 15.

In terms of age, the phone survey respondents skewed older. For reference, the Census Bureau's most recent American Community Survey (ACS) found that about 10% of the Seattle population is 65 years of age or older. Of those surveyed by phone, 35% of the phone survey respondents was 65 or older. In terms of gender, the ACS only records male and female genders and estimates a 50/50 split in the Seattle population. This suggests that the web data over-surveyed females, with 65% identifying as female.

The report uses a combination of individual and pooled in lieu of weighting tabulations to account for variations in sample sizes. Web surveying had an explicit goal of reaching subpopulations across many dimensions, including those experiencing homelessness. Researchers providing guidance on this survey, were concerned that weighting might undermine that study design goal. Without the certainty that weighting would improve the substantive conclusions, researchers opted to analyze the data as observed/collected, and use pooled estimates as an alternative way to show overall distributions, with the non-response bias of each dataset to some extent cancelling the other's out. Pooling the data potentially averages out some of the differences in demographic composition relative to the overall Seattle population.

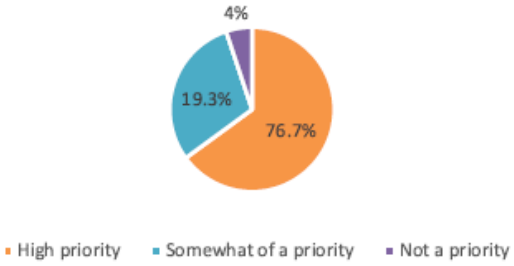
1 Ending racial inequity is a responsibility of government.

Survey respondents feel strongly that government should prioritize the racial equity gaps impacting our communities. More people see this is a high priority than two years ago.

- Nearly all respondents (96%) said government should prioritize addressing racial inequities, with **nearly 8 in 10 people saying racial equity should be a "high priority" of government** [Figure 3].

- The number respondents stating that racial equity work should be a "high priority" for government has increased over time. In our 2013 phone survey, 51% rated it as such. In the 2016 phone survey, it increased by 13 percentage points to 64%. The web responses increased only slightly from 74% in 2013 to 77% in 2016.

Figure 3. How high a priority should it be for government to address racial equity gaps in education, criminal justice, jobs, health, housing and other areas?
(Pooled data, N=1621)



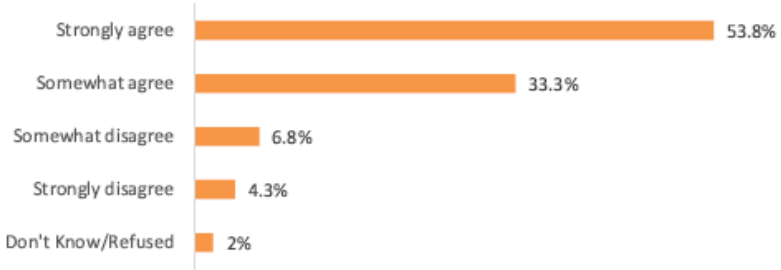
- **The urgency and responsibility for government to act was clearly reflected in responses of Black/African American and Latino respondents,** 95% and 80% of whom said addressing these gaps should be a high priority (pooled data).

2 To get to equity, resources must be allocated based on need.

- When asked if a greater portion of resources should go to those most in need to create equity for all, 87% agreed [pooled data].

- Over half (53.8%) of all phone respondents strongly agreed [Figure 4].

Figure 4. Responses to statement, "To create equity and opportunity for all, I believe a greater portion of resources should go to those who are most in need."
(Phone survey, N=400)



3 Economic prosperity is not felt by all -- Seattle's Black community experiences a disproportionate lack of opportunity.

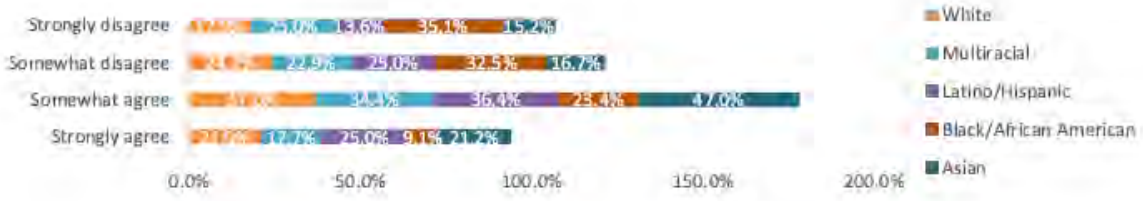
Overall, the percentage of people experiencing opportunities to get ahead economically in Seattle has decreased over time. While over half of survey respondents (62% phone and 52% web) agreed that Seattle offers good economic opportunities, these figures are a significant decrease from prior phone surveys where in 2013, 80% and in 2001, 86% of respondents reported favorable opportunities.

- The impact of a lack of economic opportunities felt by the Black community cannot be understated. **More than half (58.5%) of all Black/African American surveyed said they are *not* experiencing economic opportunities.** No other racial group reported this high a lack of opportunity (Figure 5).

Figure 5. Percent of individuals by race who disagree that Seattle has offered good opportunties for them to get ahead economically
(Pooled data, N=1448)

- An analysis of responses across race among female respondents found that **a strong majority (67%) of Black/African American women were dissatisfied with the opportunities Seattle affords them to get ahead economically** (Figure 6). Considering the 2013 survey observed a similar differential for women of color, the surveys together suggest differences in economic opportunity for Black/African American women have remained prominent post-recession.

Figure 6. Female respondents by race who responded to the question, "To what extent do you agree that Seattle has offered you good opportunities to get ahead economically?"
(Pooled data, N=916)

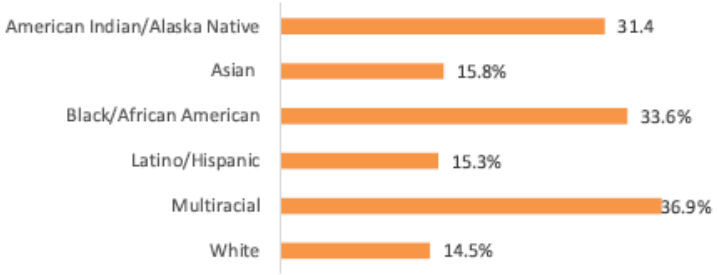


4 Environmental inequities persist by race and gender.

Seattle is noted nationally for its strong environmental efforts and as a healthy place to live. Strong majorities of phone and web survey respondents agree (88.5% phone/76.7% web). Yet when disaggregated by race and by gender, inequities emerge. People of color and transgender respondents were more likely not to find their neighborhood a healthy place to live.

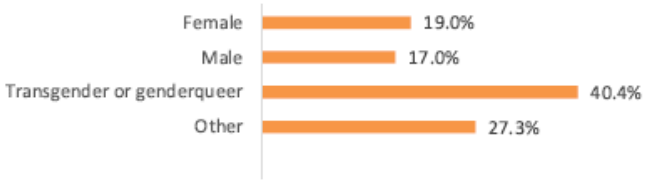
- Multiracial, Black/African American and American Indian/Alaska Native respondents were less likely to report than other groups that their neighborhood is a healthy place to live [Figure 7].

Figure 7. Percent of respondents by race who disagree with the statement, "My neighborhood is a healthy place to live."
(Pooled data, N=1480)



- In the web survey, transgender and genderqueer respondents were significantly less likely to report that their neighborhood is a healthy place to live [Figure 8].

Figure 8. Percent of respondents by gender who disagree with the statement, "My neighborhood is a healthy place to live."
(Web survey, N=1195)

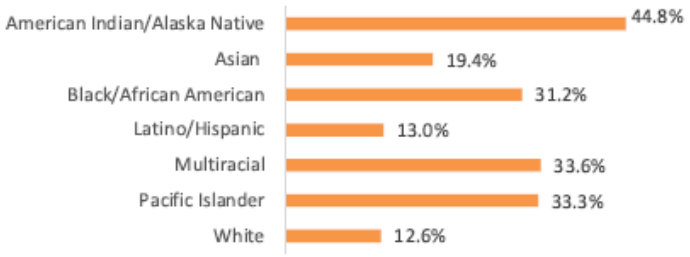


Similarly, while most respondents felt they benefited from the city's environmental progress (71% phone/ 67% web), the feeling was not shared across race.

- White survey respondents were more than twice as likely to *strongly agree* that they have benefited compared to American Indian/Alaska Native, Black/African American, and Multiracial respondents.

- Close to half (44.8%) of all American Indian/Alaska Native people who completed the web survey felt they did not benefit [Figure 9].

Figure 9. Percent of web respondents by race who disagree with the statement, "I have benefited from Seattle's environmental progress."
(Web survey, N=1033)

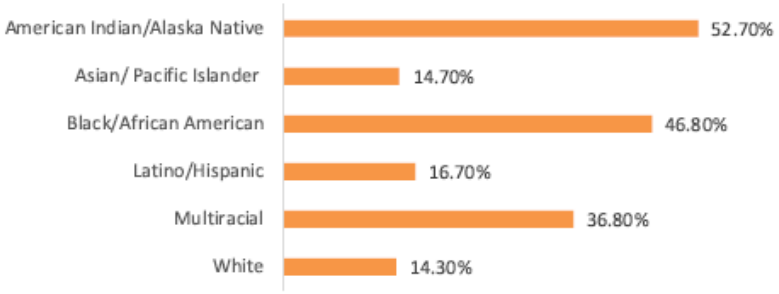


5 Criminal justice -- equal treatment not felt by communities of color.

The survey reflected strong difference in how people of color and White respondents are experiencing the criminal justice system. Confidence in the police to do a good job enforcing the law and in the police and courts to treat people of color and Whites equally found mixed evaluations—particularly when analyzed across race.

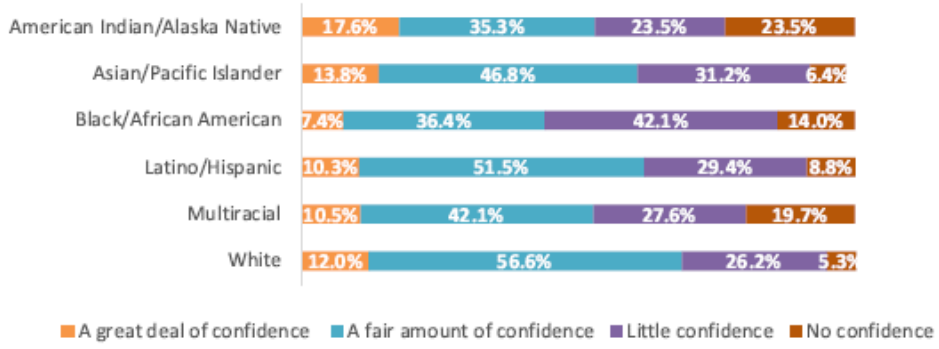
- **More than half of American Indian/Alaska Native (52.7%)** and **nearly half of all Black/African American (46.8%)** respondents surveyed reported being questioned by the police, charged or arrested when they had not committed a crime [Figure 10].

Figure 10. Responded "Yes" to the question, "Have you ever been questioned by the police, charged, or arrested when you had not committted a crime?"
(Pooled data, N = 1602)



- **More people reported confidence in the police to do a good job enforcing the law.** Seventy-eight percent of phone respondents had at least fair confidence in the police to enforce the law, an increase in the phone survey responses from 2013, when only 66% of phone respondents reported at least fair confidence. The web responses over time have not shifted in the same way. The percentage of web respondents reporting a fair amount of confidence in the police increased only 1% in the last two years, from 53% in 2013 to 54% in 2015.

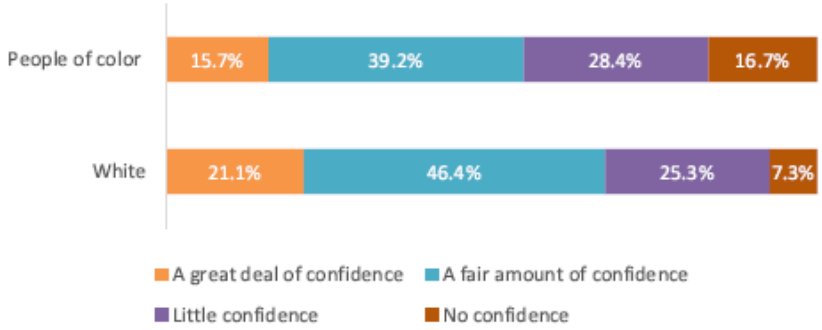
Figure 11. Confidence in police to do a good job enforcing the law?
(Pooled data, N=1,986)



- **Despite the increase, communities of color continue to have less confidence in the police than White respondents.** More than half of all African American/Black respondents (56.1%), nearly half of all Multiracial respondents (47.3%), and American Indian/Alaska Native (47%) respondents had little to no confidence in the police to do a good job enforcing the law [Figure 11].

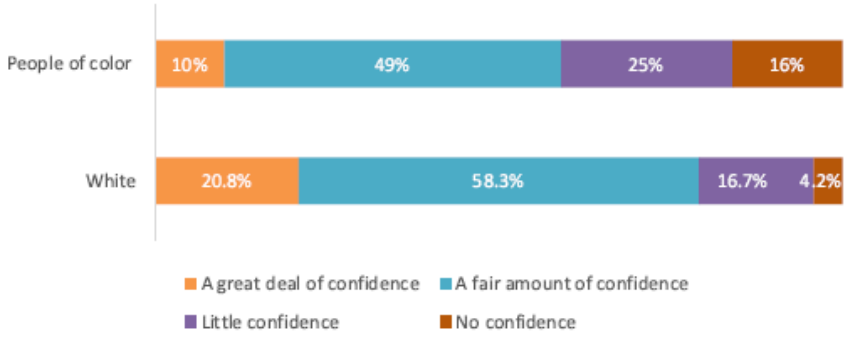
- **People of color are more likely than White respondents to report a lack of confidence in equal treatment by the police.** Close to half (45.1%) of people of color surveyed by phone had little to no confidence in police officers treating people of color and Whites equally, compared to 32.6% of White respondents [Figure 12]. The pooled data showed an even higher lack of confidence (68.8% for people of color and 61.4% for White respondents) but a smaller disparity between the two groups.

Figure 12. Confidence in police officers to treat people of color and White people equally?
(Phone data, N = 372)



- When it came to the court system, the differences in perceptions were starker between people of color and White respondents who were surveyed by phone. **People of color were twice as likely as White respondents to lack confidence in the courts to treat people equally across race.** Forty-one percent of people of color had little to no confidence in equal treatment, compared to 20.9% of White respondents [Figure 13]. Like the data regarding confidence in police, the pooled data showed across race, a greater rate of lack of confidence in equal treatment with 70% of people of color and 63% of White respondents reporting little to no confidence.

Figure 13. Confidence in courts to treat people of color and White people equally?
(Phone data, N=370)



- When asked what top three things the City should prioritize to reduce racial disproportionately in the criminal justice system, respondents were most likely to name better schools and after school programs, requiring anti-bias training for police and courts and community-based alternatives to arrest and detention [Figure 14]. This held for youth ages 15-25, and generally across race.

Figure 14. Top three actions City government should prioritize to reduce racial disproportionality in the criminal justice system
(Pooled data, N=1674)

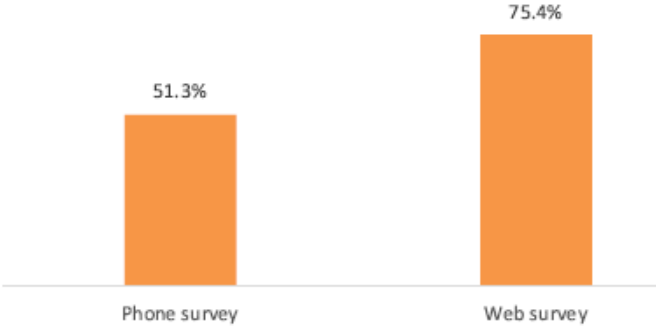
6 Housing: Communities struggle to remain in the city.

Housing Affordability: – While across race people regard Seattle's housing affordability as poor, people of color and lesbian, gay, bisexual, and transgender respondents are disproportionately feeling pushed out.

- **Since the 2013 survey, more people regard Seattle's housing as unaffordable.** In the two years between phone surveys, those reporting affordability as "only fair" or "poor" grew by 4% from 78% in 2013 to 82% in 2016.

- The majority surveyed by phone and web rated Seattle's housing affordability as "poor" [Figure 15].

Figure 15. Percent rating Seattle's housing affordability as "poor"



- **Both surveys found people of color *more likely* than White respondents to say that it was "not very likely" or "unlikely" that they would be able to afford to live in Seattle in 5 years.** The web survey found a greater percentage of respondents across the board stating that they would likely not be able to afford living in Seattle in five years. Both surveys showed a difference of 11% between people of color and White respondents, with people of color more likely to report not being able to afford living in Seattle in five years.

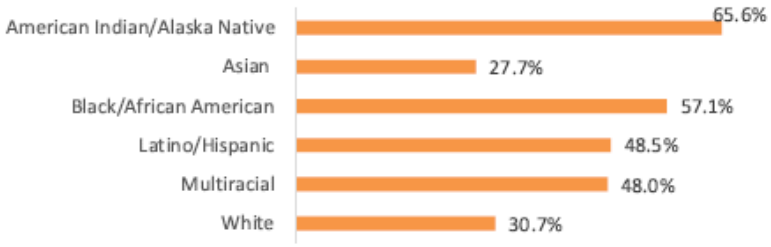
- **Nearly 70% of renters in the web survey said it was "very unlikely" to "unlikely" that they would be able to afford to live in Seattle in the next 5 years, compared to 28% of home owners.** While being a renter in Seattle clearly signals a sense of uncertainty in the ability to live in our high-cost city, **race continues to be a factor** in determining people's beliefs that they will be displaced. **African American and Black renters were disproportionately more likely than White renters to feel they will not be able to remain in Seattle in the next 5 years.** (In the web survey, 78.6% of African American/Black renters said they are not very likely or unlikely to remain in Seattle, compared to 65.4% of White renters).

- **In the web survey, transgender people of color were most likely to say they would be unable to afford living in Seattle in the next 5 years. In the web survey,** 80% of transgender/genderqueer people of color stating that it was unlikely they would be able to remain in Seattle in the next five years. Sixty-two percent (63%) of white

transgender/genderqueer respondents and 58% of lesbian, gay and bisexual respondents across race agreed.

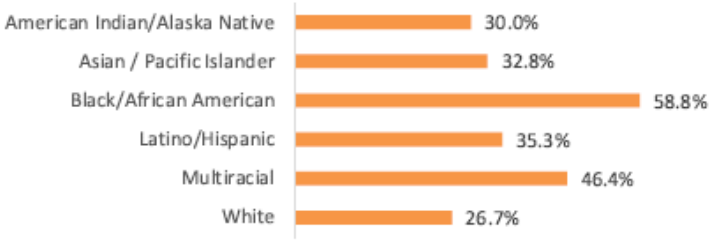
- **Thirty-four percent (34.4%) surveyed responded that they or someone in their family had moved out of Seattle in the past two years due to the rising cost of housing**. American Indian/Alaska Native, Black/African American, Multiracial, and Latino respondents were most likely to say so [Figure 16].

Figure 16. Percent by race responding "yes" to the question, "Have you or someone in your family moved out of Seattle in the past two years due to the rising cost of housing?"
(Pooled data, N=1,526)



- Places of worship, gathering places and cultural centers are often community anchors, grounding a community and providing a strong network of support. **More than half of African Americans/Black respondents (58.8%) to the web survey said it was "not very likely" or "unlikely" for their cultural center, place of worship or gathering place to remain located in Seattle in 5 years** [Figure 17].

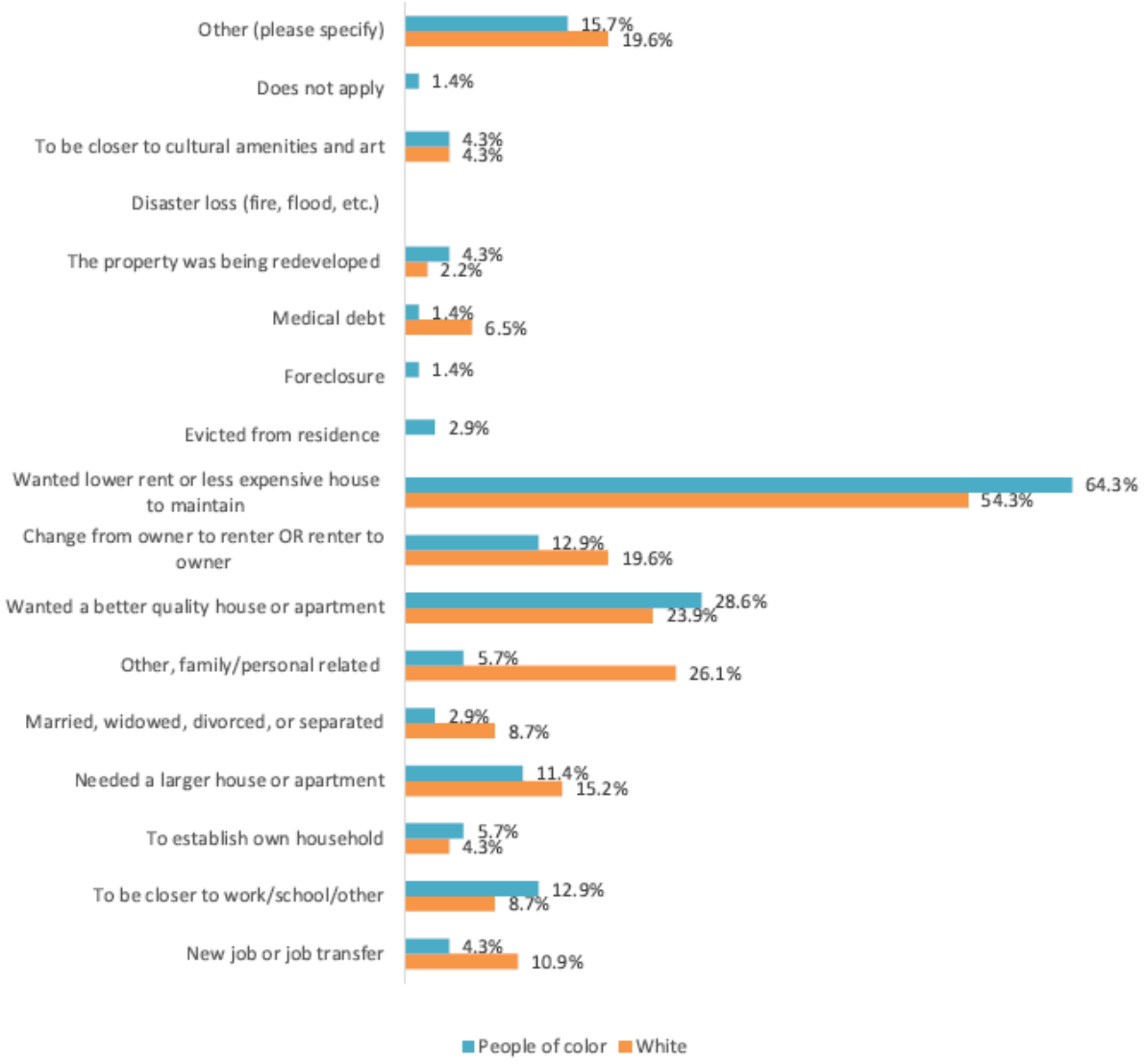
Figure 17. "Not very" or "unlikely" for your cultural center, place of worship or gathering place will be located in Seattle in 5 years
(web survey, N=342)



The web survey showed that across race, the number one reason people moved out of Seattle was for less expensive housing. People of color were more likely to cite, property redevelopment, foreclosure or eviction for having to move than White residents [Figure 18].

Figure 18. Main reasons people moved out of Seattle in last two years

(Web survey, N = 498)



Is the City doing enough to ensure people can afford to stay in Seattle?

- When asked whether the City was doing enough to ensure people can afford to stay living in Seattle, strong majorities in both the phone and web surveys (71% and 82.8% respectively) disagreed.

The role of City investments.

- The survey asked respondents if they felt City of Seattle public investments (such as transportation and utilities) have created housing affordability problems in certain neighborhoods. While 60.2% of web respondents agreed that they had, the distribution by race of those agreeing was for the most part similar, except for Asian/Pacific Islanders, who were most likely to agree by at least 7% points higher than other groups.

Quality of life is not always high for people of color, renters and people with disabilities.

- People with disabilities were nearly twice as likely to be dissatisfied with Seattle's quality of life compared to those without disabilities, 22.6% compared to 11% (pooled data).

- While all groups had a strong proportion reporting satisfaction, African Americans and American Indian/Alaska Natives who completed the web survey were nearly three times as likely as White respondents to say they were dissatisfied or very dissatisfied with the quality of life in their neighborhoods (23% and 24% compared to 8% respectively).

- Renters (29.7%) were more likely than home owners (17.6%) to be dissatisfied with Seattle as a place to raise children (web survey).

7 Education – Seattle Public Schools struggles to make the grade with communities of color.

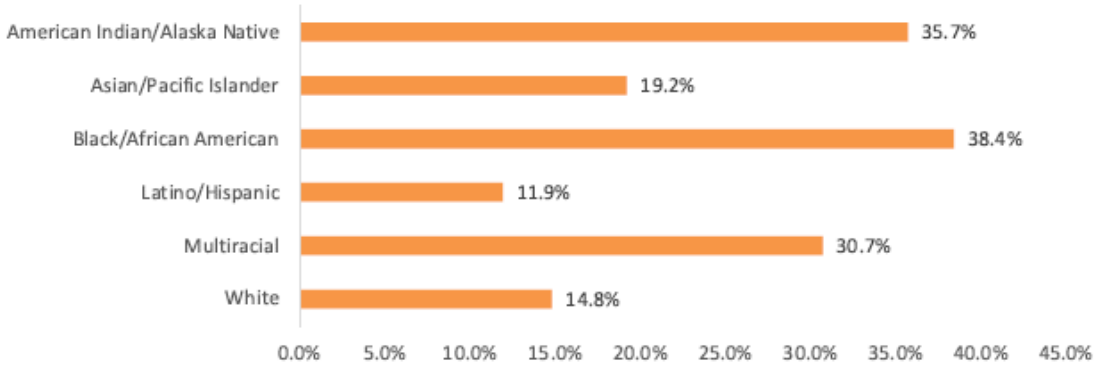
Ratings of Seattle Public Schools (SPS) were mixed across both the phone and web surveys, particularly among people of color. Despite some mixed opinions regarding SPS's performance and preparation of students for the future, responses were united in support of ending punitive discipline measures and improving schools and after-school programs to promote racial equity.

- When asked, "How do you rate Seattle Public Schools?", responses from the phone survey were nearly split in terms of favorable and unfavorable ratings (40% very good/good to 39%

fair/poor). Responses from the web data tended towards less favorable evaluations with 38.6% rating SPS as fair/poor and only 23.4% rating as good to very good [see attachment, Q 23, p11].

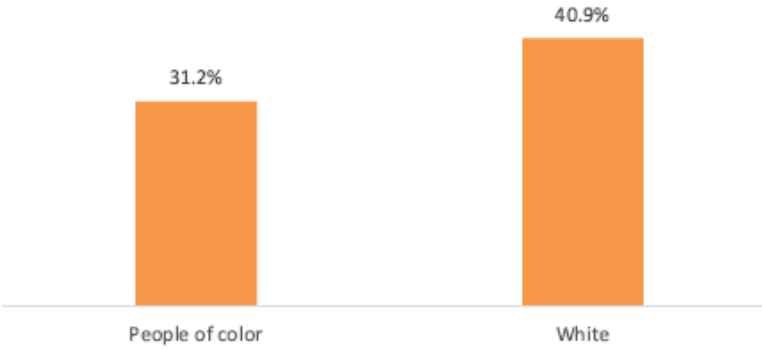
- In terms of race, Black, Native American, and Multiracial respondents gave SPS a "poor" rating more than other groups" [Figure 19].

Figure 19. Percent by race who rated Seattle Public Schools as "Poor"
(Pooled data, N=1071)



- The web survey showed that while 44.5% of young people ages 15-25 rated SPS favorably, when disaggregated by race, differences emerge. Youth of color were less likely to rate Seattle Public Schools favorably compared to their White counterparts [Figure 20].

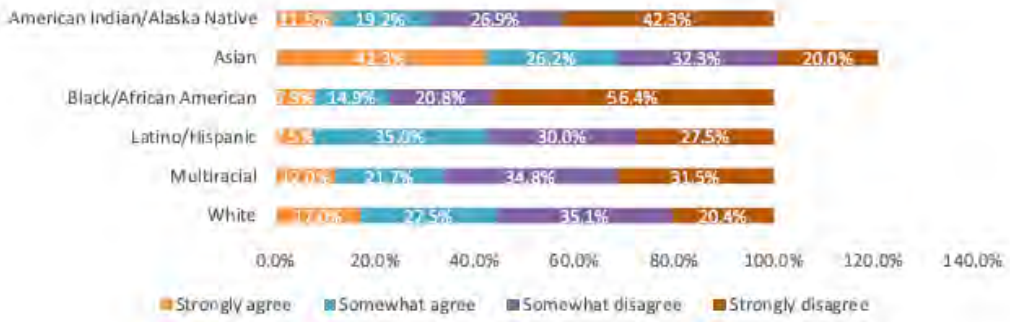
Figure 20. Percent of young people ages 15 to 25 rating SPS favorably (good/very good)
(Web survey, N=753)



- About 75% of each sample reported agreement with the statement, "Shifting from punitive discipline measures in Seattle Public Schools to measures that address harm and repair relationships is important to making sure all students, regardless of their race, receive fair and just treatment." [see Attachment, Q25] When analyzed by race, gender and sexual orientation, there was strong consensus across groups.

- Over half (56.4%) of all Black/African Americans surveyed and 42.3% of Native Americans surveyed strongly disagreed that staff and teachers at Seattle Public Schools treat students of color the same as white students [Figure 21].

Figure 21. Response by race to the statement, "Staff and teachers at Seattle Public Schools treat students of color with as much respect as white students"
(Pooled data, N=945)

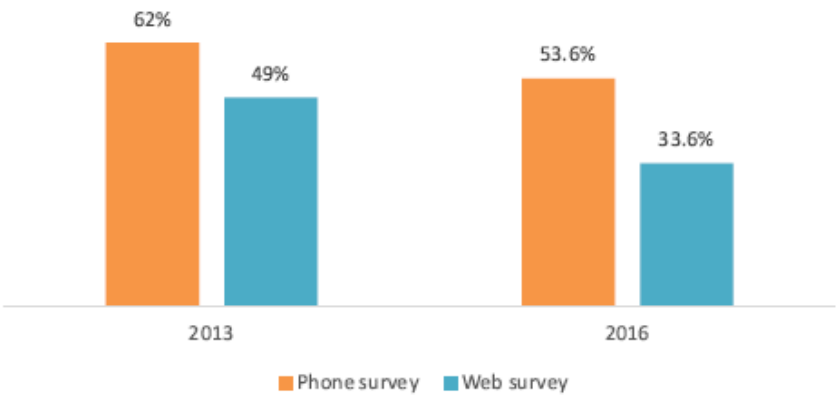


8 City efforts to be inclusive in outreach is having an impact on some groups, with more work to be done.

About half of those surveyed by phone and web (48.8% phone/51.5% web) were aware of the City of Seattle's outreach to the community on policies or projects, yet only 35.4% of those surveyed by phone and just about a quarter of those surveyed by web (26.4%) had participated.

- **Fewer people felt the City valued their participation.** Of those who had participated, over half of phone respondents (53.6%) said they felt their participation was valued a fair amount to a great deal while only 33.6% said the same in the web survey. This is a significant drop in the web responses since 2013, when 49% said they felt their participation was valued a fair amount to a great deal [Figure 22].

Figure 22. Felt participation in outreach engagement efforts was valued by the City of Seattle



- While overall, fewer people felt the City valued their participation, the racial disparity that existed in the 2013 web survey did not appear in 2016. In the 2016 web survey, **people of color were slightly more likely to say their participation was valued** a fair amount to a great deal compared to white respondents (35.1% to 32.8% respectively). This held true across race/ethnicities except for Asian Pacific Islander respondents who were approximately as likely as white respondents to say their participation was valued (32.2%).

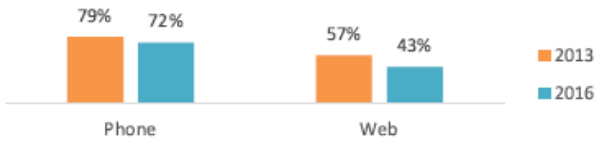
- Similarly, the disparities that existed in the 2013 web survey for lesbian, gay and bisexual respondents compared to straight respondents in terms of their participation feeling valued was not reported in the 2016 survey. Rather, **lesbian, gay, and bisexual respondents were more likely to feel their participation was valued** compared to their straight counterparts (37.3% to 32.6% respectively). This held for LGB people of color as well, of whom 39.1% said they felt their participation was valued, compared to 36% of LGB White respondents. **This did not hold for transgender respondents who were less likely to say their participation was valued** compared to 2013 (44.5% of transgender respondents said their participation was valued in 2013 which dropped to 27.3% in 2016).

- **Immigrants and refugees were slightly less likely to be aware of the City's outreach efforts than two years ago.** In 2013, 51% of web survey respondents born outside the U.S. were aware of the City's outreach efforts but fell to 46.5% in 2016.

9 Progress towards racial equity is not felt by all. Urgency and action is necessary to make a difference in people's lives.

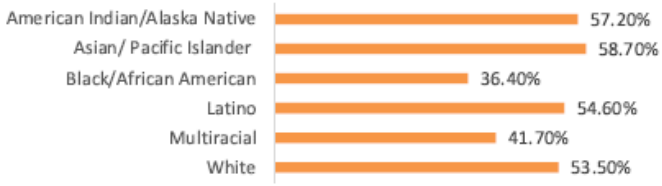
In 2016, fewer people said they believe Seattle is making progress eliminating racial inequities and creating a city where social, economic, and political opportunities and outcomes are not predicted upon a person's race than reported so in 2013 [Figure 23 and Figure 24].

Figure 23. Percent agreeing that Seattle is making progress eliminating racial inequities 2013 to 2016



Web survey data overtime shows that across race, the same or more people respond less favorably than they had in the previous survey. For example, while the percent of Black/African Americans who strongly disagreed that we are making progress held the same since the last survey (around 32%), White people were also more likely than they had been in 2013 to strongly disagree, moving from 11% in 2013 to 15% in 2016.

Figure 24. Percent agreeing that Seattle is making progress eliminating racial inequities
(web survey, N=1074)



Conclusion

For more than a decade the Race and Social Justice Initiative (RSJI) has been working to achieving racial equity within government. The 2013 Community Survey provided baseline data about who lives, works and goes to school in Seattle. The 2016 Community Survey reveals sobering facts that we cannot ignore. Despite our efforts to address the manifestations of institutional and structural racism, our communities of color continue to experience disparate outcomes in every quality of life indicator. If we are going to truly change the lives of the most impacted community members, **we must center community leadership, we must resource community-owned strategies and we must be accountable to our communities.**

We can and we must do better.

Appendix - 2016 Community Survey Frequency Tables

Question 1 — Which of the following applies to you? (Select all that apply):

Table 1: Respondent lives in Seattle

	Phone Survey	WebSurvey
Live in Seattle	375 (93.75%)	1133 (87.49%)
Does not live in Seattle	25 (6.25%)	162 (12.51%)

Table 2: Respondent works in Seattle

	Phone Survey	WebSurvey
Work in Seattle	188 (47%)	847 (65.41%)
Does not work in Seattle	212 (53%)	448 (34.59%)

Table 3: Respondent goes to school in Seattle

	Phone Survey	WebSurvey
Go to school in Seattle	33 (8.25%)	228 (17.61%)
Does not go to school in Seattle	367 (91.75%)	1067 (82.39%)

Question 2 — Please select which most closely matches your satisfaction with the quality of life in Seattle:

Table 4: Seattle as a place to live

	Phone Survey	Web Survey
Very satisfied	178 (44.5%)	434 (33.51%)
Somewhat satisfied	164 (41%)	645 (49.81%)
Dissatisfied	41 (10.25%)	115 (8.88%)
Very dissatisfied	13 (3.25%)	37 (2.86%)

Does not apply	1 (0.25%)	46 (3.55%)
Don't know / Refused	3 (0.75%)	18 (1.39%)

Table 5: Your neighborhood as a place to live

	Phone Survey	Web Survey
Very satisfied	221 (55.25%)	506 (39.07%)
Somewhat satisfied	150 (37.5%)	552 (42.63%)
Dissatisfied	21 (5.25%)	107 (8.26%)
Very dissatisfied	6 (1.5%)	30 (2.32%)
Does not apply	2 (0.5%)	66 (5.1%)
Don't know / Refused	0 (0%)	34 (2.63%)

Table 6: Seattle as a place to raise children

	Phone Survey	Web Survey
Very satisfied	134 (33.5%)	244 (18.84%)
Somewhat satisfied	139 (34.75%)	430 (33.2%)
Dissatisfied	34 (8.5%)	148 (11.43%)
Very dissatisfied	6 (1.5%)	47 (3.63%)
Does not apply	71 (17.75%)	380 (29.34%)
Don't know / Refused	16 (4%)	46 (3.55%)

Table 7: Seattle as a place to work

	Phone Survey	Web Survey
Very satisfied	186 (46.5%)	429 (33.13%)
Somewhat satisfied	131 (32.75%)	611 (47.18%)
Dissatisfied	36 (9%)	107 (8.26%)
Very dissatisfied	9 (2.25%)	31 (2.39%)
Does not apply	32 (8%)	90 (6.95%)
Don't know / Refused	6 (1.5%)	27 (2.08%)

Table 8: Seattle as a place to retire

	Phone Survey	Web Survey
Very satisfied	122 (30.5%)	179 (13.82%)
Somewhat satisfied	132 (33%)	317 (24.48%)
Dissatisfied	73 (18.25%)	243 (18.76%)
Very dissatisfied	43 (10.75%)	185 (14.29%)
Does not apply	16 (4%)	333 (25.71%)
Don't know / Refused	14 (3.5%)	38 (2.93%)

Question 3 — In comparison to other neighborhoods in the city, how do you rate your neighborhood's availability of City services, such as libraries, parks and recreation facilities?

	Phone Survey	Web Survey
Very good	235 (58.75%)	511 (39.46%)
Good	105 (26.25%)	456 (35.21%)
Fair	43 (10.75%)	217 (16.76%)
Poor	14 (3.5%)	69 (5.33%)
Don't know / Refused	3 (0.75%)	42 (3.24%)

Question 4 — Please state whether you strongly agree, somewhat agree, somewhat disagree or strongly disagree with the following statements: My neighborhood is a healthy place to live.

	Phone Survey	Web Survey
Strongly agree	207 (51.75%)	405 (31.27%)
Somewhat agree	147 (36.75%)	588 (45.41%)
Somewhat disagree	33 (8.25%)	188 (14.52%)
Strongly disagree	9 (2.25%)	56 (4.32%)
Don't know / Refused	4 (1%)	58 (4.48%)

Question 5 — Please state whether… : I have benefited from Seattle's environmental progress.

	Phone Survey	Web Survey
Strongly agree	108 (27%)	312 (24.09%)
Somewhat agree	174 (43.5%)	560 (43.24%)
Somewhat disagree	56 (14%)	146 (11.27%)
Strongly disagree	35 (8.75%)	55 (4.25%)
Don't know / Refused	27 (6.75%)	222 (17.14%)

Question 6 — Please state whether… : To what extent do you agree that Seattle has offered good opportunities for you to get ahead economically?

	Phone Survey	WebSurvey
Strongly agree	120 (30%)	238 (18.38%)
Somewhat agree	128 (32%)	451 (34.83%)
Somewhat disagree	69 (17.25%)	278 (21.47%)
Strongly disagree	56 (14%)	229 (17.68%)
Don't know / Refused	27 (6.75%)	99 (7.64%)

Question 7 — Please state whether… : And over the last two years do you think Seattle has gotten better, stayed the same, or gotten worse in terms of providing you with opportunities to get ahead economically?

	Phone Survey	Web Survey
Gotten better	171 (42.75%)	191 (14.75%)
Stayed the same	91 (22.75%)	429 (33.13%)
Gotten worse	108 (27%)	517 (39.92%)
Refused	3 (0.75%)	18 (1.39%)
Don't know	27 (6.75%)	140 (10.81%)

Question 8 — How often does your family have money left after paying your monthly bills?

	Phone Survey	Web Survey
Often	199 (49.75%)	503 (39.39%)
Sometimes	84 (21%)	245 (19.19%)
Occasionally	53 (13.25%)	297 (23.26%)
Never	56 (14%)	216 (16.91%)
Refused	8 (2%)	16 (1.25%)

Question 9 — How do you rate Seattle's housing affordability?

	Phone Survey	Web Survey
Very good	18 (4.5%)	8 (0.63%)
Good	46 (11.5%)	39 (3.06%)
Only fair	125 (31.25%)	246 (19.28%)
Poor	205 (51.25%)	962 (75.39%)
Refused	6 (1.5%)	21 (1.65%)

Question 10 — How likely is it that you will be able to afford to live in Seattle in five years?

	Phone Survey	Web Survey
Highly likely	164 (41%)	221 (17.29%)
Likely	101 (25.25%)	365 (28.56%)
Not very likely	71 (17.75%)	325 (25.43%)
Unlikely	55 (13.75%)	283 (22.14%)
Don't know / Refused	9 (2.25%)	84 (6.57%)

Question 11 — Have you or someone in your family moved out of Seattle in the past two years due to the rising cost of housing?

	Phone Survey	Web Survey
Yes	76 (19%)	498 (39.21%)
No	324 (81%)	680 (53.54%)
Refused	0 (0%)	92 (7.24%)

Question 12 — If you have moved in that last two years, which of the following describes your move? (Select all that apply)

	Phone Survey	Web Survey
Stayed in the same zip code	43 (10.75%)	148 (11.43%)
Moved out of Seattle	35 (8.75%)	113 (8.73%)
Moved into Seattle	18 (4.5%)	149 (11.51%)
Does not apply	304 (76%)	885 (68.34%)

Question 13 — And what were the main reasons you moved? (Select top two reasons)

	Phone Survey	Web Survey
New job or job transfer	12 (10.53%)	71
To be closer to work/school/other	5 (4.39%)	104
To establish own household	6 (5.26%)	53
Needed a larger house or apartment	4 (3.51%)	65
Married, widowed, divorced, or separated	5 (4.39%)	30
Other, family/personal related	4 (3.51%)	73
Wanted a better quality house or apartment	8 (7.02%)	94
Change from owner to renter OR renter to owner	1 (0.88%)	65
Wanted lower rent or less expensive house to maintain	21 (18.42%)	11
Evicted from residence	1 (0.88%)	11
Foreclosure	0 (0%)	2
Medical debt	1 (0.88%)	7
The property was being redeveloped	0 (0%)	28
Disaster loss (fire, flood, etc.)	0 (0%)	1
To be closer to cultural amenities and art	0 (0%)	40
Other	41 (35.96%)	91
Refused	5 (4.39%)	644
N	114	1541
Total Respondents	96	1130

Question 14 — What do you like most about where you live? (Please select your top two from the list)

	Phone Survey	Web Survey
Access to public transit	118 (19.44%)	581
Affordable rent/mortgage	22 (3.62%)	289
Near people who share my culture	71 (11.7%)	220
Easy to get to my job	58 (9.56%)	422
Quality of schools	32 (5.27%)	123
Safety	43 (7.08%)	231
Quality of apartment or house	51 (8.4%)	351
Access to art and culture	91 (14.99%)	301
Other	106 (17.46%)	278
None	15 (2.47%)	43
N	607	2779
Total Respondents	400	1276

Question 15 — How likely do you think it is that your cultural center, place of worship, or gathering place will be located in Seattle in five years?

	Phone Survey	Web Survey
Highly likely	193 (48.25%)	320 (24.71%)
Somewhat Likely	92 (23%)	313 (24.17%)
Not very likely	32 (8%)	187 (14.44%)
Unlikely	37 (9.25%)	141 (10.89%)
Don't know / Refused	46 (11.5%)	334 (25.79%)

Question 16 — Please state whether you strongly agree, somewhat agree, somewhat disagree, or strongly disagree with the following statements. The City of Seattle's public investments (transportation, utilities, etc) have created housing affordability problems in certain neighborhoods.

	Phone Survey	Web Survey
Strongly agree	153 (38.25%)	458 (35.37%)
Somewhat agree	118 (29.5%)	322 (24.86%)
Somewhat disagree	46 (11.5%)	144 (11.12%)
Strongly disagree	40 (10%)	105 (8.11%)
Don't know / Refused	43 (10.75%)	266 (20.54%)

Question 17 — Please state whether... : The City of Seattle is doing enough to ensure people can afford to stay living in Seattle.

	Phone Survey	Web Survey
Strongly agree	21 (5.25%)	38 (2.93%)
Somewhat agree	74 (18.5%)	90 (6.95%)
Somewhat disagree	104 (26%)	326 (25.17%)
Strongly disagree	180 (45%)	747 (57.68%)
Don't know / Refused	21 (5.25%)	94 (7.26%)

Question 18 — Please state whether... : I feel like I can rely on public transportation to get where I need to go in a reasonable amount of time.

	Phone Survey	Web Survey
Strongly agree	97 (24.25%)	142 (10.97%)
Somewhat agree	121 (30.25%)	508 (39.23%)
Somewhat disagree	63 (15.75%)	313 (24.17%)
Strongly disagree	96 (24%)	283 (21.85%)
Don't know / Refused	23 (5.75%)	49 (3.78%)

Question 19 — Please state whether... : How do you rate Seattle in terms of ability to get around by public transportation?

	Phone Survey	Web Survey
Very good	84 (21%)	113 (8.73%)
Good	116 (29%)	348 (26.87%)
Only fair	130 (32.5%)	517 (39.92%)
Poor	58 (14.5%)	275 (21.24%)
Refused	12 (3%)	42 (3.24%)

Question 20 — Please state whether... : And over the last two years, do you think Seattle has gotten better, stayed the same, or gotten worse in terms of access to public transportation?

	Phone Survey	Web Survey
Gotten better	137 (34.25%)	336 (25.95%)
Stayed the same	130 (32.5%)	444 (34.29%)
Gotten worse	121 (30.25%)	369 (28.49%)
Refused	12 (3%)	146 (11.27%)

Question 21 — Please state whether... : How do you rate Seattle in terms of your ability to access affordable health care?

	Phone Survey	Web Survey
Very good	111 (27.75%)	184 (14.21%)
Good	144 (36%)	462 (35.68%)
Fair	88 (22%)	328 (25.33%)
Poor	28 (7%)	129 (9.96%)
Don't know / Refused	29 (7.25%)	192 (14.83%)

Question 22 — And over the last two years, do you think Seattle has gotten better, stayed the same, or gotten worse in terms of access to affordable health care?

	Phone Survey	Web Survey
Gotten better	114 (28.5%)	191 (14.75%)
Stayed the same	172 (43%)	480 (37.07%)
Gotten worse	71 (17.75%)	175 (13.51%)
Refused	43 (10.75%)	449 (34.67%)

Question 23 — How do you rate Seattle's public schools?

	Phone Survey	Web Survey
Very good	33 (8.25%)	38 (2.93%)
Good	127 (31.75%)	265 (20.46%)
Fair	116 (29%)	316 (24.4%)
Poor	41 (10.25%)	184 (14.21%)
Don't know / Refused	83 (20.75%)	492 (37.99%)

Question 24 — And over the last two years, do you think Seattle has gotten better, stayed the same, or gotten worse in terms of public schools?

	Phone Survey	Web Survey
Gotten better	63 (15.75%)	72 (5.56%)
Stayed the same	178 (44.5%)	345 (26.64%)
Gotten worse	81 (20.25%)	247 (19.07%)
Refused	78 (19.5%)	631 (48.73%)

Question 25. Please state whether…: Shifting from punitive discipline measures in Seattle Public Schools to measures that address harm and repair relationships is important to making sure all students, regardless of their race, receive fair and just treatment.

	Phone Survey	WebSurvey
Strongly agree	183 (45.75%)	802 (61.93%)
Somewhat agree	127 (31.75%)	191 (14.75%)
Somewhat disagree	20 (5%)	47 (3.63%)
Strongly disagree	26 (6.5%)	33 (2.55%)
Don't know / Refused	44 (11%)	222 (17.14%)

Question 26 — Please state whether… : Staff and teachers at Seattle Public Schools treat students of color with as much respect as white students.

	Phone Survey	WebSurvey
Strongly agree	73 (18.25%)	83 (6.41%)
Somewhat agree	116 (29%)	133 (10.27%)
Somewhat disagree	58 (14.5%)	263 (20.31%)
Strongly disagree	30 (7.5%)	228 (17.61%)
Don't know / Refused	123 (30.75%)	588 (45.41%)

Question 27 — Please state whether… : Seattle Public Schools are preparing students well for the future.

	Phone Survey	WebSurvey
Strongly agree	38 (9.5%)	36 (2.78%)
Somewhat agree	169 (42.25%)	287 (22.16%)
Somewhat disagree	68 (17%)	274 (21.16%)
Strongly disagree	48 (12%)	154 (11.89%)
Don't know / Refused	77 (19.25%)	544 (42.01%)

Question 28 — How much confidence do you have in police officers in your community to do a good job of enforcing the law?

	Phone Survey	Web Survey
A great deal of confidence	99 (24.75%)	94 (7.26%)
A fair amount of confidence	213 (53.25%)	605 (46.72%)
No confidence	20 (5%)	116 (8.96%)
Refused	2 (0.5%)	89 (6.87%)

Question 29 — How much confidence do you have in police officers in your community to treat Black people and white people equally?

	Phone Survey	Web Survey
A great deal of confidence	55 (13.75%)	54 (4.17%)
A fair amount of confidence	177 (44.25%)	249 (19.23%)
Little confidence	110 (27.5%)	531 (41%)
No confidence	46 (11.5%)	324 (25.02%)
Refused	12 (3%)	137 (10.58%)

Question 30 — And what about people of color in general, how much confidence do you have in police officers in your community to treat people of color and white people equally?

	Phone Survey	Web Survey
A great deal of confidence	77 (19.25%)	50 (3.86%)
A fair amount of confidence	171 (42.75%)	267 (20.62%)
Little confidence	99 (24.75%)	543 (41.93%)
No confidence	37 (9.25%)	295 (22.78%)
Refused	16 (4%)	140 (10.81%)

Question 31 — How much confidence do you have in the courts treating people of color and white people equally?

	Phone Survey	Web Survey
A great deal of confidence	66 (16.5%)	59 (4.56%)
A fair amount of confidence	171(42.75%)	239 (18.46%)
No confidence	39 (9.75%)	328 (25.33%)
Refused	18 (4.5%)	146 (11.27%)

Question 32 — Have you ever been questioned by the police, charged, or arrested when you had not committed a crime?

	Phone Survey	Web Survey
Yes	74 (18.5%)	270 (20.85%)
No	326 (81.5%)	993 (76.68%)
Refused	0 (0%)	32 (2.47%)

Question 33 — Have you or a family member ever experienced incarceration (jail, prison, juvenile detention)?

	Phone Survey	Web Survey
Myself	33 (8.25%)	69 (5.33%)
Family member	53 (13.25%)	327 (25.25%)
Both	—	46 (3.55%)
Neither	313 (78.25%)	821 (63.4%)
Refused	1 (0.25%)	32 (2.47%)

Question 34 — Which of the following should the City prioritize to reduce racial disproportionality in the criminal justice system? [Select top three]

	Phone Survey	Web Survey
Better schools and after school programs	233 (22.47%)	577
Ending out of school suspensions and expulsions	94 (9.06%)	356
Requiring anti-bias training for police and courts	171 (16.49%)	610
Family wage jobs	110 (10.61%)	429
Better mental health services	114 (10.99%)	450
More affordable housing	71 (6.85%)	472
More parks and community centers	36 (3.47%)	127
Community-based alternatives to arrest and detention	70 (6.75%)	597
Restorative justice	30 (2.89%)	394
More police of color	72 (6.94%)	270
Other	13 (1.25%)	67
Don't know	23 (2.22%)	45
N	1037	4411
Total Respondents	400	1274

Question 35 — In the last 12 months, did you or a member of your immediate household experience discrimination, were refused services or treated unfairly because of: [Select all that apply]

	Phone Survey	Web Survey
Race or Color	32 (13.39%)	236 (19.81%)
Disability	21 (8.79%)	86 (7.22%)
Sexual orientation	10 (4.18%)	70 (5.88%)
National origin	10 (4.18%)	40 (3.36%)
Religion	15 (6.28%)	35 (2.94%)
Gender	19 (7.95%)	192 (16.12%)
Gender Identity	6 (2.51%)	64 (5.37%)
Marital status	12 (5.02%)	35 (2.94%)
Because children live in your household	11 (4.6%)	34 (0.03%)
Age	52 (21.76%)	145 (12.17%)
Veteran or military status	5 (2.09%)	11 (.01%)
A prior juvenile or criminal record	8 (3.35%)	32 (2.85%)
Credit history	20 (8.37%)	110 (9.2%)
Use of a Section 8 Housing Voucher	4 (1.67%)	11 (0.92%)
Breastfeeding in a public place	6 (2.51%)	14 (1.18%)
Other reason	8 (3.35%)	73 (6.13%)
N	239	1191
Total Respondents	113	528

Question 36 — If you said "Yes" to at least one item in the previous question, please check the box for each area that you or a member of your immediate household experienced discrimination or unfair treatment with: [Select all that apply]

	Phone Survey	Web Survey
Employment	36 (18%)	192 (18.32%)
Rental housing	18 (9%)	105 (10.02%)
Home ownership	3 (1.5%)	41 (3.91%)
Utility services	9 (4.5%)	25 (2.39%)
Law enforcement and policing	24 (12%)	110 (10.50%)
Consumer, financial services and credit	23 (11.5%)	106 (10.11%)
Health care	14 (7%)	108 (10.31%)
Access to governmental assistance, programs or services	10 (5%)	83 (7.92%)
Education	17 (8.5%)	86 (8.21%)
Private business	22 (11%)	147 (14.03%)
None	24 (12%)	46 (4.39%)
N	200	1048
Total Respondents	113	527

Question 37 — The City of Seattle conducts outreach and engagement on many projects and policies. Are you aware of such outreach, or is this your first time hearing about it?

	Phone Survey	Web Survey
Aware	195 (48.75%)	667 (51.51%)
First time hearing about it	202 (50.5%)	595 (45.95%)
Refused	3 (0.75%)	33 (2.55%)

Question 38 — Have you participated?

	Phone Survey	Web Survey
Yes	69 (35.38%)	342 (26.41%)
No	126 (64.62%)	907 (70.04%)
N	195	1249

Question 39 — If you participated, did you feel your participation was valued?

	Phone Survey	Web Survey
A great deal	13 (18.84%)	38 (2.93%)
A fair amount	24 (34.78%)	85 (6.56%)
Just some	17 (24.64%)	137 (10.58%)
Very little	5 (7.25%)	80 (6.18%)
None	7 (10.14%)	26 (2.01%)
Refused	3 (4.35%)	929 (71.74%)
N	69	1295

Question 40 — How would you rate race relations in Seattle?

	Phone Survey	Web Survey
Very good	42 (10.5%)	28 (2.16%)
Good	143 (35.75%)	234 (18.07%)
Only fair	175 (43.75%)	665 (51.35%)
Poor	31 (7.75%)	290 (22.39%)
Refused	9 (2.25%)	78 (6.02%)

Question 41 — And over the last two years, do you think Seattle has gotten better, stayed the same, or gotten worse in terms of race relations?

	Phone Survey	Web Survey
Gotten better	101 (25.25%)	161 (12.43%)
Stayed the same	212 (53%)	714 (55.14%)
Gotten worse	70 (17.5%)	360 (27.8%)
Refused	17 (4.25%)	60 (4.63%)

Question 42 — How high of a priority should it be for government to address the racial equity gaps in education, criminal justice, jobs, health, housing and other areas?

	Phone Survey	Web Survey
High priority	254 (63.5%)	989 (76.37%)
Somewhat of a priority	117 (29.25%)	196 (15.14%)
Not a priority	20 (5%)	45 (3.47%)
Refused	9 (2.25%)	65 (5.02%)

Question 43 — Please state whether… : To create equity and opportunity for all, I believe a greater portion of resources should go to those who are most in need.

	Phone Survey	WebSurvey
Strongly agree	215 (53.75%)	813 (62.78%)
Somewhat agree	133 (33.25%)	329 (25.41%)
Somewhat disagree	27 (6.75%)	51(3.94%)
Strongly disagree	17 (4.25%)	32 (2.47%)
Don't know / Refused	8 (2%)	70(5.41%)

Question 44 — Please state whether… : In Seattle we are making progress in eliminating racial inequities and creating a city where social, economic and political opportunities and outcomes are not predicted based upon a person's race.

	Phone Survey	WebSurvey
Strongly agree	78 (19.5%)	83 (6.41%)
Somewhat agree	211 (52.75%)	470 (36.29%)
Somewhat disagree	62 (15.5%)	353 (27.26%)
Strongly disagree	32 (8%)	200 (15.44%)
Don't know / Refused	17(4.25%)	189 (14.59%)

Question 45 — Please state whether... : Compared with five years ago, do you think there is a wider gap or a narrower gap between African American residents and White residents in terms of average incomes?

	Phone Survey	Web Survey
Wider gap	180 (45%)	693 (53.51%)
Narrower gap	71 (17.75%)	87 (6.72%)
About the same	67 (16.75%)	169 (13.05%)
Don't know / Refused	82 (20.5%)	346 (26.72%)

Question 46 — Which of the following have you done over the last year? (select all that apply)

	Phone Survey	Web Survey
Voted in an election	348 (25.4%)	1113
Signed a petition	252 (18.39%)	949
Organized neighbors or community members on an issue	83 (6.06%)	353
Joined a community organization or faith-based group to g...	137 (10%)	506
Written or spoken to a local elected official	179 (13.07%)	621
Attended a protest, march or demonstration	85 (6.2%)	502
Given money or volunteered time to support a community or...	266 (19.42%)	978
None of the above	20 (1.46%)	49
N	1370	5071
Total Respondents	400	1260

Question 47 — What do you think is the most important problem facing your community today?

	Phone Survey
Crime	32 (8%)
Development Impacts	19 (4.75%)
Education	23 (5.75%)
Employment	1 (0.25%)
Environment	8 (2%)
Healthcare	3 (0.75%)
Homelessness	30 (7.5%)
Housing	72 (18%)
Inequality	66 (16.5%)
Neighborhood Quality	2 (0.5%)
None	15 (3.75%)
Other	81 (20.25%)
Police brutality	1 (0.25%)
Traffic / Infrastructure	47 (11.75%)

Question 48 — What is your gender?

	Phone Survey	Web Survey
Female	223 (55.75%)	854 (65.95%)
Male	174 (43.5%)	330 (25.48%)
Transgender	0 (0%)	5 (0.39%)
Genderqueer/Gender non-conforming	0 (0%)	29 (2.24%)
Other (SPECIFY)	1 (0.25%)	26 (2.01%)
Refused	2 (0.5%)	51 (3.94%)

Question 49 — How do you identify yourself by race or ethnicity?

	Phone Survey	Web Survey
American Indian / Alaska Native	3 (0.75%)	36 (2.78%)
Asian American	24 (6%)	83 (6.41%)
Pacific Islander	5 (1.25%)	3 (0.23%)
Black / African American	33 (8.25%)	93 (7.18%)
Hispanic / Latino	11 (2.75%)	63 (4.86%)
Middle Eastern	2 (0.5%)	1 (0.08%)
White, non-Hispanic	273 (68.25%)	772 (59.61%)
Multiracial	26 (6.5%)	131 (10.12%)
Other (SPECIFY)	10 (2.5%)	55 (4.25%)
Refused	13 (3.25%)	58 (4.48%)

Question 50 — Were you born in the United States or another country?

	Phone Survey	WebSurvey
United States	351 (87.75%)	1121 (86.56%)
Another country	43 (10.75%)	119 (9.19%)
Refused	6 (1.5%)	55 (4.25%)

If responding another country:

	Phone Survey
Africa	1 (2.22%)
Argentina	1 (2.22%)
Australia	1 (2.22%)
Austria	1 (2.22%)
Barbados	1 (2.22%)
Canada	6 (13.33%)
China	1 (2.22%)
Cuba	1 (2.22%)
England	2 (4.44%)
Germany	6 (13.33%)
Great Britain	1 (2.22%)
Hong Kong	1 (2.22%)
Indonesia	1 (2.22%)
Japan	3 (6.67%)
Limerick, Ireland	1 (2.22%)
Mexico	1 (2.22%)
Netherlands	1 (2.22%)
Nigeria	1 (2.22%)
None of my business.	1 (2.22%)
Norway	1 (2.22%)
Panama	2 (4.44%)
Philippines	1 (2.22%)
Refused	1 (2.22%)
Scandinavian	1 (2.22%)
Seoul, South Korea	1 (2.22%)
Sweden	1 (2.22%)
Swiss	1 (2.22%)
The Netherlands	1 (2.22%)
UK	1 (2.22%)
United Kingdom	2 (4.44%)
N	45

Question 51 — Were your parents born in the United States or in another country?

	Phone Survey	Web Survey
Both parents born in the United States	281 (70.25%)	924 (71.35%)
Both parents born in another country	73 (18.25%)	190 (14.67%)
1 parent born in the US, 1 born in another country	39 (9.75%)	124 (9.58%)
Refused	7 (1.75%)	57 (4.4%)

Question 52 — What is your sexual orientation?

	Phone Survey	Web Survey
Straight	327 (81.75%)	926 (71.51%)
Lesbian	10 (2.5%)	33 (2.55%)
Gay	11 (2.75%)	36 (2.78%)
Bisexual	7 (1.75%)	87 (6.72%)
Queer	1 (0.25%)	74 (5.71%)
Other	17 (4.25%)	62 (4.79%)
Refused	27 (6.75%)	77 (5.95%)

Question 53 — Are you a person with a disability?

	Phone Survey	WebSurvey
Yes	75 (18.75%)	152 (11.74%)
No	318 (79.5%)	1083 (83.63%)
Refused	7 (1.75%)	60 (4.63%)

Question 54 — What is your housing situation?

	Phone Survey	Web Survey
Own	274 (68.5%)	585 (45.17%)
Rent	98 (24.5%)	556 (42.93%)
Transitional housing	0 (0%)	3 (0.23%)
Homeless / shelter	0 (0%)	21 (1.62%)
Live with someone	12 (3%)	49 (3.78%)
Other	8 (2%)	26 (2.01%)
Refused	8 (2%)	55 (4.25%)

Question 55 — How many people live in your household?

	Phone Survey	Web Survey
1	127 (31.75%)	243 (18.76%)
2	136 (34%)	496 (38.3%)
3	50 (12.5%)	239 (18.46%)
4	45 (11.25%)	174 (13.44%)
5 or more	29 (7.25%)	83 (6.41%)
Refused	13 (3.25%)	60 (4.63%)

Question 56 — How many children under the age of 18 live in your household?

	Phone Survey	Web Survey
0	164 (63.08%)	893 (68.96%)
1	49 (18.85%)	173 (13.36%)
2	37 (14.23%)	123 (9.5%)
3	8 (3.08%)	30 (2.32%)
4	1 (0.38%)	5 (0.39%)
5 or more	0 (0%)	2 (0.15%)
Refused	1 (0.38%)	69 (5.33%)

Question 57 — What is your zip code?

	Phone Survey
98004	1 (0.25%)
98018	1 (0.25%)
98026	1 (0.25%)
98031	2 (0.5%)
98038	1 (0.25%)
98055	1 (0.25%)
98057	1 (0.25%)
98077	1 (0.25%)
98101	7 (1.75%)
98102	10 (2.5%)
98103	23 (5.75%)
98104	3 (0.75%)
98105	16 (4%)
98106	8 (2%)
98107	12 (3%)
98108	5 (1.25%)
98109	8 (2%)
98112	9 (2.25%)
98114	1 (0.25%)
98115	36 (9%)
98116	16 (4%)
98117	11 (2.75%)
98118	23 (5.75%)
98119	17 (4.25%)
98121	2 (0.5%)
98122	15 (3.75%)
98125	32 (8%)
98126	16 (4%)
98133	13 (3.25%)
98136	16 (4%)
98139	1 (0.25%)
98144	18 (4.5%)
98145	1 (0.25%)
98146	7 (1.75%)
98148	1 (0.25%)
98155	6 (1.5%)
98166	2 (0.5%)
98168	7 (1.75%)
98177	4 (1%)
98178	15 (3.75%)
98188	2 (0.5%)
98199	11 (2.75%)
98223	1 (0.25%)
98275	1 (0.25%)
99999	15 (3.75%)

Question 58 — Is your age between:

	Phone Survey	Web Survey
15 and 25	15 (3.75%)	85 (6.56%)
26 and 35	24 (6%)	370 (28.57%)
36 and 50	72 (18%)	395 (30.50%)
51 and 64	140 (35%)	243 (18.76%)
65 year of age or older	143 (35.75%)	141 (10.88%)
Refused	6 (1.5%)	61 (4.71%)

Question 59 — What is the highest level of education you have completed?

	Phone Survey	Web Survey
Grade school or some high school	7 (1.75%)	29 (2.24%)
High school graduate	33 (8.25%)	26 (2.01%)
Some college, technical, vocational or two year degree	95 (23.75%)	212 (16.37%)
Four year college graduate	116 (29%)	380 (29.34%)
Post graduate work or graduate degree	141 (35.25%)	589 (45.48%)
Refused	8 (2%)	59 (4.56%)

Question 60 — How long have you lived, worked or gone to school in Seattle?

	Phone Survey	Web Survey
One year or less	15 (3.75%)	63 (4.86%)
1 to 2 years	—	71 (5.48%)
2 to 5 years	25 (6.25%)	164 (12.66%)
5 to 10 years	23 (5.75%)	187 (14.44%)
10 years or more	328 (82%)	756 (58.38%)
Refused	9 (2.25%)	54 (4.17%)

Question 61 — What is your current employment status?

	Phone Survey	Web Survey
Employed full time	150 (37.5%)	642 (49.58%)
Employed part time	32 (8%)	133 (10.27%)
Self employed	36 (9%)	90 (6.95%)
Currently unemployed	38 (9.5%)	63 (4.86%)
Student	3 (0.75%)	63 (4.86%)
Other	132 (33%)	249 (19.23%)
Refused	9 (2.25%)	55 (4.25%)

Question 62 — When it comes to politics, do you usually think of yourself as a Liberal, a Conservative, a Moderate, or have you not thought about it much?

	Phone Survey	Web Survey
Liberal	207 (51.75%)	808 (62.39%)
Conservative	42 (10.5%)	25 (1.93%)
Moderate	60 (15%)	158 (12.2%)
Haven't thought about it much	47 (11.75%)	65 (5.02%)
Other (SPECIFY)	29 (7.25%)	171 (13.2%)
Refused	15 (3.75%)	68 (5.25%)

Table 9: If responding other to Q62:

	Phone Survey
Always vote for the best candidate and independently.	1 (3.33%)
Democrat	3 (10%)
Democratic Socialist	1 (3.33%)
I don't agree with politics at all.	1 (3.33%)
In between conservative and liberal.	1 (3.33%)
Independent	14 (46.67%)
Liberal and moderate.	1 (3.33%)
Liberal in the classical sense, as in liberal education.	1 (3.33%)
Progressive	4 (13.33%)
Radical	1 (3.33%)
Socialist Party	1 (3.33%)
Sometimes depends on candidate or election, won't lump myself in one.	1 (3.33%)
N	30

	Phone Survey	Web Survey
Less than $20,000	38 (9.5%)	141 (10.89%)
$20,000 to less than $40,000	46 (11.5%)	149 (11.51%)
$40,000 to less than $60,000	43 (10.75%)	198 (15.29%)
$60,000 to less than $75,000	37 (9.25%)	151 (11.66%)
$75,000 to less than $100,000	54 (13.5%)	157 (12.12%)
$100,000 to less than $150,000	43 (10.75%)	219 (16.91%)
$150,000 to less than $200,000	19 (4.75%)	97 (7.49%)
$200,000 or above	38 (9.5%)	77 (5.95%)
Refused	82 (20.5%)	106 (8.19%)

Question 64 — If you live in Seattle, what is your City Council district?

	Phone Survey	Web Survey
District 1	24 (6%)	82 (6.82%)
District 2	5 (1.25%)	97 (8.06%)
District 3	15 (3.75%)	141 (11.72%)
District 4	13 (3.25%)	71 (5.9%)
District 5	13 (3.25%)	53 (4.41%)
District 6	10 (2.5%)	94 (7.81%)
District 7	20 (5%)	64 (5.32%)
Don't know	278 (69.5%)	470 (39.07%)
Does not apply / Don't live in Seattle	22 (5.5%)	131 (10.89%)

Chapter Listing

Chapter 10.97 RCW

WASHINGTON STATE CRIMINAL RECORDS PRIVACY ACT

Sections

10.97.010	Declaration of policy.
10.97.020	Short title.
10.97.030	Definitions.
10.97.040	Information required—Exceptions.
10.97.045	Disposition data to initiating agency and state patrol.
10.97.050	Restricted, unrestricted information—Records.
10.97.060	Deletion of certain information, conditions.
10.97.070	Disclosure of suspect's identity to victim.
10.97.080	Inspection of information by subject—Challenges and corrections.
10.97.090	Administration by state patrol.
10.97.100	Fees.
10.97.110	Civil remedies—Criminal prosecution not affected.
10.97.120	Criminal penalties—Civil action not affected.
10.97.130	Child victims of sexual assaults, identification confidential.
10.97.140	Construction.

NOTES:

*Public records: Chapter **42.56** RCW.*

*Records of community sexual assault program and underserved populations provider not available as part of discovery: RCW **70.125.065**.*

10.97.010
Declaration of policy.

The legislature declares that it is the policy of the state of Washington to provide for the completeness, accuracy, confidentiality, and security of criminal history record information and victim, witness, and complainant record information as defined in this chapter.

[1977 ex.s. c 314 § 1.]

10.97.020
Short title.

This chapter may be cited as the Washington State Criminal Records Privacy Act.

[**1977 ex.s. c 314 § 2.**]

NOTES:

Reviser's note: The phrase "This 1977 amendatory act" has been changed to "This chapter." This 1977 amendatory act [1977 ex.s. c 314] consists of chapter **10.97** RCW and the amendments of RCW **42.17.310**, **43.43.705**, **43.43.710**, **43.43.730**, and **43.43.810**.

10.97.030
Definitions.

For purposes of this chapter, the definitions of terms in this section shall apply.

(1) "The administration of criminal justice" means performance of any of the following activities: Detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The term also includes criminal identification activities and the collection, storage, dissemination of criminal history record information, and the compensation of victims of crime.

(2) "Conviction or other disposition adverse to the subject" means any disposition of charges other than: (a) A decision not to prosecute; (b) a dismissal; or (c) acquittal; with the following exceptions, which shall be considered dispositions adverse to the subject: An acquittal due to a finding of not guilty by reason of insanity and a dismissal by reason of incompetency, pursuant to chapter **10.77** RCW; and a dismissal entered after a period of probation, suspension, or deferral of sentence.

(3) "Conviction record" means criminal history record information relating to an incident which has led to a conviction or other disposition adverse to the subject.

(4) "Criminal history record information" means information contained in records collected by criminal justice agencies, other than courts, on individuals, consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, including acquittals by reason of insanity, dismissals based on lack of competency, sentences, correctional supervision, and release.

The term includes any issued certificates of restoration of opportunities and any information contained in records maintained by or obtained from criminal justice agencies, other than courts, which records provide individual identification of a person together with any portion of the individual's record of involvement in the criminal justice system as an alleged or convicted offender, except:

(a) Posters, announcements, or lists for identifying or apprehending fugitives or wanted persons;

(b) Original records of entry maintained by criminal justice agencies to the extent that such records are compiled and maintained chronologically and are accessible only on a chronological basis;

(c) Court indices and records of public judicial proceedings, court decisions, and opinions, and information disclosed during public judicial proceedings;

(d) Records of traffic violations which are not punishable by a maximum term of imprisonment of more than ninety days;

(e) Records of any traffic offenses as maintained by the department of licensing for the purpose of regulating the issuance, suspension, revocation, or renewal of drivers' or other operators' licenses and pursuant to RCW **46.52.130**;

(f) Records of any aviation violations or offenses as maintained by the department of transportation for the purpose of regulating pilots or other aviation operators, and pursuant to RCW **47.68.330**;

(g) Announcements of executive clemency;

(h) Intelligence, analytical, or investigative reports and files.

(5) "Criminal justice agency" means: (a) A court; or (b) a government agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice.

(6) "Disposition" means the formal conclusion of a criminal proceeding at whatever stage it occurs in the criminal justice system.

(7) "Dissemination" means disclosing criminal history record information or disclosing the absence of criminal history record information to any person or agency outside the agency possessing the information, subject to the following exceptions:

(a) When criminal justice agencies jointly participate in the maintenance of a single recordkeeping department as an alternative to maintaining separate records, the furnishing of information by that department to personnel of any participating agency is not a dissemination;

(b) The furnishing of information by any criminal justice agency to another for the purpose of processing a matter through the criminal justice system, such as a police department providing information to a prosecutor for use in preparing a charge, is not a dissemination;

(c) The reporting of an event to a recordkeeping agency for the purpose of maintaining the record is not a dissemination.

(8) "Nonconviction data" consists of all criminal history record information relating to an incident which has not led to a conviction or other disposition adverse to the subject, and for which proceedings are no longer actively pending. There shall be a rebuttable presumption that proceedings are no longer actively pending if more than one year has elapsed since arrest, citation, charge, or service of warrant and no disposition has been entered.

[2016 c 81 § 4; 2012 c 125 § 1; 1999 c 49 § 1; 1998 c 297 § 49; 1990 c 3 § 128; 1979 ex.s. c 36 § 1; 1979 c 158 § 5; 1977 ex.s. c 314 § 3.]

NOTES:

Reviser's note: The definitions in this section have been alphabetized pursuant to RCW **1.08.015**(2)(k).

Finding—Conflict with federal requirements—2016 c 81: See notes following RCW 9.97.010.

Effective dates—Severability—Intent—1998 c 297: See notes following RCW 71.05.010.

Index, part headings not law—Severability—Effective dates—Application—1990 c 3: See RCW 18.155.900 through 18.155.902.

10.97.040
Information required—Exceptions.

No criminal justice agency shall disseminate criminal history record information pertaining to an arrest, detention, indictment, information, or other formal criminal charge made after December 31, 1977, unless the record disseminated states the disposition of such charge to the extent dispositions have been made at the time of the request for the information: PROVIDED, HOWEVER, That if a disposition occurring within ten days immediately preceding the dissemination has not been reported to the agency disseminating the criminal history record information, or if information has been received by the agency within the seventy-two hours immediately preceding the dissemination, that information shall not be required to be included in the dissemination: PROVIDED FURTHER, That when another criminal justice agency requests criminal history record information, the disseminating agency may disseminate specific facts and incidents which are within its direct knowledge without furnishing disposition data as otherwise required by this section, unless the disseminating agency has received such disposition data from either: (1) the state patrol, or (2) the court or other criminal justice agency required to furnish disposition data pursuant to RCW 10.97.045.

No criminal justice agency shall disseminate criminal history record information which shall include information concerning a felony or gross misdemeanor without first making inquiry of the identification section of the Washington state patrol for the purpose of obtaining the most current and complete information available, unless one or more of the following circumstances exists:

(1) The information to be disseminated is needed for a purpose in the administration of criminal justice for which time is of the essence and the identification section is technically or physically incapable of responding within the required time;

(2) The full information requested and to be disseminated relates to specific facts or incidents which are within the direct knowledge of the agency which disseminates the information;

(3) The full information requested and to be disseminated is contained in a criminal history record information summary received from the identification section by the agency which is to make the dissemination not more than thirty days preceding the dissemination to be made;

(4) The statute, executive order, court rule, or court order pursuant to which the information is to be disseminated refers solely to information in the files of the agency which makes the dissemination;

(5) The information requested and to be disseminated is for the express purpose of research, evaluative, or statistical activities to be based upon information maintained in the files of the agency or agencies from which the information is directly sought; or

(6) A person who is the subject of the record requests the information and the agency complies with the requirements in RCW 10.97.080 as now or hereafter amended.

[1979 ex.s. c 36 § 2; 1977 ex.s. c 314 § 4.]

10.97.045
Disposition data to initiating agency and state patrol.

Whenever a court or other criminal justice agency reaches a disposition of a criminal proceeding, the court or other criminal justice agency shall furnish the disposition data to the agency initiating the criminal history record for that charge and to the identification section of the Washington state patrol as required under RCW 43.43.745.

[1979 ex.s. c 36 § 6.]

10.97.050
Restricted, unrestricted information—Records.

(1) Conviction records may be disseminated without restriction.

(2) Any criminal history record information which pertains to an incident that occurred within the last twelve months for which a person is currently being processed by the criminal justice system, including the entire period of correctional supervision extending through final discharge from parole, when applicable, may be disseminated without restriction.

(3) Criminal history record information which includes nonconviction data may be disseminated by a criminal justice agency to another criminal justice agency for any purpose associated with the administration of criminal justice, or in connection with the employment of the subject of the record by a criminal justice or juvenile justice agency. A criminal justice agency may respond to any inquiry from another criminal justice agency without any obligation to ascertain the purpose for which the information is to be used by the agency making the inquiry.

(4) Criminal history record information which includes nonconviction data may be disseminated by a criminal justice agency to implement a statute, ordinance, executive order, or a court rule, decision, or order which expressly refers to records of arrest, charges, or allegations of criminal conduct or other nonconviction data and authorizes or directs that it be available or accessible for a specific purpose.

(5) Criminal history record information which includes nonconviction data may be disseminated to individuals and agencies pursuant to a contract with a criminal justice agency to provide services related to the administration of criminal justice. Such contract must specifically authorize access to criminal history record information, but need not specifically state that access to nonconviction data is included. The agreement must limit the use of the criminal history record information to stated purposes and insure the confidentiality and

security of the information consistent with state law and any applicable federal statutes and regulations.

(6) Criminal history record information which includes nonconviction data may be disseminated to individuals and agencies for the express purpose of research, evaluative, or statistical activities pursuant to an agreement with a criminal justice agency. Such agreement must authorize the access to nonconviction data, limit the use of that information which identifies specific individuals to research, evaluative, or statistical purposes, and contain provisions giving notice to the person or organization to which the records are disseminated that the use of information obtained therefrom and further dissemination of such information are subject to the provisions of this chapter and applicable federal statutes and regulations, which shall be cited with express reference to the penalties provided for a violation thereof.

(7) Every criminal justice agency that maintains and disseminates criminal history record information must maintain information pertaining to every dissemination of criminal history record information except a dissemination to the effect that the agency has no record concerning an individual. Information pertaining to disseminations shall include:

(a) An indication of to whom (agency or person) criminal history record information was disseminated;

(b) The date on which the information was disseminated;

(c) The individual to whom the information relates; and

(d) A brief description of the information disseminated.

The information pertaining to dissemination required to be maintained shall be retained for a period of not less than one year.

(8) In addition to the other provisions in this section allowing dissemination of criminal history record information, RCW **4.24.550** governs dissemination of information concerning offenders who commit sex offenses as defined by RCW **9.94A.030**. Criminal justice agencies, their employees, and officials shall be immune from civil liability for dissemination on criminal history record information concerning sex offenders as provided in RCW **4.24.550**.

[2012 c 125 § 2; 2005 c 421 § 9; 1990 c 3 § 129; 1977 ex.s. c 314 § 5.]

NOTES:

Index, part headings not law—Severability—Effective dates—Application—1990 c 3: See RCW **18.155.900** through **18.155.902**.

10.97.060
Deletion of certain information, conditions.

Criminal history record information which consists of nonconviction data only shall be subject to deletion from criminal justice agency files which are available and generally searched for the purpose of responding to inquiries concerning the criminal history of a named or otherwise identified individual when two years or longer have elapsed since the record became nonconviction data as a result of the entry of a disposition favorable to the defendant, or upon the passage of three years from the date of arrest or issuance of a citation or warrant

for an offense for which a conviction was not obtained unless the defendant is a fugitive, or the case is under active prosecution according to a current certification made by the prosecuting attorney.

Such criminal history record information consisting of nonconviction data shall be deleted upon the request of the person who is the subject of the record: PROVIDED, HOWEVER, That the criminal justice agency maintaining the data may, at its option, refuse to make the deletion if:

(1) The disposition was a deferred prosecution or similar diversion of the alleged offender;

(2) The person who is the subject of the record has had a prior conviction for a felony or gross misdemeanor;

(3) The individual who is the subject of the record has been arrested for or charged with another crime during the intervening period.

Nothing in this chapter is intended to restrict the authority of any court, through appropriate judicial proceedings, to order the modification or deletion of a record in a particular cause or concerning a particular individual or event.

[1977 ex.s. c 314 § 6.]

10.97.070
Disclosure of suspect's identity to victim.

(1) Criminal justice agencies may, in their discretion, disclose to persons who have suffered physical loss, property damage, or injury compensable through civil action, the identity of persons suspected as being responsible for such loss, damage, or injury together with such information as the agency reasonably believes may be of assistance to the victim in obtaining civil redress. Such disclosure may be made without regard to whether the suspected offender is an adult or a juvenile, whether charges have or have not been filed, or a prosecuting authority has declined to file a charge or a charge has been dismissed.

(2) Unless the agency determines release would interfere with an ongoing criminal investigation, in any action brought pursuant to this chapter, criminal justice agencies shall disclose identifying information, including photographs of suspects, if the acts are alleged by the plaintiff or victim to be a violation of RCW 9A.50.020.

(3) The disclosure by a criminal justice agency of investigative information pursuant to subsection (1) of this section shall not establish a duty to disclose any additional information concerning the same incident or make any subsequent disclosure of investigative information, except to the extent an additional disclosure is compelled by legal process.

[1993 c 128 § 10; 1977 ex.s. c 314 § 7.]

NOTES:

Effective date—1993 c 128: See RCW 9A.50.902.

10.97.080
Inspection of information by subject—Challenges and corrections.

All criminal justice agencies shall permit an individual who is, or who believes that he or she may be, the subject of a criminal record maintained by that agency, to appear in person during normal business hours of that criminal justice agency and request to see the criminal history record information held by that agency pertaining to the individual. The individual's right to access and review of criminal history record information shall not extend to data contained in intelligence, investigative, or other related files, and shall not be construed to include any information other than that defined as criminal history record information by this chapter.

Every criminal justice agency shall adopt rules and make available forms to facilitate the inspection and review of criminal history record information by the subjects thereof, which rules may include requirements for identification, the establishment of reasonable periods of time to be allowed an individual to examine the record, and for assistance by an individual's counsel, interpreter, or other appropriate persons.

No person shall be allowed to retain or mechanically reproduce any nonconviction data except for the person who is the subject of the record. Such person may retain a copy of their personal nonconviction data information on file, if the criminal justice agency has verified the identities of those who seek to inspect them. Criminal justice agencies may impose such additional restrictions, including fingerprinting, as are reasonably necessary both to assure the record's security and to verify the identities of those who seek to inspect them. The criminal justice agency may charge a reasonable fee for fingerprinting or providing a copy of the personal nonconviction data information pursuant to this section. The provisions of chapter 42.56 RCW shall not be construed to require or authorize copying of nonconviction data for any other purpose.

The Washington state patrol shall establish rules for the challenge of records which an individual declares to be inaccurate or incomplete, and for the resolution of any disputes between individuals and criminal justice agencies pertaining to the accuracy and completeness of criminal history record information. The Washington state patrol shall also adopt rules for the correction of criminal history record information and the dissemination of corrected information to agencies and persons to whom inaccurate or incomplete information was previously disseminated. Such rules may establish time limitations of not less than ninety days upon the requirement for disseminating corrected information.

[2012 c 125 § 3; 2010 c 8 § 1093; 2005 c 274 § 206; 1979 ex.s. c 36 § 3; 1977 ex.s. c 314 § 8.]

10.97.090
Administration by state patrol.

The Washington state patrol is hereby designated the agency of state government responsible for the administration of the 1977 Washington State Criminal Records Privacy Act.

The Washington state patrol may adopt any rules and regulations necessary for the performance of the administrative functions provided for in this chapter.

The Washington state patrol shall have the following specific administrative duties:

(1) To establish by rule and regulation standards for the security of criminal history information systems in order that such systems and the data contained therein be adequately protected from fire, theft, loss, destruction, other physical hazard, or unauthorized access;

(2) To establish by rule and regulation standards for personnel employed by criminal justice of other state and local government agencies in positions with responsibility for maintenance and dissemination of criminal history record information; and

(3) To contract with the Washington state auditor or other public or private agency, organization, or individual to perform audits of criminal history record information systems.

[1979 ex.s. c 36 § 4; 1977 ex.s. c 314 § 9.]

10.97.100
Fees.

Criminal justice agencies shall be authorized to establish and collect reasonable fees for the dissemination of criminal history record information to agencies and persons other than criminal justice agencies.

[1977 ex.s. c 314 § 10.]

10.97.110
Civil remedies—Criminal prosecution not affected.

Any person may maintain an action to enjoin a continuance of any act or acts in violation of any of the provisions of this chapter, and if injured thereby, for the recovery of damages and for the recovery of reasonable attorneys' fees. If, in such action, the court shall find that the defendant is violating or has violated any of the provisions of this chapter, it shall enjoin the defendant from a continuance thereof, and it shall not be necessary that actual damages to the plaintiff be alleged or proved. In addition to such injunctive relief, the plaintiff in said action shall be entitled to recover from the defendant the amount of the actual damages, if any, sustained by him or her if actual damages to the plaintiff are alleged and proved. In any suit brought to enjoin a violation of this chapter, the prevailing party may be awarded reasonable attorneys' fees, including fees incurred upon appeal. Commencement, pendency, or conclusion of a civil action for injunction or damages shall not affect the liability of a person or agency to criminal prosecution for a violation of this chapter.

[2010 c 8 § 1094; 1979 ex.s. c 36 § 5; 1977 ex.s. c 314 § 11.]

10.97.120
Criminal penalties—Civil action not affected.

Violation of the provisions of this chapter shall constitute a misdemeanor, and any person whether as principal, agent, officer, or director for himself or herself or for another person, or for any firm or corporation, public or private, or any municipality who or which shall violate any of the provisions of this chapter shall be guilty of a misdemeanor for each single violation. Any criminal prosecution shall not affect the right of any person to bring a civil action as authorized by this chapter or otherwise authorized by law.

[2010 c 8 § 1095; 1977 ex.s. c 314 § 12.]

10.97.130
Child victims of sexual assaults, identification confidential.

Information identifying child victims under age eighteen who are victims of sexual assaults is confidential and not subject to release to the press or public without the permission of the child victim or the child's legal guardian. Identifying information includes the child victim's name, addresses, location, photographs, and in cases in which the child victim is a relative or stepchild of the alleged perpetrator, identification of the relationship between the child and the alleged perpetrator. Information identifying the child victim of sexual assault may be released to law enforcement, prosecutors, judges, defense attorneys, or private or governmental agencies that provide services to the child victim of sexual assault. Prior to release of any criminal history record information, the releasing agency shall delete any information identifying a child victim of sexual assault from the information except as provided in this section.

[1992 c 188 § 8.]

NOTES:

Findings—Intent—Severability—1992 c 188: See notes following RCW 7.69A.020.

10.97.140
Construction.

Nothing in RCW 40.14.060 or 40.14.070 or chapter 42.56 RCW precludes dissemination of criminal history record information, including nonconviction data, for the purposes of this chapter.

[2005 c 274 § 207; 1999 c 326 § 4.]

Chapter 11.35 - IMMOBILIZATION

Sections:

11.35.010 - Scofflaw list

A. When there are four or more parking citations issued against a vehicle for each of which a person has failed to respond, failed to appear at a requested hearing, or failed to pay amounts due for at least 45 days from the date of the filing of each of those citations, the Seattle Municipal Court shall place the vehicle on a list of scofflaws, and shall mail, by first class mail, a notice to the last known registered owner of the vehicle, as disclosed by the vehicle license number as provided by the Washington State Department of Licensing or equivalent vehicle licensing agency of the state in which the vehicle is registered. If there is no last known address that can be ascertained from the Washington Department of Licensing, or if the vehicle has no Washington vehicle license number or is not registered in the State of Washington, the notice, in the form of a readily visible notification sticker, may be affixed to the vehicle while left within a public right-of-way or other publicly owned or controlled property. A notification sticker may be used in lieu of mailing even if the last known address is ascertainable for vehicles registered in the State of Washington.

B. The registered vehicle owner may request an administrative review at the Seattle Municipal Court at any time that the vehicle is on the scofflaw list until the vehicle has been immobilized or impounded. The review should only examine whether the vehicle is properly on the scofflaw list and shall not review the underlying citations that caused the vehicle to be included on the scofflaw list. The vehicle shall be removed from the list only upon a showing by the registered owner that either:

1. fewer than four of the citations that caused the vehicle to be included on the scofflaw list were committed while the current registered owner was the legal owner of the vehicle; or

2. all amounts due pertaining to the citations that met the criteria for scofflaw under Section 11.35.010 A have been satisfied in full.

C. A vehicle shall remain on the scofflaw list until all outstanding parking infraction penalties, court costs (including but not limited to collection agency remuneration authorized under RCW 3.02.045), default penalties on parking traffic infractions imposed under Section 11.31.120, immobilization release fees imposed under subsection 11.35.020.H, costs of impoundment (including removal, towing and storage fees) imposed under Section 11.30.120, towing administrative fees imposed under Section 11.30.290 and immobilization administrative fees under subsection 11.35.020.H, and interest, have been paid, or a time payment plan has been arranged with the Seattle Municipal Court or their authorized agent.

D. When a time payment plan is created, the subject vehicle shall be temporarily removed from the scofflaw list and the payment amounts shall be applied on a pro rata basis until all penalties, fines or fees owed relating to all parking citations are satisfied. A vehicle that has been temporarily removed from the scofflaw list shall be returned to the list if the owner defaults on the time payment agreement, in accordance with guidelines adopted by the Seattle Municipal Court.

(Ord. 124558, § 1, 2014; Ord. 123563, § 1, 2011; Ord. 123447, § 1, 2010)

11.35.020 - Immobilization

A. Effective July 1, 2011 and thereafter, if the notice requirements under Section 11.35.010 A have been met, and if parked in public right-of-way or on other publicly owned or controlled property, a vehicle on the scofflaw list may be immobilized by installing on such vehicle a device known as a "boot," which clamps and locks onto the vehicle wheel and impedes vehicle movement. If a vehicle is immobilized, it shall not be released until full payment has been made, or a time payment agreement has been entered into for all outstanding penalties, fines, or fees owed for all parking citations, plus all immobilization, towing, and storage charges and administrative fees.

B. Any vehicle that remains booted for 48 hours or more, not including any of the 48 hours from the beginning of Saturday until the end of Sunday, or which becomes illegally parked while booted, shall be subject to towing and impoundment pursuant to Section 11.30.040. The Seattle Department of Transportation and Seattle Police Department shall issue joint guidelines for vehicle towing related to immobilization, based on Sections 11.30.040 and 11.16.320.

C. The person installing the boot shall leave under the windshield wiper or otherwise attach to the vehicle a notice advising the owner that the vehicle has been booted by the City of Seattle for failure to respond, failure to appear at a requested hearing, and failure to pay amounts due for four or more adjudicated parking infractions for at least 45 days from the date of the last such adjudication issued against the vehicle; that release of the boot may be obtained by paying all outstanding penalties, fines, or forfeitures owed relating to all adjudicated violations, plus all booting, removal, towing, and storage charges and administrative fees; that unless such payment is made within two business days of the date of the notice, the vehicle will be impounded; that it is unlawful for any person to remove or attempt to remove the boot, to damage the boot, or to move the vehicle with the boot attached, unless authorized by the Seattle Police Department or an authorized agent of the City; and that the owner may seek an administrative review of the booting by submitting a request to the Seattle Municipal Court within ten days of the release of the boot. The notice shall further state that the vehicle remains subject to impoundment regardless of whether the owner requests an appeal.

D. The vehicle may be released from immobilization when the vehicle owner or an agent of the owner pays all outstanding parking infraction penalties, court costs (including but not limited to collection agency remuneration authorized under RCW 3.02.045), default penalties on parking traffic infractions imposed under Section 11.31.120, immobilization release fees imposed under subsection 11.35.020.H, costs of impoundment (including removal, towing and storage fees) imposed under Section 11.30.120, towing administrative fees imposed under Section 11.30.290 and immobilization administrative fees under subsection 11.35.020.H, and interest, or enters into a time payment agreement for the payment thereof. Upon full payment or upon entry into a time payment agreement, the Seattle Police Department or other authorized agent of the City shall promptly remove or enable the removal of the boot from the vehicle. If payment is made in full, the vehicle shall be removed from the scofflaw list and shall not be subject to immobilization or impoundment for the paid citations. Upon entry into a time payment agreement, the vehicle shall be temporarily removed from the scofflaw list and shall not be subject to immobilization, provided, however, that the vehicle shall be returned to the scofflaw list and be subject to immobilization if the owner defaults on the time payment agreement. A registered owner who defaults on a time payment agreement shall not be given another opportunity to make a time payment arrangement and therefore, payment for all outstanding amounts above shall be made in full before the vehicle may be removed from the scofflaw list or released from immobilization or impound. Any person who has previously removed or enabled removal of a booting device in violation of subsection E while on the scofflaw list for any four or more parking infractions, and subsequently is booted a second time while on the scofflaw list for the same parking infractions, shall not be eligible for a time payment plan.

E. No person other than an authorized employee of the Seattle Police Department or an authorized agent of the City shall remove or enable the removal of the boot described in subsection A of this Section from any vehicle on which it has been installed unless the requirements of subsection D have been met.

F. If the Seattle Police Department or an authorized agent of the City enables the vehicle owner to remove the boot, the owner shall return the boot to a location designated by the Department within two calendar days of the removal.

G. No person, other than an authorized employee of the Seattle Police Department or other authorized agent of the City, shall move, by towing or other means, any vehicle after it has been immobilized but before the boot has been removed.

H. The Director of Finance and Administrative Services shall determine and set an immobilization fee and an administrative fee in amounts such that the sum of such fees do not exceed the sum of the lowest impound fee, minimum storage fee, and administrative fee for vehicle impoundment under Section 11.30.120. An administrative fee, if any, shall be levied when the boot is removed. The

administrative fee shall be collected by the contractor releasing the vehicle from immobilization, shall be remitted to the Department of Finance and Administrative Services, and shall be deposited in an appropriate account.

I. A person who fails to return the booting device within the time frame required by subsection F of this section may be charged a late fee as determined by the Director of Finance and Administrative Services.

J. A person who intentionally damages the booting device may be charged a replacement fee as determined by the Director of Finance and Administrative Services and also may be prosecuted for the crime of property destruction under section 12A.08.020.

K. The Director of Finance and Administrative Services shall adopt rules governing the imposition of fees under this Section 11.35.020.

(Ord. 124558, § 2, 2014; Ord. 123563, § 2, 2011; Ord. 123447, § 1, 2010)

11.35.030 - Post-immobilization review

The registered vehicle owner may seek a post-deprivation review of the immobilization by submitting a written request to the Seattle Municipal Court within ten days of the placement of the notice on the vehicle, as established by the notice date. Upon timely receipt of such written request, the Seattle Municipal Court shall, within a reasonable time as established by the Court, conduct a review on the issue of whether the immobilization was proper and shall issue a written decision setting forth the reasons on which the decision is based, provided, however, that any previously adjudicated parking infractions that formed the basis of the vehicle's scofflaw status shall not be subject to the review. The person seeking review shall have an opportunity to present evidence on his or her behalf in accordance with requirements established by the Court.

(Ord. 123447, § 1, 2010)

Chapter 11.35 - IMMOBILIZATION

Sections:

11.35.010 - Scofflaw list

A. When there are four or more parking citations issued against a vehicle for each of which a person has failed to respond, failed to appear at a requested hearing, or failed to pay amounts due for at least 45 days from the date of the filing of each of those citations, the Seattle Municipal Court shall place the vehicle on a list of scofflaws, and shall mail, by first class mail, a notice to the last known registered owner of the vehicle, as disclosed by the vehicle license number as provided by the Washington State Department of Licensing or equivalent vehicle licensing agency of the state in which the vehicle is registered. If there is no last known address that can be ascertained from the Washington Department of Licensing, or if the vehicle has no Washington vehicle license number or is not registered in the State of Washington, the notice, in the form of a readily visible notification sticker, may be affixed to the vehicle while left within a public right-of-way or other publicly owned or controlled property. A notification sticker may be used in lieu of mailing even if the last known address is ascertainable for vehicles registered in the State of Washington.

B. The registered vehicle owner may request an administrative review at the Seattle Municipal Court at any time that the vehicle is on the scofflaw list until the vehicle has been immobilized or impounded. The review should only examine whether the vehicle is properly on the scofflaw list and shall not review the underlying citations that caused the vehicle to be included on the scofflaw list. The vehicle shall be removed from the list only upon a showing by the registered owner that either:

1. fewer than four of the citations that caused the vehicle to be included on the scofflaw list were committed while the current registered owner was the legal owner of the vehicle; or

2. all amounts due pertaining to the citations that met the criteria for scofflaw under Section 11.35.010 A have been satisfied in full.

C. A vehicle shall remain on the scofflaw list until all outstanding parking infraction penalties, court costs (including but not limited to collection agency remuneration authorized under RCW 3.02.045), default penalties on parking traffic infractions imposed under Section 11.31.120, immobilization release fees imposed under subsection 11.35.020.H, costs of impoundment (including removal, towing and storage fees) imposed under Section 11.30.120, towing administrative fees imposed under Section 11.30.290 and immobilization administrative fees under subsection 11.35.020.H, and interest, have been paid, or a time payment plan has been arranged with the Seattle Municipal Court or their authorized agent.

D. When a time payment plan is created, the subject vehicle shall be temporarily removed from the scofflaw list and the payment amounts shall be applied on a pro rata basis until all penalties, fines or fees owed relating to all parking citations are satisfied. A vehicle that has been temporarily removed from the scofflaw list shall be returned to the list if the owner defaults on the time payment agreement, in accordance with guidelines adopted by the Seattle Municipal Court.

(Ord. 124558, § 1, 2014; Ord. 123563, § 1, 2011; Ord. 123447, § 1, 2010)

11.35.020 - Immobilization

A. Effective July 1, 2011 and thereafter, if the notice requirements under Section 11.35.010 A have been met, and if parked in public right-of-way or on other publicly owned or controlled property, a vehicle on the scofflaw list may be immobilized by installing on such vehicle a device known as a "boot," which clamps and locks onto the vehicle wheel and impedes vehicle movement. If a vehicle is immobilized, it shall not be released until full payment has been made, or a time payment agreement has been entered into for all outstanding penalties, fines, or fees owed for all parking citations, plus all immobilization, towing, and storage charges and administrative fees.

B. Any vehicle that remains booted for 48 hours or more, not including any of the 48 hours from the beginning of Saturday until the end of Sunday, or which becomes illegally parked while booted, shall be subject to towing and impoundment pursuant to Section 11.30.040. The Seattle Department of Transportation and Seattle Police Department shall issue joint guidelines for vehicle towing related to immobilization, based on Sections 11.30.040 and 11.16.320.

C. The person installing the boot shall leave under the windshield wiper or otherwise attach to the vehicle a notice advising the owner that the vehicle has been booted by the City of Seattle for failure to respond, failure to appear at a requested hearing, and failure to pay amounts due for four or more adjudicated parking infractions for at least 45 days from the date of the last such adjudication issued against the vehicle; that release of the boot may be obtained by paying all outstanding penalties, fines, or forfeitures owed relating to all adjudicated violations, plus all booting, removal, towing, and storage charges and administrative fees; that unless such payment is made within two business days of the date of the notice, the vehicle will be impounded; that it is unlawful for any person to remove or attempt to remove the boot, to damage the boot, or to move the vehicle with the boot attached, unless authorized by the Seattle Police Department or an authorized agent of the City; and that the owner may seek an administrative review of the booting by submitting a request to the Seattle Municipal Court within ten days of the release of the boot. The notice shall further state that the vehicle remains subject to impoundment regardless of whether the owner requests an appeal.

D. The vehicle may be released from immobilization when the vehicle owner or an agent of the owner pays all outstanding parking infraction penalties, court costs (including but not limited to collection agency remuneration authorized under RCW 3.02.045), default penalties on parking traffic infractions imposed under Section 11.31.120, immobilization release fees imposed under subsection 11.35.020.H, costs of impoundment (including removal, towing and storage fees) imposed under Section 11.30.120, towing administrative fees imposed under Section 11.30.290 and immobilization administrative fees under subsection 11.35.020.H, and interest, or enters into a time payment agreement for the payment thereof. Upon full payment or upon entry into a time payment agreement, the Seattle Police Department or other authorized agent of the City shall promptly remove or enable the removal of the boot from the vehicle. If payment is made in full, the vehicle shall be removed from the scofflaw list and shall not be subject to immobilization or impoundment for the paid citations. Upon entry into a time payment agreement, the vehicle shall be temporarily removed from the scofflaw list and shall not be subject to immobilization, provided, however, that the vehicle shall be returned to the scofflaw list and be subject to immobilization if the owner defaults on the time payment agreement. A registered owner who defaults on a time payment agreement shall not be given another opportunity to make a time payment arrangement and therefore, payment for all outstanding amounts above shall be made in full before the vehicle may be removed from the scofflaw list or released from immobilization or impound. Any person who has previously removed or enabled removal of a booting device in violation of subsection E while on the scofflaw list for any four or more parking infractions, and subsequently is booted a second time while on the scofflaw list for the same parking infractions, shall not be eligible for a time payment plan.

E. No person other than an authorized employee of the Seattle Police Department or an authorized agent of the City shall remove or enable the removal of the boot described in subsection A of this Section from any vehicle on which it has been installed unless the requirements of subsection D have been met.

F. If the Seattle Police Department or an authorized agent of the City enables the vehicle owner to remove the boot, the owner shall return the boot to a location designated by the Department within two calendar days of the removal.

G. No person, other than an authorized employee of the Seattle Police Department or other authorized agent of the City, shall move, by towing or other means, any vehicle after it has been immobilized but before the boot has been removed.

H. The Director of Finance and Administrative Services shall determine and set an immobilization fee and an administrative fee in amounts such that the sum of such fees do not exceed the sum of the lowest impound fee, minimum storage fee, and administrative fee for vehicle impoundment under Section 11.30.120. An administrative fee, if any, shall be levied when the boot is removed. The

administrative fee shall be collected by the contractor releasing the vehicle from immobilization, shall be remitted to the Department of Finance and Administrative Services, and shall be deposited in an appropriate account.

I. A person who fails to return the booting device within the time frame required by subsection F of this section may be charged a late fee as determined by the Director of Finance and Administrative Services.

J. A person who intentionally damages the booting device may be charged a replacement fee as determined by the Director of Finance and Administrative Services and also may be prosecuted for the crime of property destruction under section 12A.08.020.

K. The Director of Finance and Administrative Services shall adopt rules governing the imposition of fees under this Section 11.35.020.

(Ord. 124558, § 2, 2014; Ord. 123563, § 2, 2011; Ord. 123447, § 1, 2010)

11.35.030 - Post-immobilization review

The registered vehicle owner may seek a post-deprivation review of the immobilization by submitting a written request to the Seattle Municipal Court within ten days of the placement of the notice on the vehicle, as established by the notice date. Upon timely receipt of such written request, the Seattle Municipal Court shall, within a reasonable time as established by the Court, conduct a review on the issue of whether the immobilization was proper and shall issue a written decision setting forth the reasons on which the decision is based, provided, however, that any previously adjudicated parking infractions that formed the basis of the vehicle's scofflaw status shall not be subject to the review. The person seeking review shall have an opportunity to present evidence on his or her behalf in accordance with requirements established by the Court.

(Ord. 123447, § 1, 2010)

Seattle Police Department Manual

Carmen Best, Chief of Police

12.110 - USE OF DEPARTMENT E-MAIL & INTERNET SYSTEMS

Effective Date: 05/01/18

The Seattle Police Department provides email service and internet access to conduct Department business.

The guidelines in this section are not exclusive. They provide a general framework of prohibited and acceptable email and internet use.

This section applies to all employees and their access to the internet while on City equipment or while on duty and their use of City email by any means.

12.110-POL

1. The City of Seattle Owns the Email and Internet Systems and Determines Appropriateness

The City owns the computers, email, and internet access systems and may monitor email and internet use for policy compliance. The City retains the right to determine what is appropriate for the workplace.

Department supervisors ensure that their staff is familiar with and adhere to Department and City email and internet policy.

2. The Department Allows Limited Personal Use of Email and Internet

Recognizing the realities of the workplace, the Department allows limited personal use of email and the internet. Occasional personal use is permissible if it follows the policies and usage standards set by the Department and the City.

3. Department Email and Internet Use is Subject to Public Disclosure

There is no expectation of privacy in using Department email or internet services on Department-owned computers. All use of Department computers, whether official or personal, is subject to public disclosure laws and can be discoverable in a lawsuit.

4. All Email and Internet Communications Must be Professional, Appropriate, and Lawful

All email communications and internet use must comply with Department and City policies on professionalism and harassment in the workplace. Employees will clearly identify their personal opinions or preliminary observations.

All internet use on Department computers comply with all laws and policies. This includes policies on privacy issues, any release of confidential, sensitive, or classified information, or information exempt from public disclosure.

The Department acknowledges that email signatures and user photos may contribute to an employee's professional image. Employees wishing to include photos, emblems (other than the SPD patch), logos, quotations, or other similar items in their email signature must have their proposed email signature approved by their chain of command through the deputy chief in advance.

5. Employees May Send Criminal Justice Information (CJI) or Other

Sensitive Information via Office Message Encryption (OME)

Ensure the recipient is a member of a Criminal Justice Agency and allowed to receive CJI information.

Including the trigger word "COSSecure" in the subject line of an email message sent from an SPD Outlook email account.

- Inserting "COSSecure" within the subject line of an SPD Outlook email will activate OME for that email.

6. Employees Will Read Email at Least Once per Shift and Respond Appropriately

Employees are not required to read or respond to email when off duty or during a system outage or technical failure that prevents the receipt or sending of email.

Employees will respond (when applicable) to High Importance emails within four business days, or sooner if required by the subject matter.

Emails classified as High Importance are marked with an orange exclamation point and include the following subjects:

- Command Staff Communications
- Directives
- Special Orders
- Training Digests
- All other emails that are job-related, time sensitive, and mandatory for the recipient
- These include subpoenas, wanted bulletins, information bulletins, investigative follow-up requests, statement requests, pre-trial discovery requests, and seizure hearing notices.

A lieutenant or above must approve the use of the High Importance classification for any other email communication.

7. Employees Will Activate Automatic Email Replies for Extended Absences

Employees will activate their email Automatic Replies (Out of Office) in Outlook when they expect that they will be unable to respond to email for a period that exceeds four business days.

8. External Emails Will Contain Employee Contact Information

All email correspondence going outside the Department will contain the employee's contact information including email address, business address, and business phone numbers.

9. General Distribution Emails Require Lieutenant Approval

Emails going to large distribution lists such as SPDALL or SPDSWORN are general distribution emails. These emails require approval from a lieutenant or above, and must include the name of the approving employee in the email.

When sending a general distribution email, employees will enter the recipients using the "Bcc" (blind carbon copy) field. The "Bcc" field will prevent unnecessary disclosure of email addresses, reduce vulnerability to junk email, and improve the chances of the email being successfully sent. The "To" field is not designed to handle a large number of addresses.

10. Employees Must Use Caution When Opening Email Attachments

Employees may contact Seattle IT if they have questions about an email attachment. Due to the risk of computer virus attacks, employees should not open email attachments from an unknown source.

11. Section Captain or Director Approves "Send As" Privileges for Shared Email Accounts

Employees must request "Send As" privileges for a shared mailbox, and/or request that a shared mailbox be created, by submitting a request via email to their section captain or director.

Employees will forward the approval to Seattle IT and initiate a service request.

12. Employees Will Not use Department Email or Computers to Conduct a Personal For-Profit Business

13. Employees Will Not use Department Email or Computers to Review Personal Investments or to Transact any Investment Business

These types of transactions include trading in stocks, bonds, or mutual funds.

Exception: Employees may conduct infrequent, brief checks of their investments in the City's Deferred Compensation Program, since this is a City-sponsored and City-maintained program.

14. Employees Will Not use Department Email or Computers to Participate in any Campaign for Elected Office or for any Other Political Activity

This includes a prohibition on making any campaign contributions via a credit card and using a Department computer to do so. Similarly, employees may not "lobby" elected officials through Department computers.

15. Employees Will not use Department Email or Computers to Engage in Demeaning or Defamatory Conduct

Examples of such prohibited activities include knowingly accessing pornographic materials or sites that promote exclusivity, hatred, or positions which are contrary to the City's policy of valuing cultural diversity.

16. Employees Will Not Access Sites That Incur a Cost to the Department Without Prior Supervisor Approval

17. Employees Will Not Knowingly Access or Communicate any Material of an Obscene, Harassing, Discriminatory or Derogatory Nature

Examples of such material include sites or email containing racial or sexual slurs or jokes, or containing harassing, intimidating, abusive, or offensive material to or about others.

18. Certain Assignments May Require Access to Sensitive Sites

The Department recognizes that certain employees, such as Vice and Intelligence Unit detectives, may have a legitimate business purpose for accessing sites and information otherwise considered inappropriate or illegal.

If employees need to access such "sensitive sites", employees will abide by the following:

- Employees will obtain approval from an immediate supervisor before accessing sensitive sites. The supervisor will contact Seattle IT to request an exception to the web filtering protocols.

- Employees accessing such sites should exercise courtesy to others that may be present when doing so. This may include closing the door, turning the screen away, or notifying other employees beforehand.

19. Department Computer Usage is Subject to the Intelligence Ordinance

Employees will adhere to the following guidelines to avoid a violation of the investigation ordinance, SMC Chapter 14.12 ("Restricted information" is defined in SMC 14.12.030 (K)):

- Storage of "restricted information" (as defined in the ordinance) on disks or computer/network drives must comply with the ordinance.

- Employees may not create directories or subdirectories which organize/index "restricted information."

- Employees may not transmit "restricted information" including web addresses (URLs) to specific sites, via email.

    - Employees may not create bookmarks or hotlists in web browsers which organize/index restricted information.

Site Disclaimer: The Seattle Police Department's website was developed to provide general information. Data contained at this location is generally not reviewed for legal sufficiency. SPD documents displayed are for reference purposes only. Their completeness or currency are not guaranteed. Links or references to other information or organizations are for reference only and do not constitute an endorsement.

ADA Notice

Notice of Nondiscrimination

Privacy

© Copyright 1995-2018 City of Seattle

Seattle Police Department Manual

Carmen Best, Chief of Police

5.001 - STANDARDS AND DUTIES

Effective Date: 03/01/18

5.001-POL

This policy provides the philosophy for employee conduct and professionalism. It is not the Department's intent to interfere with or constrain the freedoms, privacy, and liberties of employees; discipline will only be imposed where there is a connection between the conduct and the duties, rank, assignment, or responsibilities of the employee.

The Department expects all employees to treat all people with dignity; remember that community care-taking is at times the focus, not always command and control; and that the guiding principle is to treat everyone with respect and courtesy, guarding against employing an officious or overbearing attitude and refraining from language, demeanor, and actions that may cause the individual feeling belittled, ridiculed, or intimidated.

This section applies to all Department employees. The content is not all-inclusive. Employees must also comply with conduct expectations in other manual sections pertaining to them.

1. The Chief of Police Determines Employee Duty Status

The Chief of Police has final authority through the Charter of the City of Seattle to determine the on-duty status of any employee, and whether their actions are within the course and scope of their duties.

Completion of overtime or other Department forms by an employee does not establish the employee's duty status.

2. Employees Must Adhere to Laws, City Policy and Department Policy

Employees adhere to:

- Federal laws
- State laws
- Laws of the City of Seattle
- City of Seattle policies
- The Seattle Police Manual
- Published Directives and Special Orders
- Applicable collective bargaining agreements and relevant labor laws

3. Employees Use Training to Assist in Following Policy

Department training is intended to provide guidance on how to implement and follow policy.

Not following training, in itself, is not a policy violation.

Regardless of the result, an employee may need to explain, and possibly document, a substantial deviation from training

4. Employees Must Attend All Mandatory Training

Employees will attend mandatory training and follow the current curriculum during their duties.

Employees who have missed any mandatory training because of excused absences, such as a sick day or court appearance, will arrange through their immediate supervisor to complete that training within a reasonable time frame.

Employees on approved limited duty who cannot participate in a mandatory training program will request a waiver using SPD Memorandum (form 1.11), and an Insurer Activity Prescription Form (APF) through their chain of command.

Also See: 1.075-Failure to complete Required Training

5. Employees Complete Work in a Timely Manner

Absent exigent circumstances or supervisory approval, employees will complete all required duties and official reports before going off duty.

6. Employees May Use Discretion

Employees are authorized and expected to use discretion in a reasonable manner consistent with the mission of the Department and duties of their office and assignment.

Discretion is proportional to the severity of the crime or public safety issue being addressed.

7. Employees Engaged in Department-Related Activities Identify Themselves When Requested

Employees will provide their name and Department serial number verbally, or in writing if requested.

Employees may use a Department-issued business card that contains their name and serial number to satisfy the request for the information.

Employees will also show their department identification card and badge (sworn) when specifically requested to do so.

Exception: Employees are not required to immediately identify themselves if:

- An investigation is jeopardized
- A police function is hindered
- There is a safety consideration

8. On-Duty Officers in Civilian Attire Identify Themselves When Contacting Citizens

Officers will accomplish this verbally and/or by displaying their badge or Department-issued identification.

Exception: Employees are not required to immediately identify themselves if:

- An investigation is jeopardized
- A police function is hindered
- There is a safety consideration

9. Uniformed Employees Will Not Initiate Contact With Officers Dressed In Civilian Clothing

When any uniformed employee meets an officer dressed in civilian attire, that uniformed employee will not openly recognize the plain-clothes officer unless greeted first.

10. Employees Shall Strive to be Professional

Regardless of duty status, employees may not engage in behavior that undermines public trust in the Department, the officer, or other officers. Employees will avoid unnecessary escalation of events even if those events do not end in reportable uses of force.

Any time employees represent the Department or identify themselves as police officers or Department employees, they will not use profanity directed as an insult or any language that is derogatory, contemptuous, or disrespectful toward any person.

Employees on duty or in uniform will not publicly ridicule:

- The Department or its policies
- Other Department employees
- Other law enforcement agencies
- The criminal justice system or police profession

This applies where such expression is defamatory, obscene, undermines the effectiveness of the Department, interferes with the maintenance of discipline, or is made with reckless disregard for truth.

11. Employees Shall Be Truthful and Complete in All Communication

Exception: Employees may use deception for a specific and lawful purpose in certain circumstances, when:

- There is an exigent threat to life safety or public safety
- It is necessary due to the nature of the employee's assignment
- There is a need to acquire information for a criminal investigation

12. Employees Must Promptly Report Exonerating Information

Employees must report any information they discover that may exonerate a person who is under investigation, or has been charged with or convicted of a crime.

13. Employees Shall Not Use Their Position or Authority for Personal Gain

14. Retaliation is prohibited

No employee will retaliate against any person who:

- Exercises a constitutional right
- Records an incident
- Makes a public disclosure request
- Publicly criticizes an SPD employee or the Department
- Initiates litigation

- Opposes any practice reasonably believed to be unlawful or in violation of Department policy
- Files a complaint or provides testimony or information related to a complaint of misconduct
- Provides testimony or information for any other administrative criminal or civil proceeding involving the Department or an officer
- Communicates intent to engage in the above-described activities
- Otherwise engages in lawful behavior

Retaliation includes discouragement, intimidation, coercion, or adverse action against any person. This prohibition will include any interference with the conduct of an administrative, civil, or criminal investigation.

Such retaliation may be a criminal act, may give rise to personal civil liability, or constitute independent grounds for discipline, up to and including termination.

15. Employees Obey any Lawful Order Issued by a Superior Officer

Failure to obey lawful orders from a superior officer constitutes insubordination. Orders may be issued directly, relayed through a subordinate employee or current Department training, published in notices, and other forms of communication.

16. Supervisors Clarify Conflicts in Orders

Should any orders conflict with a previous order, or published regulation, employees may respectfully bring this to the supervisor's attention.

The supervisor who issued the conflicting order will try to correct the conflict in orders.

17. Employees May Object to Orders Under Certain Conditions

An employee may object to a supervisor's orders under these conditions:

- When such orders represent unjustified, substantial and/or reckless disregard for life or safety
- When such orders are illegal or unethical
- When the supervisor has been relieved of duty by an employee of higher rank
- When other circumstances are present that establish the supervisor's inability to discharge the duties of the assignment

Employees in this situation will, if practical, state the basis for objecting to the order to the supervisor.

If the situation remains unresolved, the employee will immediately contact the next higher ranking supervisor in the chain of command.

18. Employees Must Avoid Conflicts of Interest

Employees will not associate with persons or organizations where such association reasonably gives the appearance of conflict of interest.

Employees will not engage in enforcement, investigative, or administrative functions that create or give the appearance of conflicts of interest.

Employees will not investigate events where they are involved. This also applies where any person with whom the employee has a personal relationship is involved in the event.

Except in cases of emergency, officers will not arrest family members, business associates, or social acquaintances.

Employees will not show preference by recommending or suggesting the employment of any attorney, bondsman, or other business during the course of, or because of, their official business as employees of the Department.

See also SMC 4.16-City Code of Ethics and 5.120 – Off-Duty Employment.

19. Employees Must Disclose Conflicts

Employees will immediately disclose to the Chief of Police, via their supervisor, any activities or relationships that may present an actual, potential, or apparent conflict of interest for themselves or other Department employees.

20. Employees Shall Not Use a Department Mailing Address for Personal Reasons

This provision includes using a Department address for a driver license, vehicle registration, telephone service, etc.

21. Employees Shall Not Imply to Another Agency the Department's Approval or Disapproval of That Agency's Actions

22. Employees Shall Not Recommend Case Dispositions to Courts

No employee below Assistant Chief will make any recommendations to any court or other judicial agency regarding the disposition of any pending court case investigated by the Department.

Exception: This does not apply to agencies conducting pre-sentence investigations.

23. Employees Notify the Department Before Initiating any Claim for Damages Related to Their Official Position

Employees must report their intention to initiate a claim for damages sustained while working in a law enforcement capacity or by virtue of employment with the Department. This notification is to the Chief of Police via the employee's chain of command.

24. Officers Report any Off-Duty Assault on Themselves Related to Department Employment

If an employee is assaulted while working off-duty in a law enforcement capacity, that employee must report the assault. The employee must then notify the Department before seeking a No Contact or Restraining Order related to the assault. This notification is to the Chief of Police via the employee's chain of command.

25. Employees Report Their Intent to Initiate Lawsuits or Seek Court Orders

Employees must report to the Chief of Police their intention to sue for damages sustained while working in a law enforcement capacity or by virtue of employment with the Department.

Sworn employees will notify their supervisor prior to applying for a No Contact or Restraining Order stemming from an assault on the employee that occurred while the employee was working in a law enforcement capacity.

26. Employees Follow the Americans With Disabilities Act (ADA) in the Performance of their Job

Employees interacting with persons with disabilities will take steps to provide needed accommodations to provide police services or achieve a law enforcement goal.

See: Commonly asked questions about the Americans with Disabilities Act and Law Enforcement, ADA.gov, City of Seattle ADA.

Site Disclaimer: The Seattle Police Department's website was developed to provide general information. Data contained at this location is generally not reviewed for legal sufficiency. SPD documents displayed are for reference purposes only. Their completeness or currency are not guaranteed. Links or references to other information or organizations are for reference only and do not constitute an endorsement.

ADA Notice

Notice of Nondiscrimination

Privacy

© Copyright 1995-2018 City of Seattle

Seattle Police Department Manual
Carmen Best, Chief of Police

5.002 - RESPONSIBILITIES OF EMPLOYEES CONCERNING ALLEGED POLICY VIOLATIONS

Effective Date: 07/15/18

5.002-POL

This policy applies to the reporting of alleged policy violations identified by the public, employees of the Department, or others and related investigations by the Department and OPA.

The purpose of this policy and the related procedures is to provide a prompt, just, and open disposition of allegations of policy violation regarding the conduct of employees.

1. The Department Will Accept Allegations of Policy Violations from Any Source and by Any Means

2. Employees Will Assist Any Person Who Wishes to File a Complaint

In addition to obligations that may arise under other parts of this manual (e.g., See 5.140-Bias-Free Policing-6, 7) employees will assist the complainant by taking the complaint and passing it on to a supervisor or OPA (see also 6 below.)

If the complainant requests information on where and how to file the allegation, the employee will provide it. However, the employee is still responsible for passing the complaint on to a supervisor or OPA.

If the employee is unable to take the complaint (e.g., the allegation is made during a demonstration while the employee is on a line, etc.), while not interfering or compromising public safety interests, the employee will provide specific information to the complainant on where and how to file the allegation.

3. Employees Shall Not Discourage, Interfere With, Hinder, or Obstruct Any Person from Filing a Complaint or Conducting or Cooperating with an Investigation of an Allegation of a Policy Violation

4. Retaliation Is Prohibited

No employee will retaliate against any person who:

- Exercises a constitutional right
- Records an incident, including videotaping and photographing
- Makes a public disclosure request
- Publicly criticizes an SPD employee or the Department
- Initiates litigation
- Opposes any practice reasonably believed to be unlawful or in a violation of Department policy

- Files a complaint or provides testimony or information related to an allegation of policy violations, including but not limited to complaints made OPA, Human Resources, or the EEO Investigator

- Provides testimony or information for any other administrative criminal or civil proceeding involving the Department or a Department employee

-Files a whistle-blower claim pursuant to Seattle Municipal Code

- Communicates an intent to engage in the above-described activities

- Otherwise engages in lawful behavior

Retaliation includes discouragement, intimidation, coercion, or undertaking any adverse action against any person because the person engaged in any of the activity set forth above. This prohibition specifically includes interference with any administrative, civil, or criminal investigation.

Retaliation may constitute independent grounds for discipline, up to and including termination.

5. Supervisors Will Investigate or Refer Allegations of Policy Violations Depending on the Severity of the Violation

a. All allegations of serious policy violations will be referred to OPA for investigation.

The following are serious policy violations that must be referred to OPA:

- Unnecessary, unreasonable, or disproportionate use of force

- Biased policing, including use of language that is derogatory based on an individual's sex, race, ethnicity, religion, homeless status, or other protected class.

  - **Exception**: Supervisors will not report an allegation of biased policing directly to OPA in those circumstances where a Bias Review Blue Team Entry is appropriate under 5.140-POL-6 and 5.140-POL-7.

  - See 5.140-Bias-Free Policing, sections 6 & 7.

- Any other violation of SPD policy that may violate a suspect/person's constitutional rights to freedom of speech, to the free exercise of religion, to peaceably assemble, to due process of law, and to be secure against unreasonable search and seizure

- Violations of law enforcement authority

- Failure to use ICV when required

- Failure to report serious policy violations to OPA

- Violations of any policy that are intentional or reckless

- Serious neglect of duty

- Insubordination

- Potential criminal violations of law

  - Failure to fully cooperate in an internal investigation

- Dishonesty

- Misuse of authority, conflicts of interest, or improper use of position for personal gain

- Repeated minor policy violations

b. If the severity of the violation is unclear, the lieutenant or civilian equivalent will consult OPA.

The level of seriousness of an alleged policy violation is sometimes contingent upon the specific facts of an incident. The Department recognizes that even some minor violations may raise concerns of public trust and warrant a referral to OPA. Employees should consider the totality of the circumstances when determining the level of seriousness of an alleged policy violation, apply common sense, and consult with an OPA lieutenant or above if uncertain.

c. Minor policy violations (allegations of policy violations that do not rise to the level of "serious") must still be investigated by the chain of command.

Supervisors who witness, have reason to believe, or receive an allegation of a minor policy violation are expected to address the violation as they deem appropriate.

Supervisors also have the discretion to refer allegations of even minor policy violations to OPA for investigation where they deem it appropriate.

Allegations of minor policy violations may include administrative, procedural, or technical violations of SPD policies that are unrelated to:

(1) The use of force,

(2) Exercise of law enforcement authority, and/or

(3) The list of serious offenses outlined above or issues involving similarly serious potential violations.

Example of allegations of minor policy violations include, but are not limited to:

- Force reporting timeline violations

  - **Exception**: Willful violations of the force reporting timelines must be considered serious violations of policy and referred to OPA

- Failure to perform a system checks on ICV/BWV equipment that causes no failure to record officer actions

- Failure to seatbelt subjects who are being transported by an officer in a seatbelt equipped Department vehicle or during performing official duties where the detainee is not injured as the result of not being secured.

- Failure to identify tactical issues or document deficiencies in the use of force packet

- Failure to turn off the vehicle's AM/FM radio when the ICV is engaged

- Engaging in law enforcement related secondary employment without a valid secondary work permit on file with the Department

- Minor Rudeness (absent bias)

- Traffic and parking infractions

- Profanity not directed as an insult

- Employee tardiness

- Uniform, equipment, and personal appearance

- Failure to attend and/or complete required training (including mandatory e-Learning modules on Cornerstone) for which the employee is registered, unless the failure is:

  - Unjustified and/or

  - The employee fails to provide reasonable advance notice he or she will not attend a scheduled training

  (Supervisors may contact the Cornerstone lieutenant in ETS to research an employee's previous instances of missed training.)

- Failure of a supervisor to register employees for training, except when that failure results in the employees missing the opportunity to attend training

6. Employees Will Report Alleged Violations

Employees will report any alleged minor policy violation to a supervisor.

Employees will report any alleged serious violations to a supervisor or directly to OPA.

For sworn employees this reporting requirement also applies to allegations of uses of force not yet reported.

Employees who witness or learn of a violation of public trust or an allegation of a violation of public trust will take action to prevent aggravation of the incident or loss of evidence that could prove or disprove the allegation.

Any employee who observes another employee engaged in dangerous or criminal conduct or abuse will take reasonable action to intervene.

7. Employees Will Avoid Conflicts of Interest Regarding Allegations of Policy Violation

Employees' duty to avoid and disclose actual, potential, or apparent conflicts of interest (See 5.001-Standards and Duties) extends to the allegation process.

If a supervisor is the subject of an allegation of policy violation, the employee receiving the allegation will refer the allegation to the next highest level employee in the supervisor's chain of command.

If the subject of the allegation of policy violation is assigned to OPA, the employee receiving the report will forward the allegation to the OPA Director.

If the subject of the allegation of policy violation is the OPA Director, the allegation will be forwarded to the City Human Resources Director.

8. Employees Will Report Certain Events

Employees will report to their supervisor, in writing, as soon as practical (and before the start of their next work shift) any of these circumstances in any jurisdiction:

- They are the subject, or they believe they may be the subject of a criminal investigation, criminal traffic citation, arrest, or conviction

- They are the respondent of an order of protection, restraining order, no contact order, anti-harassment order

- Their Washington driver license is expired, suspended, revoked, or restricted, for example,

with an ignition interlock driver license

9. The OPA Manual Sets Forth OPA Procedures

10. OPA May Choose to Investigate Any Alleged Policy Violation

If a supervisor is informed that OPA is taking over an investigation, the supervisor will cease their investigation.

11. Employees Will Cooperate with Department Internal Investigations

Employees will truthfully answer all questions, render complete, comprehensive statements, and promptly provide all available material related to investigations of alleged policy violations. The statements will include all material facts and circumstances surrounding the subject matter of the investigation, which are known by the employee. Omissions of material facts known by the employee will be a failure to cooperate in an internal investigation.

12. OPA Maintains a Record of all Allegations Referred

All allegations of policy violations and any files related to these allegations will be secured within OPA offices for a period of time consistent with the Department's record retention policies.

5.002-TSK-1 Employee Reporting of Serious Policy Violations

When any employee is referring an allegation of serious policy violations to OPA, the employee:

1. **Provides** all of the following information to OPA, if possible:

- The nature, date and place of occurrence of the alleged incident

- Name of employee involved or their serial number and other description

- Name, address, and telephone number of the complainant, aggrieved party, and all known witnesses

- A detailed summary of the allegation

- Information about perishable and other known evidence, including video recordings

- Whether the investigation presents any actual, potential, or apparent conflicts of interest

2. **Assembles** any supporting documentation.

3. **Documents** the allegation on a Complaint Blue Team entry and forwards the entry to OPA via the chain of command.

Exception: If the employee named in the allegation is assigned to OPA, the allegation is sent directly to the OPA Director.

Exception: If the allegation involves the chain of command and the employee does not want it to be viewed by the chain of command, the employee may forward it directly to an OPA lieutenant.

Exception: If the allegation is an EEO complaint, the employee will refer to 5.040-PRO-1.

Site Disclaimer: The Seattle Police Department's website was developed to provide general information. Data contained at this location is generally not reviewed for legal sufficiency. SPD documents displayed are for reference purposes only. Their completeness or currency are not guaranteed. Links or references to other information or organizations are for reference only and do not constitute an endorsement.

ADA Notice

Notice of Nondiscrimination

Privacy

© Copyright 1995-2018 City of Seattle

Seattle Police Department Manual

Carmen Best, Chief of Police

6.060 - COLLECTION OF INFORMATION FOR LAW ENFORCEMENT PURPOSES

Effective Date: 5/19/2004

PHILOSOPHY

Information will be gathered and recorded in a manner that does not unreasonably infringe upon: individual rights, liberties, and freedoms guaranteed by the Constitution of the United States and the State of Washington, including freedom of speech, press, association, and assembly; liberty of conscience; the exercise of religion; the right to petition government for redress of grievances; and the right to privacy. Consistent with this policy, Department personnel shall comply with the dictates of the Investigations Ordinances and with the requirements of Department rules and regulations.

The Department will cooperate fully with the Investigations Ordinance auditor. The Auditor will be given total access to any and all files maintained by the Seattle Police Department except in the case of files or investigations which are specifically exempted from inspection by the Investigations Ordinances.

The Investigations Ordinance requires all Department personnel to safeguard the rights of persons involved in lawful political or religious activities and places restrictions on the documenting of certain types of information. While much of the Ordinances pertains to the activities of the Criminal Intelligence Section, the Ordinances is directed at the activities of the Department as a whole. Officers must keep the Ordinances in mind when writing reports. Any documentation of information concerning a person's sexual preferences or practices, or their political or religious activities must be for a relevant reason and serve a legitimate law enforcement purpose. Officers should also be aware of the Ordinances when photographing demonstrations or other lawful political activities. If demonstrators are not acting unlawfully, police can't photograph them. Periodic review of the Ordinances is worthwhile, as violations of the Ordinances could result in civil liability or disciplinary action, including discharge.

See SMC Chapter 14.12.

Site Disclaimer: The Seattle Police Department's website was developed to provide general information. Data contained at this location is generally not reviewed for legal sufficiency. SPD documents displayed are for reference purposes only. Their completeness or currency are not guaranteed. Links or references to other information or organizations are for reference only and do not constitute an endorsement.

ADA Notice

Notice of Nondiscrimination

Privacy

© Copyright 1995-2018 City of Seattle

Seattle Police Department Manual
Carmen Best, Chief of Police

12.040 - DEPARTMENT-OWNED COMPUTERS, DEVICES & SOFTWARE

Effective Date: 07/01/2018

12.040 - POL-1 General Policy

The Department follows the City's Information Systems Security Policy.

Employees using Department-owned devices or software will follow the City's security policy:

- Protect and never share access accounts, privileges, and associated passwords
- Maintain the confidentiality of sensitive information to which they are given access privileges
- Accept accountability for all activities associated with the use of their network accounts and related access privileges
- Ensure that use of City computers, email and other electronic communications (IM, etc.), Internet access, computer accounts, networks, and information stored, or used on any of these systems is restricted to authorized purposes and defined use limitations
- Maintain information security awareness.
- Report all suspected security and/or policy violations to an appropriate authority (e.g. manager, supervisor, system administrator or the Office of Information Security).

For this policy, the term device means any electronic equipment that has the capability to:

- Connect to the internet or department computer network and/or;
- Be used as a means of communication.

Exception: This policy does not apply to devices being used while conducting undercover operations. Employees will refer to their unit guidelines when using undercover devices.

12.040 - POL-2-Protecting Department Hardware, Software and Computer Systems

The City's Information Technology Department (ITD) ensures the security of computer systems and software. ITD will audit and monitor the use of the equipment and access to information.

1. Only Authorized Users Operating Authorized Devices May Access the Seattle Police Department's Computer Network

Employees will access the SPD network only with devices authorized by ITD.

- This requirement includes devices used by other agencies assisting SPD or vendors working with ITD.

2. ITD Controls Department-Owned Software

ITD will review and evaluate purchases of computer and device software. ITD will approve or reject the purchase of software based on internal policies and the City's ITD guidelines.

ITD will maintain the software licenses for Department-owned software.

3. ITD Monitors Software Use on Department Devices

ITD will audit the software used on Department computers and will remove unauthorized software.

4. Employees Will Not Violate the License Agreement of Department Software

Employees will not copy Department-owned software or install the software on any other computer.

5. Employees Will Not Install or Download Non-Department- Owned Software, Applications or Programs on Department Devices

6. With Approval from their Lieutenant/Civilian Equivalent or Above, Employees May Request New Applications and Software (including free technologies) by Completing the SPD Change or Enhancement Intake Request Form

This form is required for all requests to change any kind of IT system.

This includes, but is not limited to changes in hardware, network connections, addition or removal of applications, and additions or changes in application configurations, data elements, check lists, and drop down lists

The link to this form can be found below See 12.040-TSK-1 Submitting a Request for Change or Enhancement Intake Request

- Non-Department-owned software cannot interfere with the operation of any Department-owned software or hardware.

- The unit assigned the software will maintain the license agreement. A copy of the license agreement is sent to ITD by the unit.

7.Employees Will Report Malfunctions of IT, Systems or Software By Calling the Seattle ITD Service Desk at 4-HELP to Complete a HEAT Ticket

Seattle ITD (previously known as DoIT help desk) is available M-F, 8-5 for routine desktop equipment or software related issues. Seattle ITD can be reached via telephone at 4-HELP or 386-4011, or via e-mail at 4-Help@seattle.gov.

After hours assistance can also be requested via 4-HELP or 386-4011. After hours requests are handled by the on duty Seattle ITD personnel.

Seattle ITD assistance via SPD Radio is also available 24/7 via Zone 2 / ITS. This resource is for in-car equipment issues related to the VMDT. Assistance is also provided to patrol officers that need a password reset to complete their patrol related tasks.

8. Employees Will Not Use Unauthorized Encryption Tools on a Department Computer or Device

9. Employees Will Not Password-Protect a Work File or Hard Drive

Exception: A lieutenant or above may authorize an employee to password-protect a file or drive based on an investigative or operational need.

Exception: This does not apply to Department-required passwords for Department computers, programs or devices.

12.040 - POL-3-Using Department Devices

1. Employees Have No Expectation of Privacy When Using a Department Device

The Department has the right to review all records related to department devices including, but not limited to phone logs, text messages, photographs, email and internet usage.

2. Employees Use Devices in a Professional Manner

Employees will use Department devices to communicate in a professional, appropriate, and lawful manner both on and off-duty.

Employees are accountable for all transmissions made on department devices.

3. Personal Use of Department-Provided Devices Must Follow Department Guidelines

The Department allows limited, reasonable, personal use of Department devices with the knowledge that all use of Department devices may be monitored and subject to public disclosure.

Personal use of Department devices must not:

- Be illegal,
- Incur a cost to the City,
- Interfere with work responsibilities,
- Disrupt the workplace,
- Store unlicensed, copyrighted materials on any City-owned technology,
- Create a device-to-device connection between Non-City owned Technology and City-owned Technology,
- Comprise commercial or solicitation activities,

Or,

- Cause an embarrassment to the Department.

The Department may monitor and review all use of Department devices.

4. Department Devices Equipped with the VMobile Application Must Be Password Protected

Any use of the VMobile application must comply with Manual Section 12.050 - Criminal Justice Information Systems.

5. Employees Will Report Lost or Stolen Department Devices

In the event of a lost or stolen Department-issued device, the employee assigned the device must comply with 9.030-PRO-1 Reporting Destroyed, Lost, or Stolen Equipment.

6. Employees Will Not Access the VMobile Application in an Off-Duty, Unofficial Department Capacity

Off-duty use must comply with Manual Section 12.050 - Criminal Justice Information Systems.

7. The Act of Carrying a Department Device While Off-Duty Does Not, In Itself, Constitute Overtime

Overtime expectations vary by assignment. Supervisors will clarify their expectations for any off-duty use of Department devices. Unless an employee has been explicitly ordered by a supervisor to be available, check emails, or conduct other department business outside of normal shift hours, they are not expected or encouraged to do so.

See Manual Section 4.020-Reporting and Recording Overtime/Out-of-classification Pay

8. The Fiscal Unit Assists Employees with Cellular Phones

Employees making a request for a new or replacement cell phone will submit a 1.5 through their chain of command. Once approved, the Fiscal Unit will order the new phone and service.

9. The Department Telephone Coordinator Assists Employees with Desktop (Land-Line) Phones

Employees may contact the Telephone Coordinator at spd_telephone_coord@seattle.gov The Telephone Coordinator can assist employees in the acquisition of phones and moving phone numbers to new locations.

Section Captain or civilian equivalent will approve the acquisition or moving of desk phones.

10. Employees Will Not Use Department Devices Internationally Without the Approval of a Captain/Civilian Equivalent or Above

After captain or civilian equivalent approval, employees will contact ITD to upgrade their device plan for international use.

International travel with a Department device may incur roaming charges to the Department.

11. Employees Will Comply with All Department Public Disclosure Requests

See Manual Section 12.080 Department Records Access, Inspection and Dissemination.

12. When Receiving a Public Disclosure Request or Subpoena, Employees Must Retain All Requested Content

Employees will not delete requested items after receiving a public disclosure request or subpoena.

Department personnel may review content of any messages or photos contained on the device to make informed disclosure decisions.

13. Employees Will Retain Public Records According to the City Records Management Program

This includes, but is not limited to text messages and photographs.

Employees seeking long-term retention may elect to transfer the content from the device to an appropriate Department network or system.

14. Employees Will Hold and Preserve All Public Records Relating to Litigation or Anticipated Litigation

Employees will hold and preserve all requested records until the City Attorney's Office releases the legal hold.

Employees will retain all records, including transitory records, responsive to a pending public records request until the Department's response to the request has been completed.

15. Employees Acknowledge that Public Disclosure Laws Apply to Personally Owned Devices Used for Department Business

Employees using their personally-owned devices for official Department business and correspondence do so with the knowledge of this admonishment.

The Department prefers employees use Department-provided devices for Department-related matters.

Employees may request that their supervisor provide a Department-owned phone to make phone calls for official business.

16. The Department May Request Employees Review Their Own Personal Devices in Compliance with Public Disclosure Requests

The employee may be required to sign a declaration demonstrating the adequacy of the search of a personal cellphone or device regardless of whether the search resulted in responsive records.

Employees with questions regarding public disclosure may contact the Legal Unit.

17. Employees Will Not Charge Personally Owned Devices in Department USB Ports

Vehicle USB ports and USB ports that connect to a device may retain data from a personally owned device when plugged in.

Employees may use wall outlets or vehicle 12-volt DC sockets to charge personal devices.

12.040-TSK-1 Employees Submitting a Request for Change or Enhancement Intake Request

1. **Requests** approval for change via their chain of command to the level of Lieutenant/civilian equivalent or above

2. **Receives** approval for the request via their chain of command

3. **Clicks** here to complete an SPD Change or Enhancement Intake Form

4. **Completes** the fillable PDF form

5. **Clicks the "Click to Submit Form" button** on the request form PDF. An outlook email will automatically open.

6. **Selects** Default email application (Microsoft Outlook)

7. **Clicks Continue**

   When the Outlook email opens, it auto-populates the email recipient as SPD_ChangeRequest@Seattle.gov. It will also automatically attach your completed PDF change request and auto-populate the subject line as "Form Returned: SPD_ChangeRequest.pdf"

8. **CCs** their approving chain of command within the email request and **clicks send** to forward your email change request to ChangeRequest@Seattle.gov.

Site Disclaimer: The Seattle Police Department's website was developed to provide general information. Data contained at this location is generally not reviewed for legal sufficiency. SPD documents displayed are for reference purposes only. Their completeness or currency are not guaranteed. Links or references to other information or organizations are for reference only and do not constitute an endorsement.

ADA Notice

Notice of Nondiscrimination

Privacy

© Copyright 1995-2018 City of Seattle

Seattle Police Department Manual
Carmen Best, Chief of Police

12.050 - CRIMINAL JUSTICE INFORMATION SYSTEMS

Effective Date: 05/01/2017

Criminal Justice Information Services Security Policy

WSP ACCESS/WACIC/NCIC/User Acknowledgement

1. Definitions

Criminal History Record Information: Information contained in records collected by criminal justice agencies, other than courts, on individuals, consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition arising there from, including sentences, correctional supervision, and release. The term includes information contained in records maintained by or obtained from criminal justice agencies, other than courts, which records provide individual identification of a person together with any portion of the individual's record of involvement in the criminal justice system as an alleged or convicted offender, except:

- Posters, announcements, or lists for identifying or apprehending fugitives or wanted persons,
- Original records of entry maintained by criminal justice agencies to the extent that such records are compiled and maintained chronologically and are accessible only on a chronological basis,
- Court indices and records of public judicial proceedings, court decisions, and opinions, and information disclosed during public judicial proceedings, and
- Records of traffic violations that are not punishable by a maximum term of imprisonment of more than ninety days.

For the purposes of this policy, the RideAlong Response application is considered a criminal justice record system that contains criminal history record information.

Dissemination: Disclosing criminal history record information, or the absence of criminal history record information, to any person or agency outside the agency possessing the information, subject to the following exceptions:

- Agencies participating in a single (joint) record-keeping department,
- Furnishing information to process a matter through the criminal justice system (information to a prosecutor), and
- Reporting events to a record-keeping agency.

NCIC III: The National Crime Information Center Interstate Identification Index, managed by the FBI and state law enforcement agencies. The NCIC Advisory Policy Board has established a set of standards and goals that the FBI and state agencies enforce. The information contained in the NCIC includes all records collected by criminal justice agencies on individuals including identifiable descriptions, notations of arrests, detentions, indictments, formal criminal charges, dispositions, sentences, correctional supervision, and release. Federal, state and local laws and regulations dictate that this information is to

be accessed and used only by authorized individuals within a criminal justice agency, that this information is to be used for criminal justice reasons, that this information is to be kept confidential, and that this information is to be stored in a secure location.

- Employees must be working for the Seattle Police Department in an on-duty or extra-duty capacity and investigating a criminal offense.

- Employees shall not run names or make inquiries through NCIC III, or any other criminal record system while working for an off-duty employer or on behalf of an off-duty employer.

2. Inquiries Through ACCESS, or Any Other Criminal Justice Record System, Are Only to Be Made for Legitimate Law Enforcement Purposes

This includes, but is not limited to, inquiries made to DOL, DOC, WACIC, WASIS, NCIC III, LInX, and any inquiries processed through NLETS to other states. Inquiries made for personal use, or inappropriate use or dissemination of the information, can result in internal discipline, as well as penalties under Federal and State law.

3. All Employees Who Use Terminals That Have Access to Information in WACIC/NCIC Files Must Be Certified

After initial certification, employees shall take a recertification test every two years.

- For inquiries only, employees shall attain Level I certification.

- If employees make data entries into the system, they shall attain Level II certification.

4. SPD Must Remain in Compliance With the ACCESS/WACIC/NCIC User Acknowledgement or Risk Termination of One or More of the Services Provided

The ACCESS/WACIC/NCIC User Acknowledgement is the formal agreement between WSP and SPD. This document acknowledges the standards established in the FBI's Criminal Justice Information Service Security Policy. The standards require accuracy, completeness, timeliness, and security in the dissemination and recording of information.

5. Data Center Manager is the Technical Agency Coordinator

The Department must designate a Technical Agency Coordinator (TAC) to act as the point of contact for the WSP and the Federal Bureau of Investigation (FBI). The individual designated to function as a TAC will be responsible to ensure compliance with state and National Crime Information Center (NCIC) policies and regulations. The TAC must maintain a Level II training certification and attend TAC training once every three years. Additionally, the TAC shall participate in and ensure that all appropriate records be available during the triennial audit conducted by the ACCESS audit staff. Responsibility for proper operator performance, strict adherence to regulations, prompt notification of CJIS violations to the ACCESS Section, and subsequent training rests with the TAC. The SPD TAC is the Data Center Manager.

6. All Employees Shall Adhere to WASIS and NCIC Policies

Use of WASIS (Washington State Identification System and Criminal History Section) and NCIC Interstate Identification Index (NCIC III) is regulated by the FBI and WSP in accordance with the 28 CFR Part 20, WAC 446-20-260, and RCW Chapter 10.97. Improper use of the system may result in severe penalties to the Department and the individual user.

All employees shall adhere to the following WASIS and NCIC policies:

1. Any information obtained through these systems shall not be disseminated to anyone outside the Department, except to a prosecutor. If necessary, officers may confirm to a criminal justice agency the WASIS or FBI number, if it is known.

a. Examples of agencies and/or organizations to whom we cannot release criminal history information include, DSHS, Passport Agencies, CPS, Adult Protective Services, Crimestoppers, victims, and witnesses.

b. Inquiries for criminal history information from outside agencies, organizations, and individuals should be referred to Washington State Patrol.

2. Inquiries into these systems shall not be made in response to a request by another criminal justice agency or by any retired employees, including those holding any extended authority, special police commission, or similar police commission.

3. The Department of Justice Criminal Justice Information System (CJIS) restricts the use of all criminal-related data bases to official investigations when conducted while working for a criminal justice organization. As a result, no employee shall run names or make inquiries through ACCESS, WACIC, WASIS, NCIC III, LInX, or any other criminal record system while working for an off-duty employer or on behalf of an off-duty employer.

4. All NCIC III queries made through Versadex are stored in the system. A program has been developed to create an automated user log from that data.

5. This log is audited by the Washington State Patrol, the FBI, and the Compliance Section, and shall be available for inspection by any of the agencies at any time. The following procedures must be followed when accessing the Criminal History Database:

a. All NCIC III queries should be made using Transaction Code CQCH – Common Query Criminal History

b. The Purpose Code box must be filled in with 1 of the 2 authorized Purpose Codes that appear in the pull-down. The query will not go through if the box is left blank. The only authorized Purpose Codes are:

C - Criminal Justice purposes as well as authorized uses in relation to the security of the criminal justice facility including, vendors/contractors who are not involved with administration of criminal justice; e.g. janitors, maintenance personnel, visitors, etc.

J – Criminal Justice employment/applicants and re-background requirement for criminal justice agency personnel as well as vendors, contractors, volunteers, and interns, who are involved with the administration of criminal justice for the agency.

c. The Reason field must be filled in with a specific criminal justice reason. The general offense number should always be listed in the reason field if available. If a general offense number has not been generated the specific criminal justice reason must be listed in the reason field such as theft, narcotics, homicide, missing person, or criminal justice applicant. Listing terms such as investigation, arrest, criminal history, or employment in the reason field are not valid. Listing abbreviations of any kind in the reason field is not authorized unless the abbreviation has been approved and is on file with the department TAC.

6. An automated user log for all queries made using the Omnixx system is maintained by the Washington State Patrol. Data Center and Public Request Unit Personnel may request access to this log via the "Request for Off-Line Search." The following information must be included in the Attention Field (ATN) when making a criminal history inquiry using Omnixx:

a. Requestor's SPD serial number.

b. Specific criminal justice reason such as theft, narcotics, homicide, or general offense number.

c. Examples:

ATN/4000 WP Entry

ATN/4000 Burglary

ATN/4000 14-16735

d. Use of abbreviations is acceptable but must be on file and approved by the Department TAC.

e. The proper purpose code must be used for all inquiries.

7. The NCIC III system is to only be used by personnel involved in criminal investigations, and background investigations. As of 2/11/15, a NICS check will be required for firearms returns. The Public Request Unit is the only unit authorized to complete NICS checks.

8. MDCs and PDTs (mobile and portable data computers/terminals) are not authorized to access NCIC III information because the terminals are unable to comply with NCIC audit requirements.

9. It is important to enter inquiries to the Criminal History Records system properly. The following information must be accurate and complete on the inquiry mask:

a. The "Purpose Code" must be entered correctly, "C", for criminal investigation, or another appropriate code. See NCIC manual for details.

b. The "Requestor Full Name/Serial" must contain the name and SPD serial number of the person making the inquiry. It is not acceptable to use "Det", "Off", or the "unit title" in this field.

7. Employees Shall Not Discuss or Provide Information to Any Person Who Is Not a Member of the Criminal Justice System Without the Permission of the Chief of Police, or By Due Process of Law

The Washington State Criminal Records Privacy Act (RCW 10.97) provides for the completeness, accuracy, confidentiality, and security of criminal history record information, as well as victim, witness, and complainant record information. Employees shall not discuss or provide information to any person who is not a member of the criminal justice system (prosecuting attorney, court, etc.) without the permission of the Chief of Police, or by due process of law. Violations may lead to criminal sanctions.

8. Criminal Records Releases Are Restricted

Requests for information shall be referred to the appropriate section.

- Criminal history record information dissemination to individuals, agencies, or groups outside the Department shall be administered by the Records File Unit and Data Center Unit.

- Juvenile record information dissemination to individuals, agencies, or groups outside the Department shall be administered by the Records File Unit.

Printouts of criminal history record information from the Department's computerized and manual files are prohibited except when:

- Required for a detective investigative file
- Required by a prosecuting attorney
- Required by agencies or individuals authorized by the Records, Evidence and Identification Section access procedures
- Required in a mutual criminal investigation with a court or government agency authorized by the Washington State Patrol to receive criminal history record information
    - The Records File Unit and Data Center Unit shall maintain a current list of agencies so authorized.
- Authorized by a watch, section, or unit supervisor as required for an investigation or in an emergency

When releasing criminal history information to a prosecutor the release tracking function in Versadex should always be used to indicate release to either King County Prosecutor's Office or the City Law Department. The release tracking serves as the automated secondary dissemination log.

In authorized instances when criminal history is secondarily disseminated to any agency or person the following information relating to secondary dissemination of criminal history record information shall be maintained by the appropriate section in the form of a manual log and will include the following:

- An indication of to whom (agency or person) criminal history information was released,
- The date of release, and
- A brief description of the information released

The disposal of printouts from computer terminals shall be by destruction.

9. Individuals Have the Right to Inspect and Review Their Criminal History Record Information Maintained By the Department

A copy of the Department Operating Instruction titled, "Inspection and Review of Criminal History Record Information" and "Challenge and Deletion of Criminal History Record Information" shall be maintained at locations where the public can make inquiries concerning Department procedures.

An individual's right to access and review of their criminal history record information shall not extend to data contained in intelligence, investigative, or other related files and shall not be construed to include any information other than that defined as Criminal History Record Information by RCW 10.97.030.

In order to inspect, review, or challenge and have deleted criminal history record information, the individual must appear in person at the 1st floor of the Police Headquarters Building 610 Fifth Avenue, Monday through Thursday (excluding holidays) between the hours of 8:00 a.m. and 4:30 p.m., and make a request in writing on the forms provided.

- Employees are responsible for directing individuals to the Records File Unit in order to facilitate review of their criminal history record information.

An individual will be provided an opportunity, following review of the criminal history record information collected, stored, and maintained by the Department, to challenge the accuracy and completeness of the data and request deletion of certain non-conviction arrests.

If the challenge is rejected, the individual has a right to appeal the decision to the Office of the Chief of Police.

It shall be the duty of the Records File Unit manager and supervisors to administer the rules pertaining to an individual's right to review their criminal history record information, concurrent with the aforementioned laws, regulations, and ordinances.

10. All SPD Personnel Must Have a Background Re-Investigation Every Five Years

To complete this compliance measure the Department must:

- Run a criminal history inquiry using purpose code "J". Use "Criminal Justice Re-background" as a reason. Log the date and SID# of the employee. Do not retain rap sheet information.

  - If there are felony findings within the employee's rap sheet they will be denied continued use and certification with ACCESS. The TAC must notify the WSP Information Security Officer of any findings.

  - If there are charges pending a disposition, the TAC must notify the WSP Information Security Officer (ISO).

  - If there are misdemeanor findings the TAC shall notify the WSP Information Security Officer. The Seattle Police Department will ultimately decide whether to limit ACCESS.

  - Keep a log of all personnel SID numbers and the date of the background re-investigation for future ACCESS audits.

11. SPD Must Comply With ACCESS/NCIC Security Requirements

All upper management and administrators/managers who are not ACCESS-certified but oversee certified ACCESS users must review the Upper Management and Administrator Overview Training. Upon review of the training, they must sign the Upper Management and Administrator Log. There is no requirement to reaffirm this training.

All employees must complete the Security Awareness Training within six months of initial hire. Any employee not Level I or Level II-certified must review the Security Awareness Training every two years.

Maintaining security of the terminal sites and information received is the responsibility of agency personnel operating the terminal, the TAC, and the agency head. Terminal locations must be secure from authorized access, and all employees authorized to use the system shall be instructed on the proper use of equipment and the dissemination of information received. Federal and state laws protect the information provided by ACCESS.

Violations of the rules, regulations, policies, or procedures developed by FBI and adopted by the WSP or any other misuse or abuse of the ACCESS system may result in agency disciplinary measures and/or criminal prosecution. Disciplinary measures imposed by the WSP may include revocation of individual certification, discontinuance of system access to the department, or purging the department's records.

Any misuse of the NCIC III system must be reported to the TAC (Data Center Manager) immediately. The TAC shall report the misuse to the Washington State Patrol and the FBI. The violator's chain of command will be notified of the misuse.

12. The Captain of the Compliance Section Will Assign Personnel to Conduct Regular Audits of the Department's Criminal History Records Inquiries

The Department audits will be completed biannually and the results of these audits will be reported to

the Chief Operating Officer.

The audit will look for any violations of the CJIS Security Policy, The WSP User Acknowledgement, and Department Policy. Violations include but are not limited to:

- Queries made for personal reasons
- Reason Field errors, such as using general terms such as investigation, arrest, warrant, criminal history
    - The Reason Field must contain a specific crime such as murder, assault, burglary.

Any users who are in violation of any or all of the above will have their access to the Criminal History system shut off. Access will be denied until they have attended a remedial class for making Criminal History inquiries.

- An e-mail will be sent to the employee and their immediate supervisor from the Compliance Section Captain that their access to the Criminal History system has been denied.
- The e-mail will contain information about the remedial classes that they must take in order to regain access.
- A copy of the e-mail will be sent to the Data Center Manager/TAC for implementation.

Site Disclaimer: The Seattle Police Department's website was developed to provide general information. Data contained at this location is generally not reviewed for legal sufficiency. SPD documents displayed are for reference purposes only. Their completeness or currency are not guaranteed. Links or references to other information or organizations are for reference only and do not constitute an endorsement.

ADA Notice

Notice of Nondiscrimination

Privacy

© Copyright 1995-2018 City of Seattle

Seattle Police Department Manual

Carmen Best, Chief of Police

12.055 - CRIMINAL JUSTICE RESEARCH

Effective Date: 8/15/2012

12.055–POL

This policy pertains to the Department's facilitation of research.

1. The Department Encourages Criminal Justice Research and will Facilitate Research as Allowed by Law and Available Resources

The Department may permit researchers to have direct access to police files and/or personnel under properly executed research and confidentiality agreements.

- The Chief of Staff will have final approval over outside research requests.
- A written Research Agreement is required for the release of any Department data for research, evaluative or statistical purposes.
- Research requests for criminal history shall comply with WAC 446-20-420.

2. Agencies, Institutions and Individuals Desiring the Use of Police Records for Research will Use the Seattle Police Department Research Request Instructions as a Guide to Complete a Request

Click here for instructions.

3. The Compliance Section will Receive and Vet all Outside Research Requests

See 12.055–PRO–1 Vetting Process for Outside Research Requests

The following questions will be considered when requests are analyzed:

- Is the information requested available?
- What is the estimated cost to complete the request?
- Personnel time
- File research
- Copying
- Can the additional workload required to complete the request be absorbed at the time it is requested?
- How will the completed research project be beneficial to the Department or to the criminal justice system?
- Are there privacy issues?
- Does the request comply with RCW 13.50.010?

4. Costs Shall be Forwarded to the Fiscal Section for Billing and Reimbursement

5. Department Employees are Encouraged to Submit Their Own Ideas for Research Topics

See 12.055–PRO–2 Receiving Internal Ideas for Research Topics

The Compliance Section Captain will maintain a list of research topics for assignment within the SPD-University of Washington Research Consortium.

6. The Compliance Section will Review Results of Completed Research and Determine if There is a Practical Application to Department Operations

12.055–PRO–1 Vetting Process for Outside Research Requests

Compliance Section Captain

1. **Receives** outside research request

Assigned Compliance Section Staff:

2. **Reviews** request
3. **Prepares** recommendation on how to proceed
4. **Shares** recommendation with work group (Compliance Section Sergeant, legal advisors, Records Manager, and Grants and Contracts Manager).

Work Group

5. **Reviews** the recommendation

Assigned Compliance Section Staff

6. **Schedules** a meeting with the work group and the Compliance Section Captain
   a. The chief or captain of the Bureau or Section which will benefit from, or be affected by, the research project may also be included.

Compliance Section Captain

7. **Determines** whether Compliance Section will endorse the request
   a. If Compliance Section will not endorse, then advises the work group
   b. If Compliance Section will endorse, then forwards the request to the Chief of Staff

Chief of Staff

8. **Determines** whether SPD will endorse the request
   a. If SPD will endorse, signs research agreement on behalf of the Department

Assigned Compliance Section Staff

9. **Advises** requester of the Department's decision via formal letter

12.055–PRO–2 Receiving Internal Ideas for Research Topics

Any SPD employee

1. **Develops** an idea for a research topic
2. **Submits** an e-mail to the Compliance Section, with the subject line: Research Topic

Assigned Compliance Section Staff

3. **Reviews** the memo
4. **Develops** a specific research topic
5. **Follows-up** with the employee
    a. **Verifies** that his research topic is consistent with the employee's intent
6. **Submits** research topic to Compliance Section Captain

Compliance Section Captain

7. **Maintains** file of research topics

Site Disclaimer: The Seattle Police Department's website was developed to provide general information. Data contained at this location is generally not reviewed for legal sufficiency. SPD documents displayed are for reference purposes only. Their completeness or currency are not guaranteed. Links or references to other information or organizations are for reference only and do not constitute an endorsement.

ADA Notice

Notice of Nondiscrimination

Privacy

© Copyright 1995-2018 City of Seattle

Seattle Police Department Manual

Carmen Best, Chief of Police

12.080 - DEPARTMENT RECORDS ACCESS, INSPECTION & DISSEMINATION

Effective Date: 11/20/2013

12.080-POL

This policy applies to access, inspection and dissemination of Department records.

1. All Records are Subject to Public Disclosure Unless a Specific Legal Exemption Exists

Per RCW 42.56.070, the Department must make all public records available to a requester, unless the record falls within the specific exemptions in the Public Records Act (PRA) or other statute which exempts or prohibits disclosure of specific information or records.

2. Public Records are Available for Release to the Maximum Extent Allowed by Law

A public record is any writing containing information relating to the conduct of the Department or the performance of any governmental or proprietary function prepared, owned, used, or retained by the Department, regardless of physical form or characteristics.

- Public records may include records received or created that relate to the conduct of the Department or the performance of any governmental or proprietary function and are prepared, owned, used, or retained by the Department.
- The Department frequently receives records from outside agencies. Any and all records that are in the Department's possession are Department records for the purposes of PRA.
- Writing means handwriting, typewriting, printing, photostating, photographing, and every other means of recording any form of communication or representation, including, but not limited to, letters, words, pictures, sounds, symbols, or combination thereof, and all papers, maps, magnetic or paper tapes, photographic films and prints, motion picture, film and video recordings, magnetic or punched cards, discs, drums, diskettes, sound recordings, and other documents including existing data compilations from which information may be obtained or translated.

Under RCW 42.56 Public Records Act (PRA) as interpreted by Washington courts, all Department records must be identified to the public, so long as the records are not part of an open and active investigation.

Exception: Department records that fall under a specific exemption within the PRA or other statute are not required to be identified to the public. Specific exemptions include, but are not limited to, public safety considerations and privacy concerns.

- The Department cannot withhold an entire record because portions of it fall under an exemption. The Department shall redact exempted information and release the record with an explanation for any redactions.

3. All Records That Relate to a Public Disclosure Request (PDR) Must Be Provided or Identified to the Public Disclosure Unit (PDU)

If an employee withholds known records that relate to a PDR, he or she may be subject to civil liability and/or Department discipline.

- Employees are advised to contact PDU (684-4848 or spdpdr@seattle.gov) when they are uncertain as to whether documents that they have constitute records that relate to a PDR.

4. Officers/Detectives Must Ask Victims, Witnesses and Complainants if They Want Their Identifying Information Disclosed or Not Disclosed

When gathering information at the time of reporting, officers and detectives must ask victims, witnesses and complainants if they want their identifying information disclosed or not disclosed. This decision supersedes any disclosure requests made by another person.

- When a victim, witness or complainant is unable to discuss disclosure due to incapacity, the reporting officer shall:
- Document the incapacity in the entity portion of the General Offense Report, and
- Document any specific evidence that disclosure of the identity of the victim, witness or complainant would threaten life, safety or property.

5. PDU Responds to PDRs

The Public Disclosure Unit (PDU) handles all public disclosure requests (PDRs) in accordance with the Public Records Act (PRA). See 12.080-PRO-1 Handling Public Disclosure Requests.

- Any Department employee who receives a PDR, or any request that appears to be a PDR, shall immediately forward it to spdpdr@seattle.gov.
- The request does not have to cite the PRA.

There are four options for member of the public to submit PDRs:

- E-mail: spdpdr@seattle.gov (preferred method)
- Mail: SPD PDU; PO Box 34986; 610 5th Ave; Seattle, WA 98124-4986
- Fax: (206) 684-5240
- In-person at the public counter at SPD Headquarters, 610 5th Ave.

6. Public Request Unit (PRU) Responds to Certain Requests

The PRU handles the following:

- Requests for police reports
- Requests for clearance letters
- Fingerprinting and criminal background checks on applicants for concealed pistol licenses
- Fingerprinting criminal justice applicants
- Fingerprinting citizens for general purposes
- Processing applications for transferring ownership of handguns
- Electronically redacting police reports for release to the SPD My Neighborhood Map website

7. Crime Records Unit (CRU) Responds to Certain Requests

The CRU receives and records all incoming requests for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies.

8. The Public Disclosure Request Steering Committee Resolves Complex PDR

The PDR Steering Committee, which meets each Monday, is comprised of the Chief Administrative Officer, PDU Manager and staff, Records Manager, SPD Legal Advisor, Compliance Section Captain or designee, and one or more representatives of the Seattle Law Department.

See 12.080-PRO-1 Handling Public Disclosure Requests.

12.080-PRO-1 Handling Public Disclosure Requests

PDU

1. **Receives** PDR
2. **Contacts** relevant units or specific employees to **request** records and **provides** a due date

Relevant Unit/Employee

3. **Gathers** all relevant records and **contacts** PDU with any questions

   a. If an employee believes that some or all of the information in the record(s) is protected from public disclosure, **provides** the record(s) to the PDU, with a memo stating what should be protected and why

   b. Whether the record(s) at issue is protected from public disclosure shall be discussed at the next meeting of the PDR Steering Committee

   - Absent conflicting advice from the Law Department and the SPD Legal Advisor, the Chief Administrative Officer shall determine whether record(s) will be disclosed wholly or in part, and whether any exemptions apply.
   - When there is conflicting advice from legal counsel, the issue shall be elevated to the Chief of Staff and the Law Department's Chief of the Civil Division for resolution.

4. **Provides** records to PDU by the due date

PDU

5. **Collects** records and **makes** any and all necessary redactions
6. **Provides** records to the requestor

Site Disclaimer: The Seattle Police Department's website was developed to provide general information. Data contained at this location is generally not reviewed for legal sufficiency. SPD documents displayed are for reference purposes only. Their completeness or currency are not guaranteed. Links or references to other information or organizations are for reference only and do not constitute an endorsement.

ADA Notice

Notice of Nondiscrimination

Privacy

© Copyright 1995-2018 City of Seattle

Seattle Police Department Manual

Carmen Best, Chief of Police

12.111 - USE OF CLOUD STORAGE SERVICES

Effective Date: 03/01/17

12.111-POL

The Seattle Police Department receives information from the FBI's Criminal Justice Information Service (CJIS) and must comply with the CJIS security policy and the rules governing the access, use, and dissemination of CJIS information found in Title 28, Part 20, CFR

SPD employees deal with CJIS data as part of daily Department business. This policy applies to employee use of cloud storage services as a whole and as it specifically relates to CJIS data.

1. Definitions

Cloud storage services are electronic, external storage locations where information can be deposited for shared use. Examples include OneDrive, DropBox, Google Drive, iCloud, etc.

Criminal Justice Information (CJI) is the term used to refer to all of the FBI provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

Personally Identifiable Information (PII) a subset of CJI, is information which can be used to distinguish or trace an individual's identity, such as name, social security number, biometric records, date and place of birth, or mother's maiden name.

Criminal History Record Information (CHRI), sometimes informally referred to as "restricted data", is also subset of CJI.

Restricted Files are hosted by the National Crime Information Center (NCIC) and are treated as CHRI. Restricted Files include the following:

- Gang Files
- Known or Appropriately Suspected Terrorist Files
- Supervised Release Files
- National Sex Offender Registry Files
- Historical Protection Order Files of the NCIC
- Identity Theft Files
- Protective Interest Files
- Person With Information (PWI) data in the Missing Person Files
- Violent Person File
- NICS Denied Transactions File

2. Employees May Only Store, Edit, and Share City Files on Cloud Storage Services Provided By the Department or the City

Employees may store, edit, and share files on city-provided cloud storage such as Microsoft Office 365's OneDrive.

Employees will not use personal cloud storage services, such as Drop Box Google Drive, and iCloud, for any city file.

Site Disclaimer: The Seattle Police Department's website was developed to provide general information. Data contained at this location is generally not reviewed for legal sufficiency. SPD documents displayed are for reference purposes only. Their completeness or currency are not guaranteed. Links or references to other information or organizations are for reference only and do not constitute an endorsement.

ADA Notice

Notice of Nondiscrimination

Privacy

© Copyright 1995-2018 City of Seattle

Seattle Police Department Manual

Carmen Best, Chief of Police

16.170 - AUTOMATIC LICENSE PLATE READERS

Effective Date: 8/15/2012

16.170-POL

This policy applies to the use of automatic license plate readers (ALPR) by Department employees.

1. Criminal Intelligence Section has Operational Control

The ALPR system administrator will be a member of the Technical and Electronic Support Unit (TESU).

2. Operators Must be Trained

Operators must be ACCESS certified and trained in the proper use of ALPR.

- Training will be administered by TESU and Parking Enforcement, as applicable.

3. ALPR Operation Shall be for Official Department Purposes

ALPR may be used during routine patrol or any criminal investigation.

4. Only Employees With ACCESS Level 1 Certification May Access ALPR Data

Employees are permitted to access ALPR data only when the data relates to a specific criminal investigation.

- A record of requests to review stored ALPR data will be maintained by TESU.

Site Disclaimer: The Seattle Police Department's website was developed to provide general information. Data contained at this location is generally not reviewed for legal sufficiency. SPD documents displayed are for reference purposes only. Their completeness or currency are not guaranteed. Links or references to other information or organizations are for reference only and do not constitute an endorsement.

ADA Notice

Notice of Nondiscrimination

Privacy

© Copyright 1995-2018 City of Seattle

Part 3 - ENFORCEMENT

Chapter 11.30 - IMPOUNDING

Sections:

11.30.010 - Impoundment defined.

"Impoundment" means removal of a vehicle to a storage facility either by an officer or authorized agent of the Seattle Police Department or by a contractor for towing and storage in response to a request from an officer or authorized agent of the Seattle Police Department or the Seattle Housing Authority.

(Ord. 117306 § 1, 1994: Ord. 108200 , § 2(11.30.010), 1979.)

11.30.020 - Vehicle defined.

The term "vehicle" as used in this chapter shall have the definition set forth in Section 11.14.710 and, in addition, shall include any vehicle hulk as the same is defined in Section 11.14.045.

(Ord. 108200 , § 2(11.30.020), 1979.)

11.30.030 - Applicable State law adopted by reference.

Applicable provisions of Chapter 46.55 RCW, as now or hereafter amended, are hereby incorporated into Seattle Municipal Code Chapter 11.30 by this reference.

(Ord. 117306 § 2, 1994.)

11.30.040 - When a vehicle may be impounded without prior notice.

A. A vehicle may be impounded with or without citation and without giving prior notice to its owner as required in Section 11.30.060 hereof only under the following circumstances:

1. When the vehicle is impeding or is likely to impede the normal flow of vehicular or pedestrian traffic; or
2. When the vehicle is illegally occupying a truck, commercial load zone, restricted parking zone, bus, loading, hooded-meter, taxi, street construction or maintenance, or other similar zone where, by order of the Director of Transportation or Chiefs of Police or Fire or their designees, parking is limited to designated classes of vehicles or is prohibited during certain hours, on designated days or at all times, if the zone has been established with signage for at least twenty-four (24) hours giving notice that a vehicle will be removed if illegally parked in the zone and where such vehicle is interfering with the proper and intended use of such zones; or
3. When a vehicle without a special license plate, card, or decal indicating that the vehicle is being used to transport a disabled person as defined under Chapter 46.16 RCW, as now or hereafter amended, is parked in a stall or space clearly and conspicuously marked as provided in Section 11.72.065 A, as now or hereafter amended, whether the space is provided on private property without charge or on public property; or
4. When the vehicle poses an immediate danger to the public safety; or
5. When a police officer has probable cause to believe that the vehicle is stolen; or

6. When a police officer has probable cause to believe that the vehicle constitutes evidence of a crime or contains evidence of a crime, if impoundment is reasonably necessary in such instance to obtain or preserve such evidence; or

7. When a vehicle is parked in a public right-of-way or on other publicly owned or controlled property and there are four or more parking infractions issued against the vehicle for each of which a person has failed to respond, failed to appear at a requested hearing, or failed to pay a parking infraction for at least 45 days from the date of the filing of the notice of infraction;

8. When the vehicle is a "junk motor vehicle" as defined in SMC 11.14.268, and is parked on a street, alley, or way open to the public, or on municipal or other public property.

9. When the vehicle is impounded pursuant to Section 11.30.105A, but if the vehicle is a commercial vehicle and the driver is not the registered owner of the vehicle, then the police officer shall attempt in a reasonable and timely manner to contact the registered owner before impounding the vehicle and may release the vehicle to the registered owner if the registered owner is reasonably available, was not in the vehicle at the time it was stopped and the driver arrested, and has not received a prior release under this Subsection 11.30.040 A9 or Subsection 11.30.120 C2.

10. When a vehicle with an expired registration of more than forty-five days is parked on a public street.

11. When the vehicle is impounded pursuant to Section 12A.10.115.

12. When the vehicle is impounded pursuant to Washington Laws of 2011, chapter 167, section 3.

B. Nothing in this section shall be construed to authorize seizure of a vehicle without a warrant where a warrant would otherwise be required.

(Ord. 123632, § 9, 2011; Ord. 123447, § 2, 2010; Ord. 123190, § 8, 2009; Ord. 123035, § 3, 2009; Ord. 121525 § 4, 2004; Ord. 120102 § 1, 2000; Ord. 119782 § 1, 1999; Ord. 119180 § 3, 1998; Ord. 117306 § 3, 1994; Ord. 114518 § 4, 1989; Ord. 111835 § 1, 1984; Ord. 108200 , § 2(11.30.040), 1979.)

11.30.060 - When a vehicle may be impounded after notice.

A vehicle not subject to impoundment under Section 11.30.040 may be impounded after notice of such proposed impoundment has been securely attached to and conspicuously displayed on the vehicle for a period of twenty-four (24) hours prior to such impoundment, for the following reasons:

A. When such vehicle is parked and/or used in violation of any law, ordinance or regulation; or

B. When such vehicle is abandoned, as that term is defined in SMC 11.14.015, as now or hereafter amended; or

C. When such vehicle is so mechanically defective as to be unsafe for operation; provided, however, that this section shall not be construed to prevent the operation of any such defective vehicle to a place for correction of equipment defect in the manner directed by any peace officer.

(Ord. 120102 § 2, 2000; Ord. 117306 § 4, 1994: Ord. 108200 , § 2(11.30.060), 1979.)

11.30.080 - How impoundment is to be effected.

When impoundment is authorized by this chapter, a vehicle may be impounded either by an officer or authorized agent of the Police Department or by a contractor for towing and storage acting at the request

of an officer or authorized agent of the Police Department or Seattle Housing Authority and in accordance with a contract authorized by Section 11.30.220.

(Ord. 117306 § 5, 1994: Ord. 108200 , § 2(11.30.080), 1979.)

11.30.100 - Owner of impounded vehicle to be notified.

A. Not more than twenty-four (24) hours after impoundment of any vehicle, the tow contractor shall mail a notice by first class mail to the last known and legal owners of the vehicles, as may be disclosed by the vehicle identification number, and as provided by the Washington State Department of Licenses. The notice shall contain the full particulars of the impoundment, redemption, and opportunity for hearing to contest the propriety of the impoundment as hereinafter provided.

B. Similar notice shall be given to each person who seeks to redeem an impounded vehicle, except that if a vehicle is redeemed prior to the mailing of notice, then notice need not be mailed.

C. The Seattle Police Department shall give written notification to the last registered and legal owner that the investigatory hold has been removed, except that if a vehicle is redeemed following notice by telephone and prior to the mailing of notice, then notice need not be mailed. In addition, the Police Department shall notify the towing contractor, by telephone or in writing, of the authorization to release such vehicle.

(Ord. 117306 § 6, 1994; Ord. 108200 , § 2(11.30.100), 1979.)

11.30.105 - Impoundment of vehicle where driver is arrested for a violation of Section 11.56.320 B or C or Section 11.56.020—Period of impoundment.

A. Whenever the driver of a vehicle who is also the registered owner of the vehicle is arrested for a violation of Section 11.56.020, 11.56.320 B or C, the vehicle is subject to impoundment at the direction of a police officer. For purposes of this subsection, "arrested" includes, but is not limited to, being temporarily detained under Section 12A.02.140 B and served with a citation and notice to appear pursuant to Section 12A.02.140 C and RCW 46.64.015.

B. Reserved.

C. Reserved.

D. If a vehicle is impounded because the driver is arrested for a violation of Section 11.56.320 B or C and the Washington Department of Licensing's records show that the driver has not been convicted of a violation of RCW 46.20.342(1)(a) or (b) or similar local ordinance within the past five (5) years, the vehicle shall be impounded for thirty (30) days.

E. If a vehicle is impounded because the driver is arrested for a violation of Section 11.56.320 B or C and the Washington Department of Licensing's records show that the driver has been convicted one (1) time of a violation of RCW 46.20.342(1)(a) or (b) or similar local ordinance once within the past five (5) years, the vehicle shall be impounded for sixty (60) days.

F. If a vehicle is impounded because the driver is arrested for a violation of Section 11.56.320 B or C and the Washington Department of Licensing's records show that the driver has been convicted of a violation of RCW 46.20.342(1)(a) or (b) or similar local ordinance two (2) or more times within the past five (5) years, the vehicle shall be impounded for ninety (90) days.

(Ord. 121483 § 1, 2004; Ord. 120006 § 1, 2000; Ord. 12005 § 1, 2000; Ord. 119180 § 4, 1998.)

11.30.120 - Redemption of impounded vehicles

Vehicles impounded by the City shall be redeemed only under the following circumstances:

A. The vehicle may be redeemed only by the following persons or entities: the legal owner; the registered owner; a person authorized in writing by the registered owner; the vehicle's insurer or a vendor working on behalf of the vehicle's insurer; a third-party insurer that has a duty to repair or replace the vehicle, has obtained consent from the registered owner or the owner's agent to move the vehicle, and has documented that consent in the insurer's claim file, or a vendor working on behalf of a third-party insurer that has received such consent; a person, who is known to the registered or legal owner of a motorcycle or moped, as each are defined in Chapter 11.14, that was towed from the scene of an accident, may redeem the motorcycle or moped as a bailment in accordance with chapter 46.55 RCW, as amended by Chapter 152, Section 4, Laws of 2017, while the registered or legal owner is admitted as a patient in a hospital due to the accident; provided, however, that at all times the registered owner must be granted access to and may reclaim possession of the vehicle. For the purposes of this subsection 11.30.120.A, "owner's agent" means the legal owner of the vehicle, a driver in possession of the vehicle with the registered owner's permission, or an adult member of the registered owner's family; a person who is determined and verified by the operator to have the permission of the registered owner of the vehicle; or a person who has purchased the vehicle from the registered owner, who produces proof of ownership or authorization and signs a receipt therefore. A person redeeming a vehicle impounded pursuant to Section 11.30.105 must prior to redemption establish that he or she has a valid driver's license and is in compliance with Section 11.20.340. A vehicle impounded pursuant to Section 11.30.105 can be released only pursuant to a written release authorization from the Seattle Police Department pursuant to subsection 11.30.120.C or a written release authorization or order from Municipal Court pursuant to subsection 11.30.120.B or 11.30.120.C.

B. Any person so redeeming a vehicle impounded by the City shall pay the towing contractor for costs of impoundment (removal, towing, and storage) and administrative fee prior to redeeming such vehicle. Such towing contractor shall accept payment as provided in RCW 46.55.120(1)(b), as now or hereafter amended. If the vehicle was impounded pursuant to Section 11.30.105 and was being operated by the registered owner when it was impounded, it may not be released to any person until all penalties, fines, or fees owed by the registered owner to the City of Seattle have been satisfied by payment in full, by establishment of a time payment agreement with the Municipal Court, or by other means acceptable to the Municipal Court. If the vehicle was impounded pursuant to Section 11.30.040.A.7, it may not be released to any person until all penalties, fines, or fees on all parking infractions described in that section, and all booting, removal, towing, storage, lost boot, and administrative fees charged against the vehicle and owed by the registered owner to the City of Seattle have been satisfied by payment in full or through a time payment plan. Upon payment in full or time payment arrangement of such obligations, the court may issue a written release authorization allowing the vehicle to be released from impoundment.

C. The Chief of Police or Municipal Court shall release a vehicle impounded pursuant to Section 11.30.105 prior to the expiration of any period of impoundment:

1. Upon petition of the spouse of the driver, or the person registered pursuant to Ordinance 117244 as the domestic partner of the driver, based on economic or personal hardship to such spouse or domestic partner resulting from the unavailability of the vehicle and after consideration of the threat to public safety that may result from release of the vehicle, including, but not limited to, the driver's criminal history, driving record, license status, and access to the vehicle; or

2. If the registered owner of the vehicle was not the driver, did not know that the driver's license was suspended or revoked and has not received a prior release under this Subsection 11.30.120 C2 or Subsection 11.30.040 A9.

In order to avoid discriminatory application, the Chief of Police and Municipal Court shall deny release without discretion in all circumstances other than for the reasons set forth in this Subsection

11.30.120 C. If such release is authorized, the person redeeming the vehicle still must satisfy the requirements of Section 11.30.120 A and B.

D. Any person seeking to redeem a vehicle impounded as a result of a parking or traffic citation or under Section 12A.10.115 has a right to a hearing before a Municipal Court judicial officer to contest the validity of an impoundment or the amount of removal, towing, and storage charges or administrative fee if such request for hearing is in writing, in a form approved by the Municipal Court and signed by such person, and is received by the Municipal Court within ten (10) days (including Saturdays, Sundays, and holidays) of the latter of the date the notice was mailed to such person pursuant to Section 11.30.100 A or B, or the date the notice was given to such person by the registered tow truck operator pursuant to RCW 46.55.120(2)(a). Such hearing shall be provided as follows:

1. If all of the requirements to redeem the vehicle, including expiration of any period of impoundment under Section 11.30.105, have been satisfied, then the impounded vehicle shall be released immediately, and a hearing as provided for in Section 11.30.160 shall be held within ninety (90) days of the written request for hearing.

2. If not all of the requirements to redeem the vehicle, including expiration of any period of impoundment under Section 11.30.105, have been satisfied, then the impounded vehicle shall not be released until after the hearing provided pursuant to Section 11.30.160, which shall be held within two (2) business days (excluding Saturdays, Sundays and holidays) of the written request for hearing.

3. Any person seeking a hearing who has failed to request such hearing within the time specified in Section 11.30.120 D may petition the Municipal Court for an extension to file a request for hearing. Such extension shall only be granted upon the demonstration of good cause as to the reason(s) the request for hearing was not timely filed. For the purposes of this section, "good cause" shall be defined as circumstances beyond the control of the person seeking the hearing that prevented such person from filing a timely request for hearing. In the event such extension is granted, the person receiving such extension shall be granted a hearing in accordance with this chapter.

4. If a person fails to file a timely request for hearing and no extension to file such a request has been granted, the right to a hearing is waived, the impoundment and the associated costs of impoundment and administrative fee are deemed to be proper, and the City shall not be liable for removal, towing, and storage charges arising from the impoundment.

5. In accordance with RCW 46.55.240 (1)(d), a decision made by a Municipal Court judicial officer may be appealed to Municipal Court for final judgment. The hearing on the appeal under this subsection shall be de novo. A person appealing such a decision must file a request for an appeal in Municipal Court within fifteen (15) days after the decision of the Municipal Court judicial officer and must pay a filing fee in the same amount required for the filing of a suit in district court. If a person fails to file a request for an appeal within the time specified by this section or does not pay the filing fee, the right to an appeal is waived and the Municipal Court judicial officer's decision is final.

(Ord. 125344 , § 1, 2017; Ord. 124302, § 6, 2013; Ord. 123447, § 3, 2010; Ord. 123190, § 9, 2009; Ord. 121525 § 5, 2004; Ord. 121483 § 2, 2004; Ord. 120007 § 1, 2000; Ord. 120006 § 2, 2000; Ord. 119180 § 5, 1998: Ord. 117306 § 7, 1994: Ord. 115634 § 1, 1991: Ord. 110106 § 1, 1981: (Ord. 108200 , § 2(11.30.120), 1979.)

11.30.160 - Post-impoundment hearing procedure.

Hearings requested pursuant to Section 11.30.120 shall be held by a Municipal Court judicial officer, who shall determine whether the impoundment was proper and whether the associated removal, towing, storage, and administrative fees were proper. The Municipal Court judicial officer shall not have the

authority to determine the commission or mitigation of any parking infraction unless a timely response under Section 11.31.050 A was filed to that notice of infraction requesting a hearing and the hearing date for that infraction has not passed, in which case the Municipal Court judicial officer has discretion to consolidate the impoundment hearing and the notice of infraction hearing.

A. At the hearing, an abstract of the driver's driving record is admissible without further evidentiary foundation and is prima facie evidence of the status of the driver's license, permit, or privilege to drive and that the driver was convicted of each offense shown on the abstract. In addition, a certified vehicle registration of the impounded vehicle is admissible without further evidentiary foundation and is prima facie evidence of the identity of the registered owner of the vehicle.

B. If the impoundment is found to be proper, the Municipal Court judicial officer shall enter an order so stating. In the event that the costs of impoundment (removal, towing, and storage) and administrative fee have not been paid or any other applicable requirements of Section 11.30.120 B have not been satisfied or any period of impoundment under Section 11.30.105 has not expired, the Municipal Court judicial officer's order shall also provide that the impounded vehicle shall be released only after payment to the City of any fines imposed on any underlying traffic or parking infraction and satisfaction of any other applicable requirements of Section 11.30.120 B and payment of the costs of impoundment and administrative fee to the towing company and after expiration of any period of impoundment under Section 11.30.105. In the event that the Municipal Court judicial officer grants time payments for the costs of impoundment and administrative fee, the City shall be responsible for paying the costs of impoundment to the towing company. The Municipal Court judicial officer shall grant such time payments only in cases of extreme financial need, and where there is an effective guarantee of payment.

C. If the impoundment is found to be improper, the Municipal Court judicial officer shall enter an order so stating and order the immediate release of the vehicle. If the costs of impoundment and administrative fee have already been paid, the Municipal Court judicial officer shall enter judgment against the City and in favor of the person who has paid the costs of impoundment and administrative fee in the amount of the costs of the impoundment and administrative fee.

D. In the event that the Municipal Court judicial officer finds that the impound was proper, but that the removal, towing, storage, or administrative fees charged for the impoundment were improper, the Municipal Court judicial officer shall determine the correct fees to be charged. If the costs of impoundment and administrative fee have been paid, the Municipal Court judicial officer shall enter a judgment against the City and in favor of the person who has paid the costs of impoundment and administrative fee for the amount of the overpayment.

E. No determination of facts made at a hearing under this section shall have any collateral estoppel effect on a subsequent criminal prosecution and such determination shall not preclude litigation of those same facts in a subsequent criminal prosecution.

F. An appeal of the Municipal Court judicial officer's decision in Municipal Court shall be conducted according to, and is subject to, the procedures of this section. If the court finds that the impoundment or the removal, towing, storage, or administrative fees are improper, any judgment entered against the City shall include the amount of the filing fee.

(Ord. 120006 § 3, 2000: Ord. 119180 § 6, 1998: Ord. 115634 § 3, 1991: Ord. 110106 § 2, 1981: Ord. 108200 , § 2(11.30.160), 1979.)

11.30.180 - Responsibility for fees as to standby time or vehicles held for investigatory purposes.

A. No fee shall be assessed against the owner of a vehicle for time elapsed after the towing equipment has arrived at the location of the vehicle to be towed and prior to the operation of the towing equipment or performance of the impound service.

B. No impoundment fee and/or towing or storage charges shall be assessed against the owner of a vehicle which is being held for investigatory purposes pursuant to Section 11.30.040 A6 and which is redeemed within forty-eight (48) hours after the Police Department shall have notified the owner of the release of such vehicle in writing in the manner provided in Section 11.30.100 C; provided that such owner or person authorized to obtain possession of such impounded vehicle shall pay any charges assessed for storage after such forty-eight (48) hour period; provided further, that if the registered owner or the driver authorized by the registered owner is arrested or charged with a crime in connection with the incident leading to impoundment, the City shall not pay the towing or storage charges.

(Ord. 117306 § 8, 1994: Ord. 115634 § 4, 1991: Ord. 112421 § 6, 1985; Ord. 109031 § 1, 1980: Ord. 108200 , § 2 (11.30.180), 1979.)

11.30.200 - Abandoned vehicles.

A. Any impounded vehicle not redeemed within fifteen (15) days of mailing of the notice required by Section 11.30.100 shall be deemed abandoned.

B. No tow truck operator shall sell or otherwise dispose of an abandoned vehicle unless all applicable provisions of State law have been complied with.

(Ord. 117306 § 9, 1994: Ord. 108200 , § 2(11.30.200), 1979.)

11.30.220 - Contract for towing and storage.

A. The Director of Finance and Administrative Services is authorized and directed to prepare specifications for towing and storage of vehicles, including instructions to bidders, containing such provisions as the Director shall deem advisable and not in conflict with this chapter.

B. A call for bids responsive to such specifications shall then be made, and the contract shall be awarded to the lowest and best bidder whose proposal is deemed by the Director of Finance and Administrative Services to be the most advantageous for the public and the City; provided that, in the event all bids are deemed by the Director to be too high or irregular, he or she may reject all such bids and make another call for bids or proceed alternatively pursuant to ordinance passed for such purpose.

The Director shall consider, among other relevant factors, the following:

1. Integrity, skill, and business judgment of the bidder;
2. General experience in providing towing and storage services;
3. Conduct and performance under a previous City towing impound contract demonstrating honesty, promptness, skill, efficiency, and a satisfactory relationship with vehicle owners;
4. Existing availability of equipment, facilities, and personnel; and
5. The bidder's financial ability and willingness to expand or improve available equipment, facilities, and services.

The contract award shall be in accordance with the specifications so approved for towing and storage service necessary for carrying out the provisions of this chapter.

C. Subsequent to the award of the contract, the Director of Finance and Administrative Services shall file a written statement with the City Clerk giving the name and address of the contractor for towing and storage of vehicles and, if more than one place of storage has been provided, the name and address or location of each storage place. The Director shall administer and enforce contracts made pursuant to this section.

(Ord. 123361, § 251, 2010; Ord. 122589 , § 1, 2007; Ord. 120794 § 199, 2002: Ord. 117169 § 128, 1994: Ord. 116368 § 214, 1992; Ord. 108200 , § 2(11.30.220), 1979.)

11.30.240 - Contract for towing and storage—Financial responsibility.

Any contract for towing and storage under the provisions of this chapter shall require the contractor to demonstrate proof of financial responsibility for any liability which the City may have as a result of any negligence, willful conduct or breach of contract by the contractor and for any damages which the owner of an impounded vehicle may sustain as a result of damage to or loss of the vehicle, or the contents of a vehicle in the custody of the contractor. Proof of financial responsibility shall be furnished either by proof of insurance, by filing a surety bond and/or by depositing cash in such amounts as the Director of Finance and Administrative Services shall determine necessary.

(Ord. 123361, § 252, 2010; Ord. 117306 § 10, 1994: Ord. 117169 § 129, 1994: Ord. 108200 , § 2(11.30.240), 1979.)

11.30.260 - Contract for towing and storage—Notice to owners of impounded vehicles.

Any contract for towing and storage under provisions of this chapter shall require the contractor, at any location where vehicles are impounded, to post conspicuous notice of the rights of the owners of such vehicles under Section 11.30.220.

(Ord. 108200 , § 2(11.30.260), 1979.)

11.30.280 - Contractor to file monthly claim for services.

The contractor shall, on or before the tenth day of each month, file his or her claim with the Department of Finance and Administrative Services for towing and storage charges accruing to him or her upon vehicles redeemed as provided in this chapter during the preceding month, in accordance with this chapter and with the specifications for the contract authorized in Section 11.30.220, and such claim shall be sworn to by him or her under oath. The Director of Finance and Administrative Services shall audit such claim and any payment thereof at least once annually. A warrant or warrants for payment of such claim shall be drawn and paid by the Director from such expenditure allowances as may be provided therefor in the annual budget or from such moneys as may otherwise be appropriated for such purpose. If the appropriate fund is solvent at the time payment is ordered, the Director may elect to make payment by check.

(Ord. 123361, § 253, 2010; Ord. 120794 § 200, 2002; Ord. 120181 § 115, 2000; Ord. 120114 § 34, 2000; Ord. 118397 § 100, 1996; Ord. 117169 § 130, 1994; Ord. 116368 § 215, 1992; Ord. 108200 , § 2(11.30.280), 1979.)

11.30.290 - Contract for towing and storage—Administrative fee.

A. If a vehicle is impounded pursuant to Section 11.30.105, an administrative fee shall be levied when the vehicle is redeemed under the specifications of the contract provided for by Section 11.30.220.

B. If a vehicle is impounded pursuant to subsection 11.30.040.A7, an administrative fee shall be levied when the vehicle is redeemed under the specifications of the contract provided for by Section 11.30.220.

C. If a vehicle is impounded other than pursuant to subsection 11.30.040.A7 or Section 11.30.105, an administrative fee shall be levied when the vehicle is redeemed under the specifications of the contract provided for by Section 11.30.220.

D. The administrative fee shall be collected by the contractor performing the impound, and shall be remitted to the Department of Finance and Administrative Services in the manner directed by the Director of Finance and Administrative Services and as specified in the contract provided by subsection 11.30.220.A. The administrative fee shall be for the purpose of offsetting, to the extent practicable, the cost to the City of implementing, enforcing, and administering the provisions of this chapter and shall be deposited in an appropriate account. The administrative fee shall be set by rule by the Director in an amount not to exceed $100.

(Ord. 123361, § 254, 2010; Ord. 120794 § 201, 2002; Ord. 120181 § 116, 2000; Ord. 119180 § 7, 1998; Ord. 118397 § 101, 1996; Ord. 117306 § 11, 1994.)

11.30.300 - Record of impounded vehicles.

A. The Police Department shall keep, and make available for public inspection, a record of all vehicles impounded under the provisions of this chapter. The record shall include at least the following information:

1. Manufacturer's trade name or make;
2. Vehicle license number and state of registration;
3. Vehicle identification number;
4. Such other descriptive information as the Chief of Police deems useful for purposes of vehicle identification;
5. Basis for impoundment, including reference to the appropriate section or sections of this subtitle; and
6. Disposition of the vehicle and date of disposition.

B. The Police Department shall furnish to the towing contractor, upon request, the name of the registered owner of any vehicle impounded by such contractor pursuant to this chapter.

(Ord. 108200 , § 2(11.30.300), 1979.)

11.30.320 - Rules and regulations.

The Director of Finance and Administrative Services and the Chief of Police are authorized and directed to promulgate rules and regulations consistent with this chapter, the Charter of the City, and Chapter 3.02 to provide for the fair and efficient administration of any contract or contracts awarded pursuant to Section 11.30.220 and to provide for the fair and efficient administration of any vehicle impoundment, redemption, or release or any impoundment hearing under this chapter.

(Ord. 123361, § 255, 2010; Ord. 120794 § 202, 2002; Ord. 119180 § 8, 1998; Ord. 117169 § 131, 1994; Ord. 108200 , § 2(11.30.320), 1979.)

11.30.340 - Vehicle immobilization prohibited.

A. A property owner, other than the State of Washington or any unit of local government, shall not immobilize any vehicle owned by a person other than the property owner. "Immobilize" means the use of a locking wheel boot that, when attached to the wheel of a vehicle, prevents the vehicle from moving without damage to the tire to which the locking wheel boot is attached.

B. A violation of this section is a gross misdemeanor. (RCW 46.55.300)

(Ord. 122742, § 6, 2008.)

11.30.360 - Violations constituting abandoning—Evidence—Penalty.

A. No person shall wilfully leave an abandoned vehicle on private property for more than twenty-four (24) hours without the permission of the person having the right to possession of the property, or a wrecked, dismantled, or inoperative vehicle or automobile hulk on a street, alley or way open to the public for twenty-four (24) hours or longer without notification to the Chief of Police of the reasons for leaving the motor vehicle in such a place. Any such vehicle or hulk shall be abated and removed in accordance with the provisions of Ordinance 98223, [13] as amended, and enforcement shall be by the Director of Transportation in accordance with said ordinance as amended. For the purposes of this section, the fact that a motor vehicle has been so left without permission or notification is prima facie evidence of abandonment.

B. Any person found to have abandoned a vehicle or hulk shall, in addition to any penalty imposed, also be assessed any costs incurred by the City in the removal of such abandoned vehicle or hulk less any moneys received by the City from such removal.

(Ord. 121420 § 6, 2004; Ord. 117306 § 13, 1994; Ord. 109476 § 3(part), 1980; Ord. 108200 , § 2(11.30.360), 1979.)

Footnotes:

--- (13) ---

Editor's note— Ord. 98223 is codified in Chapter 11.92 of this Code.

Chapter 11.31 - DISPOSITION OF TRAFFIC OFFENSES

Sections:

11.31.010 - Violations as traffic infractions.

Except as otherwise provided in Section 11.34.020 or elsewhere in this title, failure to perform any act required or the performance of any act prohibited by this title is designated as a traffic infraction and may not be classified as a criminal offense.

(Ord. 123632, § 10, 2011; Ord. 122003 , § 2, 2005; Ord. 115040, § 6, 1990; Ord. 112975 , § 1, 1986; Ord. 112466 , § 2, 1985; Ord. 110967 , § 5, 1983; Ord. 109476 , § 1, 1980; Ord. 108200 , § 2(11.31.010), 1979.)

11.31.020 - Notice of traffic infraction—Issuance.

A. A peace officer has the authority to issue a notice of traffic infraction:

1. when the infraction is committed in the officer's presence;
2. if an officer investigating at the scene of a motor vehicle accident has reasonable cause to believe that the driver of a motor vehicle involved in the accident has committed a traffic infraction; or
3. when a violation of Section 11.50.140, 11.50.150, 11.52.040, or 11.52.100 is detected through the use of an automated traffic safety camera as authorized pursuant to RCW 46.63.170 and Section 11.50.570.

B. A court may issue a notice of traffic infraction upon receipt of a written statement of the officer that there is reasonable cause to believe that an infraction was committed. (RCW 46.63.030)

(Ord. 124950 , § 5, 2015; Ord. 123632, § 8, 2011; Ord. 123420, § 6, 2010; Ord. 123035, § 2, 2009; Ord. 119011 , § 7, 1998; Ord. 118105, § 2, 1996; Ord. 112421 , § 12, 1985; Ord. 109476 , § 3(part), 1984; Ord. 108200 , § 2(11.23.400), 1979.) Ord. 123946, § 4, 2012; Ord. 123170, § 1, 2009; Ord. 121944 , § 2, 2005; Ord. 109476 , § 1(part), 1980; Ord. 108200 , § 2(11.31.020), 1979.)

11.31.030 - Parking notices.

Whenever any motor vehicle without an operator is found parked, standing or stopped in violation of this subtitle, the officer finding it may take its registration number and any other information displayed on the vehicle which may identify its user, and shall fix conspicuously to such vehicle a notice of traffic infraction. (RCW 46.63.030(3))

(Ord. 109476 § 2(part), 1980; Ord. 108200 , § 2(11.31.030), 1979.)

11.31.040 - Notice of traffic infraction—Determination—Response.

A notice of traffic infraction represents a determination that an infraction has been committed. The determination will be final unless contested as provided in this chapter. (RCW 46.63.060)

(Ord. 109476 § 1(part), 1980: Ord. 108200 , § 2(11.31.020), 1979.)

11.31.050 - Response to notice of traffic infraction—Contesting determination—Hearing—Failure to appear.

A. Any person who receives a notice of traffic infraction shall respond to such notice as provided in this section within fifteen (15) days of the date of the notice.

B. If the person determined to have committed the infraction does not contest the determination the person shall respond by completing the appropriate portion of the notice of infraction and submitting it, either by mail or in person, to the Municipal Court of Seattle. A check or money order in the amount of the penalty prescribed for the infraction must be submitted with the response. When a response which does not contest the determination is received, an appropriate order shall be entered in the court's records, and a record of the response and order shall be furnished to the Department of Licensing in accordance with RCW 46.20.270.

C. If the person determined to have committed the infraction wishes to contest the determination the person shall respond by completing the portion of the notice of infraction requesting a hearing and submitting it, either by mail or in person, to the Municipal Court of Seattle. The court shall notify the person in writing of the time, place, and date of the hearing, and that date shall not be sooner than seven (7) days from the date of the notice, except by agreement.

D. If the person determined to have committed the infraction does not contest the determination but wishes to explain mitigating circumstances surrounding the infraction, the person shall respond by completing the portion of the notice of infraction requesting a hearing for that purpose and submitting it, either by mail or in person, to the Municipal Court of Seattle. The court shall notify the person in writing of the time, place, and date of the hearing.

E. In any hearing conducted pursuant to subsections C or D of this section, the court may defer findings, or in a hearing to explain mitigating circumstances may defer entry of its order, for up to one (1) year and impose conditions upon the defendant the court deems appropriate. Upon deferring

findings, the court may assess costs as the court deems appropriate for administrative processing. If at the end of the deferral period the defendant has met all conditions and has not been determined to have committed another traffic infraction, the court may dismiss the infraction. A person may not receive more than one (1) deferral within a seven (7) year period for traffic infractions for moving violations and more than one (1) deferral within a seven (7) year period for traffic infractions for nonmoving violations. A person who commits negligent driving in the second degree with a vulnerable user victim may not receive a deferral for this infraction under this section.

F. If any person issued a notice of traffic infraction:

1. Fails to respond to the notice of traffic infraction as provided in subsection B of this section; or

2. Fails to appear at a hearing requested pursuant to subsections C or D; the court shall enter an appropriate order assessing the monetary penalty prescribed for the traffic infraction and any other penalty authorized by this chapter and shall notify the Department of Licensing in accordance with RCW 46.20.270 of the failure to respond to the notice of infraction or to appear at a requested hearing. (RCW 46.63.070)

(Ord. 123946, § 5, 2012; Ord. 120060 , § 1, 2000; Ord. 111859 , § 2, 1984; Ord. 109476 , § 1(part), 1980; Ord. 108200 , § 2(11.31.050), 1979.)

11.31.060 - Hearing—Contesting determination that infraction committed—Appeal.

A. A hearing held for the purpose of contesting the determination that an infraction has been committed shall be without a jury.

B. The court may consider the notice of traffic infraction and any other written report made under oath submitted by the officer who issued the notice or whose written statement was the basis for the issuance of the notice in lieu of the officer's personal appearance at the hearing. The person named in the notice may subpoena witnesses, including the officer, and has the right to present evidence and examine witnesses present in court.

C. The burden of proof is upon the City to establish the commission of the infraction by a preponderance of the evidence.

D. After consideration of the evidence and argument, the court shall determine whether the infraction was committed. Where it has not been established that the infraction was committed, an order dismissing the notice shall be entered in the court's records. Where it has been established that the infraction was committed an appropriate order shall be entered in the court's records. A record of the court's determination and order shall be furnished to the Department of Licensing in accordance with RCW 46.20.270 as now or hereafter amended.

E. An appeal from the court's determination or order shall be to the Superior Court. The decision of the Superior Court is subject only to discretionary review pursuant to Rule 2.3 of the Rules of Appellate Procedure. (RCW 46.63.090)

(Ord. 109476 § 1(part), 1980: Ord. 108200 , § 2(11.31.060), 1979.)

11.31.070 - Hearings—Explanation of mitigating circumstances.

A. A hearing held for the purpose of allowing a person to explain mitigating circumstances surrounding the commission of an infraction shall be an informal proceeding. The person may not subpoena witnesses. The determination that an infraction has been committed may not be contested at a hearing held for the purpose of explaining mitigating circumstances.

B. After the court has heard the explanation of the circumstances surrounding the commission of the infraction an appropriate order shall be entered in the court's records. A record of the court's

determination and order shall be furnished to the Department of Licensing in accordance with RCW 46.20.270 as now or hereafter amended.

C. There may be no appeal from the court's determination or order. (RCW 46.63.100)

(Ord. 109476 § 1(part), 1980: Ord. 108200 , § 2(11.31.070), 1979.)

11.31.080 - Owner responsible for stopping, standing, parking, or alarm violation.

A. In any traffic infraction case involving a violation of this title relating to the stopping, standing or parking of a vehicle, or the sounding of an audible alarm, proof that the particular vehicle described in the notice of traffic infraction was stopping, standing or parking or emitting an audible alarm in violation of any such provision in this title together with proof of registered ownership of the vehicle at the time of the violation, shall constitute in evidence a prima facie presumption that the registered owner of the vehicle was the person who parked or placed the vehicle at the point where, and for the time during which, the violation occurred or was responsible for the failure to turn off the audible alarm as required.

B. The foregoing stated presumption shall apply only when the procedure prescribed in Section 11.31.030 has been followed. (RCW 46.63)

C. If a car rental agency declares that the vehicle was under lease at the time of the violation, and supplies the name and address of the lessee, there shall be a prima facie presumption that the lessee so identified parked or placed the vehicle at the point where the violation occurred, or was responsible for the failure to turn off the audible alarm as required.

(Ord. 116701 § 2, 1993: Ord. 109476 § 2(part), 1980: Ord. 108200 , § 2(11.31.080), 1979.)

11.31.090 - Traffic infractions detected through the use of an automated traffic safety camera

A. A notice of infraction based on evidence detected through the use of an automated traffic safety camera must be mailed to the registered owner of the vehicle within 14 days of the violation, or to the renter of a vehicle within 14 days of establishing the renter's name and address under subsection C1 of this section, SMC 11.31.090. The peace officer issuing the notice of infraction shall include with it a certificate or facsimile thereof, based upon inspection of photographs, microphotographs, or electronic images produced by an automated traffic safety camera, stating the facts supporting the notice of infraction. This certificate or facsimile is prima facie evidence of the facts contained in it and is admissible in a proceeding charging a violation of Section 11.50.140, Section 11.50.150, Section 11.52.040, or Section 11.52.100. The photographs, microphotographs, or electronic images evidencing the violation must be available for inspection and admission into evidence in a proceeding to adjudicate the liability for the infraction.

B. A person receiving such a notice of infraction may respond to the notice by mail. The registered owner of a vehicle is responsible for such an infraction unless the registered owner overcomes the presumption in SMC subsection 11.31.090.E, or, in the case of a rental car business, satisfies the conditions under SMC subsection 11.31.090.C. If appropriate under the circumstances, a renter identified under SMC subsection 11.31.090.C1 is responsible for such an infraction.

C. If the registered owner of the vehicle is a rental car business, the peace officer shall, before such a notice of infraction is issued, provide a written notice to the rental car business that a notice of infraction may be issued to the rental car business if the rental car business does not, within 18 days of receiving the written notice, provide to the peace officer by return mail:

1. A statement under oath stating the name and known mailing address of the individual driving or renting the vehicle when the infraction occurred; or

2. A statement under oath that the business is unable to determine who was driving or renting the vehicle at the time the infraction occurred; or

3. In lieu of identifying the vehicle operator, the rental car business may pay the applicable penalty.

Timely mailing of this statement to the peace officer relieves a rental car business of any liability under Chapter 11.31 for the notice of infraction.

D. The term "automated traffic safety camera" means a device that uses a vehicle sensor installed to work in conjunction with an intersection traffic control system, a railroad grade crossing system or speed measuring device, and a camera synchronized to automatically record one or more sequenced photographs, microphotographs, or electronic images of the rear of a motor vehicle at the time the vehicle fails to stop when facing a steady red traffic control signal or an activated railroad grade crossing control signal or exceeds a speed limit in a school speed zone as detected by a speed measuring device. An automated traffic safety camera includes a camera used to detect violations other than stoplight, railroad crossing and school speed zone violations as authorized by and subject to the restrictions imposed by the Washington Legislature.

E. In a traffic infraction case involving an infraction detected through the use of an automated traffic safety camera, proof that the particular vehicle described in the notice of traffic infraction was in violation of Section 11.50.140, Section 11.50.150, 11.52.040, or Section 11.52.100, together with proof that the person named in the notice of traffic infraction was at the time of the violation the registered owner of the vehicle, constitutes in evidence a prima facie presumption that the registered owner of the vehicle was the person in control of the vehicle at the point where, and for the time during which, the violation occurred. This presumption may be overcome only if the registered owner states, under oath, in a written statement to the court or in testimony before the court that the vehicle involved was, at the time, stolen or in the care, custody, or control of some person other than the registered owner.

(Ord. 124686 , § 2, 2015; Ord. 123946, § 6, 2012; Ord. 123170, § 2, 2009; Ord. 122725 , § 1, 2008; Ord. 122554 , § 1, 2007; Ord. 121944 § 3, 2005.)

11.31.115 - Monetary penalty doubled for certain traffic infractions.

A person found to have committed a traffic infraction relating to right of way, speed restrictions, overtaking and passing or regard for pedestrians in a school or playground crosswalk zone under Sections 11.40.040, 11.44.120, 11.52.100, 11.53.400, 11.58.230 or 11.58.310, speed restrictions in a roadway construction zone under Section 11.52.110 or an emergency zone under Section 11.58.272 or overtaking and passing a school bus under Section 11.53.440 A shall be assessed a monetary penalty equal to twice the penalty assessed under Section 11.31.120. This penalty may not be waived, reduced or suspended. (RCW 46.61.212(3); RCW 46.61.235(5); RCW 46.61.245(2); RCW 46.61.261(2); RCW 46.61.440(3); RCW 46.61.527(3); RCW 46.61.370(6))

(Ord. 123420, § 8, 2010; Ord. 123420, § 7, 2010; Ord. 119011 § 9, 1998.)

11.31.120 - Monetary penalties.

A. A person found to have committed a traffic infraction shall be assessed a monetary penalty. No penalty may exceed $250.00 for each offense unless a higher penalty is specifically provided for in this title or by statute.

B. There shall be a penalty of $25.00 for failure to respond to a notice of traffic infraction, to appear at a requested hearing or to pay a monetary penalty imposed pursuant to this chapter.

C. A traffic infraction for violation of Section 11.50.140, Section 11.50.150, Section 11.52.040, or Section 11.52.100 detected through the use of an automated traffic safety camera shall be processed in the same manner as a parking infraction, with a monetary penalty equal to the total penalty, including the base penalty plus any statutory assessments authorized under state law, for violations of such Sections otherwise detected by a police officer. However, the monetary penalty for

a violation of Section 11.50.140 or Section 11.50.150 detected through the use of an automated traffic safety camera shall not exceed the monetary penalty for a violation of Section 11.50.380 as provided under subsection A of this Section, including all applicable statutory assessments.

(Ord. 123946, § 7, 2012; Ord. 123445, § 1, 2010; Ord. 123170, § 4, 2009; Ord. 122725 , § 2, 2008; Ord. 122554 , §§ 1, 2, 2007; Ord. 121944 , § 4, 2005; Ord. 120481 , § 3, 2001; Ord. 115927, § 1, 1991; Ord. 114839, § 1, 1989; Ord. 113186 , § 1, 1986; Ord. 110013 , § 1, 1981; Ord. 109476 , § 1(part), 1980; Ord. 108200 , § 2(11.31.120), 1979.)

11.31.121 - Monetary penalties—Parking infractions

The base monetary penalty for violation of each of the numbered provisions of the Seattle Municipal Code listed in the following table is as shown, unless and until the penalty shown below for a particular parking infraction is modified by Local Rule of the Seattle Municipal Court adopted pursuant to the Infraction Rules for Courts of Limited Jurisdiction ("IRLJ") or successor rules to the IRLJ:

Municipal Code reference	Parking infraction short description	Base penalty amount
11.23.400	UNAUTHORIZED USE - DISABLED	$250
11.23.410	CARPOOL, FREE & PREFERENTIAL	$47
11.23.415	CARPOOL PERMIT	$47
11.26.060	SERVICE CONTROLLED PARKING AREA	$47
11.26.080	HOOD, CONTROLLED PARKING AREA	$47
11.26.100	HOOD, FREE PARKING AREA	$47
11.26.120	HOOD, WORK LOCATION	$47
11.26.140	HOOD ON OCCUPIED METER	$47
11.26.160	HOODED METER, UNOCCUPIED	$47
11.26.180	HOOD ON METER OVER 2 DAYS	$47
11.26.200	HOOD, PROH. HOURS	$47
11.26.220	HOOD, PASSENGER VEH.	$47

11.26.240	HOOD, REVOKED	$47
11.26.280	HOOD, VIOLATION	$47
11.70.020	ANGLE, GEN.	$47
11.70.040	PARALLEL R. SIDE	$47
11.70.060	PARALLEL 1 WAY ST.	$47
11.70.080	SHOULDER	$47
11.70.100	STALLS/SPACES	$47
11.70.120	PARK, R/W	$47
11.70.140	SECURE VEH.	$44
11.70.160	KEYS IGNITION	$47
11.70.180	REMOVE KEY, LOCK DOOR	$47
11.70.200	ILLEGAL ON STREET/ALLEY	$47
11.72.010	ADVERTISING	$47
11.72.020	ALLEY	$47
11.72.025	ALLEY/DRIVEWAY	$47
11.72.030	ANGLE/ARTERIAL OR BUS ROUTE	$47
11.72.035	BLOCK TRAF OR WALK UNOCCUPIED	$47
11.72.045	BUS SHELTER	$47
11.72.050	BUS ZONE	$47
11.72.051	CURB BULBS	$47

11.72.053	UNAUTHOR. VEH/CARPOOL	$47
11.72.054	CAR SHARING VEH ZONE	$47
11.72.055	CLASS OF VEH.	$47
11.72.060	CLEAR ROADWAY	$47
11.72.065	IN MARKED DISABLED, INVALID PLACARD	$250
11.72.070	COMMERCIAL VEH.	$47
11.72.075	RESTRICTIONS - COMM LOAD ZONE	$53
11.72.080	CROSSWALK	$47
11.72.090	XWALK APPROACH	$47
11.72.100	DOUBLE PARKED	$47
11.72.110	DRIVEWAY OR ALLEY ENTRANCE	$47
11.72.125	ELECTRIC VEHICLE CHARGING STATION	$124
11.72.130	ELEVATED STRUCTURE	$47
11.72.140	EXCAVATION OR OBSTRUCTION	$47
11.72.145	EXPIRED/IMPROPER PLATES	$47
11.72.150	FIRE APPARATUS	$47
11.72.155	FIRE EXIT DOOR	$47
11.72.160	FIRE HYDRANT	$47
11.72.170	FIRE STATION DRIVEWAY	$47
11.72.180	FIRE AREA	$47

11.72.185	FIRE LANE	$47
11.72.190	FLASHING SIGNAL	$47
11.72.195	FOOD-VEHICLE ZONE	$47
11.72.200	FUEL LOSS	$47
11.72.205	DROPPING OIL OR GREASE	$47
11.72.210	INTERSECTION	$47
11.72.215	LOAD/UNLOAD ZONE	$47
11.72.220	HOODED METERS, SIGNS	$47
11.72.230	MOVING VEHICLE OF ANOTHER	$47
11.72.240	MOVE VEH. AVOID TIME LIMIT	$47
11.72.250	PARK, MUNICIPAL PROPERTY	$44
11.72.260	OVERTIME	$44
11.72.270	REPEATED OVERTIME	$47
11.72.280	IN PARK	$47
11.72.285	PASS. LOAD ZONE	$47
11.72.290	PAVEMENT MARKINGS	$47
11.72.300	PEAK HOUR	$47
11.72.310	PLANTED AREA	$44
11.72.320	PLANTING STRIP	$44
11.72.330	SIGN POSTED LOCATIONS	$47

11.72.350	TOO CLOSE TO R.R.	$47
11.72.351.A	RESTRICTED PARKING ZONE	$53
11.72.351.B	RPZ PERMIT DISPLAY IN IMPROPER LOCATION ON VEHICLE	$29
11.72.351.C	ILLEGAL SALE, PURCHASE OR POSSESSION OF RPZ PERMIT	$250
11.72.352	HUSKY STADIUM EVENT RESTRICTED PARKING	$53
11.72.353	SCHOOL LOAD ZONE	$47
11.72.355	SERVICE VEH. IN ST.	$47
11.72.357	SHUTTLE BUS LOAD ZONE	$47
11.72.360	SIDEWALK	$47
11.72.370	STOP SIGN APPROACH (30')	$47
11.72.390	LIMITED ACCESS, STREET	$47
11.72.400	TAXI CAB ZONE	$47
11.72.410	TOW AWAY ZONE	$47
11.72.415	TRAIL OR PATH (VEH/BIKE)	$47
11.72.420	TRF. CONTROL SIGNAL APPROACH	$47
11.72.430	TRL./CAMPER DETACHED	$47
11.72.435	PASS. VEH. IN TRUCK ZONE	$47
11.72.440	OVER 72 HOURS	$44
11.72.450	TYPE OF VEH.	$47
11.72.460	WALL OR FENCE	$47

11.72.465	CURB RAMP	$47
11.72.470	WRONG SIDE	$47
11.72.480	W/IN 30 FT. OF YIELD SIGN	$47
11.72.500	PARKING JUNK VEHICLE ON STREET (IMPOUND)	$250
11.74.010	STAND/ALLEY/COMM. VEH.	$47
11.74.020	TRUCK LOAD ZONE - CMCRL VEH.	$47
11.74.030	LOAD ZONE - TIME RESTRICTIONS	$53
11.74.060	LOAD/UNLOAD PROH.	$47
11.74.120	RESTRICTED AREA	$47
11.76.005	IMPROPER PARKING RECEIPT DISPLAY	$29
11.76.015	PAY-TO-PARK VIOLATIONS	$44
11.76.020	PARKING TIME LIMIT	$47
11.76.030	METER RESTRICTION	$44
11.76.040	ILLEGAL USE, PARKING PAYMENT, TAMPERING	$47
11.82.300	LIGHTS, PARKED VEHICLE	$47
11.82.320	LIGHTS, PARKED, HIGHBEAM	$47
11.84.345	FALSE ALARM - PARKED AUTO	$47
18.12.235	RESTRICTIONS IN CERTAIN PARKS (REQ)	$47

(Ord. 125609 , § 5, 2018; Ord. 124302, § 7, 2013; Ord. 123712, § 2, 2011; Ord. 123705, § 1, 2011; Ord. 123659, § 8, 2011; Ord. 123161, § 1, 2009; Ord. 123035, § 4, 2009; Ord. 123001, §

10, 2009; Ord. 122779, § 6, 2008; Ord. 122761, § 2, 2008; Ord. 121954, § 2, 2005; Ord. 121917, § 5, 2005; Ord. 121388, § 11, 2004; Ord. 121005, § 1, 2002.)

11.31.125 - Civil infraction — Automobile alarm — Failure to respond.

A. The violation of or failure to comply with Section 11.84.345 is a civil infraction as contemplated by RCW Chapter 7.80, and subject as a Class 4 civil infraction to a maximum penalty and a default amount of Twenty-three Dollars ($23).

B. There shall be a maximum penalty and default amount of Twenty-five Dollars ($25) for failure to respond to a notice of violation under Section 11.84.345 within fifteen (15) days from the date of notice as contemplated by RCW 7.80.030(1) and 7.80.076(2)(K), a failure to appear at a hearing requested by the recipient of the notice as contemplated by RCW 7.80.160(2) and RCW 7.80.070(2)(K), and a failure to pay a penalty imposed under subsection A of this section, as contemplated by RCW 7.80.160(3).

C. If the court determines that a person has insufficient funds to pay the monetary penalty, the court may order performance of a number of hours of community service instead.

(Ord. 116701 § 3, 1993.)

11.31.130 - Order of court—Civil in nature.

An order entered after the receipt of a response which does not contest the determination, or after it has been established at a hearing that the infraction was committed, or after a hearing for the purpose of explaining mitigating circumstances is civil in nature. (RCW 46.63.120)

(Ord. 109476 § 1(part), 1980: Ord. 108200, § 2(11.31.130), 1979.)

Chapter 11.32 - CITATIONS

Sections:

11.32.020 - Service of citation.

Whenever any person is charged with any violation of this subtitle, other than a traffic infraction, the officer may serve upon him or her a traffic citation and notice to appear in court. Such citation and notice shall be handled and disposed of as set forth in RCW 46.64.010 and also shall conform with the requirements of RCW 46.64.010 and be in the form prescribed in RCW 46.64.015. (RCW 46.64.010, 46.64.015)

(Ord. 123946, § 8, 2012; Ord. 109476 § 3(part), 1980: Ord. 108200, § 2(11.32.020), 1979.)

11.32.080 - Return of citation.

The original or a copy of every citation issued by an enforcement officer shall be transmitted to the Municipal Court of Seattle as soon as is practicable. (RCW 46.64.010)

(Ord. 108200, § 2(11.32.080), 1979.)

11.32.160 - Cancellation.

No person shall cancel or solicit the cancellation of any citation in any manner other than as provided in this chapter.

(Ord. 108200 , § 2(11.32.160), 1979.)

Chapter 11.34 - PENALTIES

Sections:

11.34.020 - Penalties for criminal offenses

A. Any person convicted of any of the following offenses may be punished by a fine in any sum not to exceed $5,000 or by imprisonment for a term not to exceed 364 days, or by both such fine and imprisonment:

1. Subsection 11.22.070.B, Licenses and plates required—Penalties—Exceptions;
2. Section 11.22.090, Vehicle trip permits—Restrictions and requirements—Penalty;
3. Section 11.22.200, Special license plates—Hulk hauler;
4. Section 11.23.400, Disabled parking—Enforcement;
5. Section 11.30.340, Vehicle immobilization prohibited;
6. Section 11.55.340, Vehicles carrying explosives, flammable liquids, poison gas, liquefied petroleum gas (LPG) and cryogenics must stop at all railroad grade crossings;
7. Section 11.56.120, Reckless driving;
8. Section 11.56.130, Reckless endangerment of roadway workers;
9. Section 11.56.140, Reckless endangerment of emergency zone workers;
10. Subsection 11.56.320.B, Driving while license is suspended or revoked in the first degree;
11. Subsection 11.56.320.C, Driving while license is suspended or revoked in the second degree;
12. Section 11.56.330, Violation of an occupational, temporary restricted or ignition interlock driver's license;
13. Section 11.56.340, Operation of motor vehicle prohibited while license is suspended or revoked;
14. Section 11.56.350, Operation of a motor vehicle without required ignition interlock or other biological or technical device;
15. Section 11.56.355, Tampering with or assisting another in circumventing an ignition interlock device;
16. Section 11.56.420, Hit and run (attended);
17. Section 11.56.445, Hit and run (by unattended vehicle);
18. Section 11.56.450, Hit and run (pedestrian or person on a device propelled by human power);
19. Section 11.60.690, Transportation of liquified petroleum gas;
20. Section 11.62.020, Flammable liquids, combustible liquids and hazardous chemicals;
21. Section 11.62.040, Explosives;
22. Subsection 11.74.160.B, Failure to secure load in the first degree;
23. Subsection 11.80.140.B, Certain vehicles to carry flares or other warning devices (subsection B only);

24. Subsection 11.80.160.E, Display of warning devices when vehicle disabled (subsection E only);

25. Subsection 11.84.370.D, Using, selling or purchasing a signal preemption device except as authorized;

26. Section 11.84.380, Fire extinguishers;

27. Section 11.86.080, Flammable or combustible labeling;

28. Section 11.86.100, Explosive cargo labeling;

29. Section 11.34.040, with respect to aiding and abetting the foregoing criminal offenses.

B. Any person convicted of any of the following offenses may be punished by a fine in any sum not to exceed $1,000 or by imprisonment for a term not to exceed 90 days, or by both such fine and imprisonment:

1. Section 11.20.010, Driver's license required—Exception—Penalty, unless the person cited for the violation provided the citing officer with an expired driver's license or other valid identifying documentation under RCW 46.20.035 at the time of the stop and was not in violation of Section 11.56.320 or Section 11.56.340, in which case the violation is an infraction;

2. Section 11.20.100, Display of nonvalid driver's license;

3. Section 11.20.120, Loaning driver's license;

4. Section 11.20.140, Displaying the driver's license of another;

5. Section 11.20.160, Unlawful use of driver's license;

6. Section 11.20.200, Unlawful to allow unauthorized person to drive;

7. Subsection 11.20.350.C, Providing false evidence of financial responsibility;

8. Section 11.22.025, Transfer of ownership;

9. Subsection 11.23.400.B, Unlawfully obtaining placard or special license plate;

10. Subsection 11.23.400.C, Unlawful sale of placard or special license plate;

11. Section 11.32.160, Cancellation of citation;

12. Section 11.40.180, Standard of care for drivers of motor vehicles - blind pedestrians carrying white cane or using guide dog;

13. Section 11.40.430, Prohibited entry to no admittance area;

14. Subsection 11.56.320.D, Driving while license is suspended or revoked in the third degree;

15. Section 11.56.430, Hit and run (unattended vehicle)—Duty in case of accident with unattended vehicle;

16. Section 11.56.440, Hit and run (property damage)—Duty in case of accident with property;

17. Subsection 11.58.005.A, Negligent driving in the first degree;

18. Section 11.58.190, Leaving minor children in unattended vehicle;

19. Section 11.59.010, Obedience to peace officers, flaggers, and firefighters;

20. Section 11.59.040, Refusal to give information to or cooperate with officer;

21. Section 11.59.060, Refusal to stop;

22. Section 11.59.080, Examination of equipment;

23. Section 11.59.090, Duty to obey peace officer—Traffic infraction;

24. Section 11.66.240, Obstructing or delaying train;

25. Subsection 11.74.160.C, Failure to secure load in the second degree;

26. Subsection 11.84.370.C, Possessing signal preemption device except as authorized;

27. Section 11.34.040, Aiding and abetting with respect to the criminal offenses in this subsection 11.34.020.B.

(Ord. 124950, § 6, 2015; Ord. 124686, § 3, 2015; Ord. 123632, § 11, 2011; Ord. 123420, § 10, 2010; Ord. 123420, § 9, 2010; Ord. 122742, § 7, 2008; Ord. 120885, § 3, 2002; Ord. 119189, § 5, 1998; Ord. 119011, § 10, 1998; Ord. 118105, § 3, 1996; Ord. 116872, § 3, 1993; Ord. 116538, § 2, 1993; Ord. 115757, § 1, 1991; Ord. 115040, § 5, 1990; Ord. 112975, § 2, 1986; Ord. 112466, § 3, 1985; Ord. 111859, § 4, 1984: Ord. 109476, § 3(part), 1980: Ord. 108200, § 2(11.34.020), 1979.)

11.34.040 - Aiding and abetting violation.

It is unlawful to counsel, aid, or abet the violation of or failure to comply with any of the provisions of this subtitle.

(Ord. 108200, § 2(11.34.040), 1979.)

Chapter 11.35 - IMMOBILIZATION

Sections:

11.35.010 - Scofflaw list

A. When there are four or more parking citations issued against a vehicle for each of which a person has failed to respond, failed to appear at a requested hearing, or failed to pay amounts due for at least 45 days from the date of the filing of each of those citations, the Seattle Municipal Court shall place the vehicle on a list of scofflaws, and shall mail, by first class mail, a notice to the last known registered owner of the vehicle, as disclosed by the vehicle license number as provided by the Washington State Department of Licensing or equivalent vehicle licensing agency of the state in which the vehicle is registered. If there is no last known address that can be ascertained from the Washington Department of Licensing, or if the vehicle has no Washington vehicle license number or is not registered in the State of Washington, the notice, in the form of a readily visible notification sticker, may be affixed to the vehicle while left within a public right-of-way or other publicly owned or controlled property. A notification sticker may be used in lieu of mailing even if the last known address is ascertainable for vehicles registered in the State of Washington.

B. The registered vehicle owner may request an administrative review at the Seattle Municipal Court at any time that the vehicle is on the scofflaw list until the vehicle has been immobilized or impounded. The review should only examine whether the vehicle is properly on the scofflaw list and shall not review the underlying citations that caused the vehicle to be included on the scofflaw list. The vehicle shall be removed from the list only upon a showing by the registered owner that either:

1. fewer than four of the citations that caused the vehicle to be included on the scofflaw list were committed while the current registered owner was the legal owner of the vehicle; or

2. all amounts due pertaining to the citations that met the criteria for scofflaw under Section 11.35.010 A have been satisfied in full.

C. A vehicle shall remain on the scofflaw list until all outstanding parking infraction penalties, court costs (including but not limited to collection agency remuneration authorized under RCW 3.02.045), default penalties on parking traffic infractions imposed under Section 11.31.120, immobilization release fees imposed under subsection 11.35.020.H, costs of impoundment (including removal,

towing and storage fees) imposed under Section 11.30.120, towing administrative fees imposed under Section 11.30.290 and immobilization administrative fees under subsection 11.35.020.H, and interest, have been paid, or a time payment plan has been arranged with the Seattle Municipal Court or their authorized agent.

D. When a time payment plan is created, the subject vehicle shall be temporarily removed from the scofflaw list and the payment amounts shall be applied on a pro rata basis until all penalties, fines or fees owed relating to all parking citations are satisfied. A vehicle that has been temporarily removed from the scofflaw list shall be returned to the list if the owner defaults on the time payment agreement, in accordance with guidelines adopted by the Seattle Municipal Court.

(Ord. 124558, § 1, 2014; Ord. 123563, § 1, 2011; Ord. 123447, § 1, 2010)

11.35.020 - Immobilization

A. Effective July 1, 2011 and thereafter, if the notice requirements under Section 11.35.010 A have been met, and if parked in public right-of-way or on other publicly owned or controlled property, a vehicle on the scofflaw list may be immobilized by installing on such vehicle a device known as a "boot," which clamps and locks onto the vehicle wheel and impedes vehicle movement. If a vehicle is immobilized, it shall not be released until full payment has been made, or a time payment agreement has been entered into for all outstanding penalties, fines, or fees owed for all parking citations, plus all immobilization, towing, and storage charges and administrative fees.

B. Any vehicle that remains booted for 48 hours or more, not including any of the 48 hours from the beginning of Saturday until the end of Sunday, or which becomes illegally parked while booted, shall be subject to towing and impoundment pursuant to Section 11.30.040. The Seattle Department of Transportation and Seattle Police Department shall issue joint guidelines for vehicle towing related to immobilization, based on Sections 11.30.040 and 11.16.320.

C. The person installing the boot shall leave under the windshield wiper or otherwise attach to the vehicle a notice advising the owner that the vehicle has been booted by the City of Seattle for failure to respond, failure to appear at a requested hearing, and failure to pay amounts due for four or more adjudicated parking infractions for at least 45 days from the date of the last such adjudication issued against the vehicle; that release of the boot may be obtained by paying all outstanding penalties, fines, or forfeitures owed relating to all adjudicated violations, plus all booting, removal, towing, and storage charges and administrative fees; that unless such payment is made within two business days of the date of the notice, the vehicle will be impounded; that it is unlawful for any person to remove or attempt to remove the boot, to damage the boot, or to move the vehicle with the boot attached, unless authorized by the Seattle Police Department or an authorized agent of the City; and that the owner may seek an administrative review of the booting by submitting a request to the Seattle Municipal Court within ten days of the release of the boot. The notice shall further state that the vehicle remains subject to impoundment regardless of whether the owner requests an appeal.

D. The vehicle may be released from immobilization when the vehicle owner or an agent of the owner pays all outstanding parking infraction penalties, court costs (including but not limited to collection agency remuneration authorized under RCW 3.02.045), default penalties on parking traffic infractions imposed under Section 11.31.120, immobilization release fees imposed under subsection 11.35.020.H, costs of impoundment (including removal, towing and storage fees) imposed under Section 11.30.120, towing administrative fees imposed under Section 11.30.290 and immobilization administrative fees under subsection 11.35.020.H, and interest, or enters into a time payment agreement for the payment thereof. Upon full payment or upon entry into a time payment agreement, the Seattle Police Department or other authorized agent of the City shall promptly remove or enable the removal of the boot from the vehicle. If payment is made in full, the vehicle shall be removed from the scofflaw list and shall not be subject to immobilization or impoundment for the paid citations. Upon entry into a time payment agreement, the vehicle shall be temporarily removed from the scofflaw list and shall not be subject to immobilization, provided, however, that the vehicle shall be returned to the scofflaw list and be subject to immobilization if the owner defaults on the time

payment agreement. A registered owner who defaults on a time payment agreement shall not be given another opportunity to make a time payment arrangement and therefore, payment for all outstanding amounts above shall be made in full before the vehicle may be removed from the scofflaw list or released from immobilization or impound. Any person who has previously removed or enabled removal of a booting device in violation of subsection E while on the scofflaw list for any four or more parking infractions, and subsequently is booted a second time while on the scofflaw list for the same parking infractions, shall not be eligible for a time payment plan.

E. No person other than an authorized employee of the Seattle Police Department or an authorized agent of the City shall remove or enable the removal of the boot described in subsection A of this Section from any vehicle on which it has been installed unless the requirements of subsection D have been met.

F. If the Seattle Police Department or an authorized agent of the City enables the vehicle owner to remove the boot, the owner shall return the boot to a location designated by the Department within two calendar days of the removal.

G. No person, other than an authorized employee of the Seattle Police Department or other authorized agent of the City, shall move, by towing or other means, any vehicle after it has been immobilized but before the boot has been removed.

H. The Director of Finance and Administrative Services shall determine and set an immobilization fee and an administrative fee in amounts such that the sum of such fees do not exceed the sum of the lowest impound fee, minimum storage fee, and administrative fee for vehicle impoundment under Section 11.30.120. An administrative fee, if any, shall be levied when the boot is removed. The administrative fee shall be collected by the contractor releasing the vehicle from immobilization, shall be remitted to the Department of Finance and Administrative Services, and shall be deposited in an appropriate account.

I. A person who fails to return the booting device within the time frame required by subsection F of this section may be charged a late fee as determined by the Director of Finance and Administrative Services.

J. A person who intentionally damages the booting device may be charged a replacement fee as determined by the Director of Finance and Administrative Services and also may be prosecuted for the crime of property destruction under section 12A.08.020.

K. The Director of Finance and Administrative Services shall adopt rules governing the imposition of fees under this Section 11.35.020.

(Ord. 124558, § 2, 2014; Ord. 123563, § 2, 2011; Ord. 123447, § 1, 2010)

11.35.030 - Post-immobilization review

The registered vehicle owner may seek a post-deprivation review of the immobilization by submitting a written request to the Seattle Municipal Court within ten days of the placement of the notice on the vehicle, as established by the notice date. Upon timely receipt of such written request, the Seattle Municipal Court shall, within a reasonable time as established by the Court, conduct a review on the issue of whether the immobilization was proper and shall issue a written decision setting forth the reasons on which the decision is based, provided, however, that any previously adjudicated parking infractions that formed the basis of the vehicle's scofflaw status shall not be subject to the review. The person seeking review shall have an opportunity to present evidence on his or her behalf in accordance with requirements established by the Court.

(Ord. 123447, § 1, 2010)

WAC 446-20-260

Auditing of criminal history record information systems.

(1) Every criminal justice agency, including contractors authorized to collect, retrieve, maintain, and disseminate criminal history record information pursuant to WAC 446-20-180, must make its records available under RCW 10.97.090(3) to determine the extent of compliance with the following:

(a) Dissemination records as required under RCW 10.97.050(7);

(b) Security procedures as required by RCW 10.97.090(1); and

(c) Personnel standards as required by RCW 10.97.090(2).

(2) Personnel engaged in the auditing function will be subject to the same personnel security requirement as required under WAC 446-20-230, 446-20-240, and 446-20-250, as employees who are responsible for the management and operation of criminal history record information systems.

[Statutory Authority: Chapters 10.97 and 43.43 RCW. WSR 10-01-109, § 446-20-260, filed 12/17/09, effective 1/17/10. Statutory Authority: RCW 10.97.080 and 10.97.090. WSR 80-08-057 (Order 80-2), § 446-20-260, filed 7/1/80.]

JAY INSLEE
Governor

JOHN R. BATISTE
Chief

STATE OF WASHINGTON
WASHINGTON STATE PATROL
General Administration Building • PO BOX 42602 • Olympia, WA 98504-2602 • (360) 596-4043 • www.wsp.wa.gov

March 11, 2014

Mr. Mark Knutson
Seattle Police Department
610 5th Ave
PO Box 34986
Seattle WA 98104

Dear Mr. Knutson:

Subject: WSP Memorandum of Understanding No. C141174GSC

Enclosed with this letter is one fully executed original of the referenced agreement between the Washington State Patrol and your organization. Please keep this original for your records.

The Washington State Patrol agreement tracking number is the agreement number referenced above; please use this number on all correspondence regarding this agreement. If you need further assistance, please contact Terri Johnson at (360) 596-4063 or terri.johnson@wsp.wa.gov.

Sincerely,

Terri L. Johnson

for Mr. Robert L. Maki, CFE, CGFM
Budget and Fiscal Services

RLM: tlj

Enclosure

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE WASHINGTON STATE PATROL

AND

THE SEATTLE POLICE DEPARTMENT

1. PURPOSE: The purpose of this Memorandum of Understanding (MOU) between the Washington State Patrol (WSP) and the Police Department for the City of the Seattle hereinafter referred to as the "parties", is to memorialize the parties' understanding regarding transmitting, receiving, and storage of information contained in the National Crime Information Center (NCIC) and Washington Crime Information Center (WACIC) systems of records made available through a data transfer program. The data provided by WSP will be used by Seattle Police Department as input to a law enforcement application.

WSP provides NCIC/WACIC data to the Seattle Police Department through WSP's A Central Computerized Enforcement Service System (ACCESS). Department has a separate agreement with WSP regarding access to, use of, and subsequent dissemination of information obtained through ACCESS, including NCIC/WACIC data. This MOU has no affect on that agreement.

2. BACKGROUND: The Federal Bureau of Investigation (FBI) maintains the NCIC system of records containing multiple files. WSP maintains the WACIC system of records containing multiple files. Information included may be stolen vehicles, vehicles wanted in conjunction with felonies, wanted persons, and vehicles subject to seizure based on federal court orders.

The Seattle Police Department has instituted state-of-the-art license plate screening technology from mobile and fixed sites. The Seattle Police Department's vendors provide software and screening devices that have the capability of scanning license plates and searching a local database loaded into a patrol vehicle computer or other locations controlled by the agency. The Seattle Police Department has requested to obtain relatively current information from the NCIC and WACIC files in order to compare scanned numbers against stolen license plates. The Seattle Police Department certifies its vendors providing license plate screening technology do not have access to NCIC/WACIC data provided to the Seattle Police Department by WSP.

3. SCOPE: This MOU applies to WSP making information from the NCIC and WACIC Vehicle File, License Plate File and Wanted Person File available to Seattle Police Department via a secure FTP Server environment.

A. WSP will:

1) Provide the Seattle Police Department with the data elements and disqualifying items are described in Attachment 1, Data Elements and Handling Instructions, which is attached hereto and incorporated herein.

2) Provide updated extract information on a mutually agreed to frequency;

3) Respond to specific inquiries from the Seattle Police Department; and

4) Provide the Seattle Police Department with the name and telephone number of a technical and an administrative point of contact.

B. the Seattle Police Department will:

1) Use the NCIC and WACIC extracts for law enforcement purposes;

2) Update its local database as FBI and WACIC updates become available via WSP, ensuring that those numbers deleted from the NCIC/WACIC system are also deleted from all local databases;

3) Confirm extract hits are still active in NCIC and WACIC, at the earliest reasonable opportunity, in accordance with current hit confirmation policy;

4) Provide the WSP with the name and telephone number of a technical and an administrative point of contact; and

5) Ensure that the Seattle Police Department's use and dissemination of data provided by WSP under this MOU is in accordance with federal and state laws and regulations, including but not limited to the FBI's Criminal Justice Systems Information (CJIS) regulations.

4. FUNDING: Each party will fund its own activities unless otherwise agreed in writing. PCSO has a separate agreement with WSP for use of ACCESS. This MOU has no affect on that agreement, or the rates and fees WSP charges for the services provided thereunder.

5. LIAISON REPRESENTATIVES

For the Washington State Patrol:	For the City of Seattle Police Department:
Mr. Jim Anderson, Administrator	Mr. Mark Knutson, IT Manager
Criminal Records Division	Information Technology Section
PO Box 42619	610 5th Ave , PO Box 34986
Olympia WA 98504-2619	Seattle WA 98104
Phone: (360) -534-2101	Phone: (206) - 684-0970
Fax: (360) – 534-2070	Fax: (206) – 684-5109
E-mail: jim.anderson@wsp.wa.gov	Email: Mark.Knutson@seattle.gov

5. CONFIDENTIAL INFORMATION: The Seattle Police Department acknowledges that some of the material and information that may come into its possession or knowledge in connection with this MOU or its performance may consist of information that is exempt from disclosure to the public or other unauthorized persons under either chapter 42.56 RCW or other state or federal statutes ("Confidential Information"). Confidential Information includes, but is not limited to, names, addresses, Social Security numbers, e-mail addresses, telephone numbers, financial profiles, credit card information, driver's license numbers, medical data, law enforcement records, agency source code or object code, agency security data, or information identifiable to an individual that relates to any of these types of information. The Seattle Police Department agrees to hold Confidential Information in strictest confidence and not to make use of Confidential Information for any purpose other than the performance of this MOU, to release it only to authorized employees requiring such information for the purposes of carrying out this MOU, and not to release, divulge, publish, transfer, sell, disclose, or otherwise make it known to any other party without WSP's

express written consent or as provided by law. Furthermore, the Seattle Police Department's use and dissemination of NCIC data provided by WSP under this MOU is governed by the Seattle Police Department's agreement with WSP regarding access to, use of, and subsequent dissemination of NCIC data and other information obtained through ACCESS.

6. SETTLEMENT OF DISPUTES: Disagreements between the parties arising under or relating to this MOU will be resolved only by consultation between the parties and will not be referred to any other person or entity for settlement.

7. AMENDMENT, TERMINATION, ENTRY INTO FORCE, AND DURATION:

A. All activities of the parties under this MOU will be carried out in accordance to the above-described provisions.

B. This MOU may be amended or terminated by the mutual written consent of the parties' authorized representatives.

c. Either party may terminate this MOU upon 30 days written notification to the other party. The parties will continue participation up to the effective date of termination.

8. This MOU, which consists of eight Sections, will enter into effect upon signature of both parties, will be reviewed annually to determine whether amendments are needed, and will remain in effect until terminated. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

The foregoing represents the understandings reached between the WSP and the Seattle Police Department.

State of Washington
Washington State Patrol

John R. Batiste, Chief

3/10/14
Date

Seattle Police Department

Signature

3 DEC 13
Date

Attachment 1

NCIC/WACIC Data Elements and Handling Instructions

1) Data Elements: WSP will transmit to the Seattle Police Department information from the Vehicle File, License Plate File, and vehicle information from the Wanted Person Files.

2) Data Handling

   a) If the Seattle Police Department has no need for a particular class of data, they will delete that data immediately on receipt.

   b) Record updates are accomplished by record replacement. The Seattle Police Department may have to compare a new data file with former files provided by WSP in order to determine any changes.

   c) If a record is present within the Seattle Police Department's application and not present in the transferred file from WSP, the record has been removed for operational reasons by local law enforcement. Reasons for that removal include cancellation of the subject plate, or the vehicle has been located.

   d) The Seattle Police Department will not retain any data file provided by WSP longer than 30 calendar days.

e) The Seattle Police Department will not enter or modify NCIC/WACIC data directly.

3) Schedule: WSP shall refresh the data files provided to the Seattle Police Department in a mutually agreed upon process and at agreed upon intervals. WSP shall notify the Seattle Police Department if files will not be available due to problems or of updated code tables.

4) Problem Reporting: Problem reporting by WASPC under this MOU is governed by Attachment 2, WSP Secure FTP Problem Notification Procedures, which is attached hereto and incorporated into this MOU herein.

Attachment 2

WSP Secure FTP Problem Notification Procedures

- When a problem with acquiring data occurs with the WSP Secure FTP Server, the Seattle Police Department will call WSP ITD Customer Services at (360) 705-5999 or send an e-mail to ITDcustomerservicesg@wsp.wa.gov explaining the issue and having a work order opened. The Seattle Police Department will include identifying information about the Seattle Police Department staff that identified the problem in the explanation with e-mail address and phone number(s).
- The WSP Information Technology Division (ITD) Customer Services group will escalate the work order to the appropriate ITD group.
- That group will notify the Seattle Police Department that the issue is being worked on or has been completed.
- If there is no contact within four business hours, the Seattle Police Department should do a follow-up contact.
- The ITD Customer Services group working the problem may call or send e-mail to the Seattle Police Department in order to determine problem particulars or to request testing. The Seattle Police Department will only call or e-mail that person or group in the context of an existing, open problem, and not for new problems.
- Once the Seattle Police Department is satisfied with the results, the work order will be closed. Another work order should be opened for any new problem with receiving data from the WSP Secure FTP Server. The prior work order can be cited by the Seattle Police Department in any subsequent work orders if it seems relevant.

APPENDIX J: CTO NOTICE OF SURVEILLANCE TECHNOLOGY

Thank you for your department's efforts to comply with the new Surveillance Ordinance, including a review of your existing technologies to determine which may be subject to the Ordinance. I recognize this was a significant investment of time by your staff; their efforts are helping to build Council and public trust in how the City collects and uses data.

As required by the Ordinance (SMC 14.18.020.D), this is formal notice that the technologies listed below will require review and approval by City Council to remain in use. This list was determined through a process outlined in the Ordinance and was submitted at the end of last year for review to the Mayor's Office and City Council.

The first technology on the list below must be submitted for review by March 31, 2018, with one additional technology submitted for review at the end of each month after that. The City's Privacy Team has been tasked with assisting you and your staff with the completion of this process and has already begun working with your designated department team members to provide direction about the Surveillance Impact Report completion process.

Please let me know if you have any questions.

Thank you,

Michael

Technology	Description	Proposed Review Order
Automated License Plate Recognition (ALPR)	ALPRs are computer-controlled, high-speed camera systems mounted on parking enforcement or police vehicles that automatically capture an image of license plates that come into view and converts the image of the license plate into alphanumeric data that can be used to locate vehicles reported stolen or otherwise sought for public safety purposes and to enforce parking restrictions.	1
Booking Photo Comparison Software (BPCS)	BCPS is used in situations where a picture of a suspected criminal, such as a burglar or convenience store robber, is taken by a camera. The still screenshot is entered into BPCS, which runs an algorithm to compare it to King County Jail booking photos to identify the person in the picture to further investigate his or her involvement in the crime. Use of BPCS is governed by SPD Manual §12.045.	2

Technology	Description	Proposed Review Order
Forward Looking Infrared Real-time video (FLIR)	Two King County Sheriff's Office helicopters with Forward Looking Infrared (FLIR) send a real-time microwave video downlink of ongoing events to commanders and other decision-makers on the ground, facilitating specialized radio tracking equipment to locate bank robbery suspects and provides a platform for aerial photography and digital video of large outdoor locations (e.g., crime scenes and disaster damage, etc.).	3
Undercover/ Technologies	The following groups of technologies are used to conduct sensitive investigations and should be reviewed together. • **Audio recording devices**: A hidden microphone to audio record individuals without their knowledge. The microphone is either not visible to the subject being recorded or is disguised as another object. Used with search warrant or signed Authorization to Intercept (RCW 9A.73.200). • **Camera systems**: A hidden camera used to record people without their knowledge. The camera is either not visible to the subject being filmed or is disguised as another object. Used with consent, a search warrant (when the area captured by the camera is not in plain view of the public), or with specific and articulable facts that a person has or is about to be engaged in a criminal activity and the camera captures only areas in plain view of the public. • **Tracking devices**: A hidden tracking device carried by a moving vehicle or person that uses the Global Positioning System to determine and track the precise location. U.S. Supreme Court v. Jones mandated that these must have consent or a search warrant to be used.	4
Computer-Aided Dispatch (CAD)	CAD is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field.	5

Technology	Description	Proposed Review Order
CopLogic	System allowing individuals to submit police reports on-line for certain low-level crimes in non-emergency situations where there are no known suspects or information about the crime that can be followed up on. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.	6
Hostage Negotiation Throw Phone	A set of recording and tracking technologies contained in a phone that is used in hostage negotiation situations to facilitate communications.	7
Remotely Operated Vehicles (ROVs)	These are SPD non-recording ROVs/robots used by Arson/Bomb Unit to safely approach suspected explosives, by Harbor Unit to detect drowning victims, vehicles, or other submerged items, and by SWAT in tactical situations to assess dangerous situations from a safe, remote location.	8
911 Logging Recorder	System providing networked access to the logged telephony and radio voice recordings of the 911 center.	9
Computer, cellphone and mobile device extraction tools	Forensics tool used with consent of phone/device owner or pursuant to a warrant to acquire, decode, and analyze data from smartphones, tablets, portable GPS device, desktop and laptop computers.	10
Video Recording Systems	These systems are to record events that take place in a Blood Alcohol Concentration (BAC) Room, holding cells, interview, lineup, and polygraph rooms recording systems.	11
Washington State Patrol (WSP) Aircraft	Provides statewide aerial enforcement, rapid response, airborne assessments of incidents, and transportation services in support of the Patrol's public safety mission. WSP Aviation currently manages seven aircraft equipped with FLIR cameras. SPD requests support as needed from WSP aircraft.	12
Washington State Patrol (WSP) Drones	WSP has begun using drones for surveying traffic collision sites to expedite incident investigation and facilitate a return to normal traffic flow. SPD may then request assistance documenting crash sites from WSP.	13
Callyo	This software may be installed on an officer's cell phone to allow them to record the audio from phone communications between law enforcement and suspects. Callyo may be used with consent or search warrant.	14

Technology	Description	Proposed Review Order
I2 iBase	The I2 iBase crime analysis tool allows for configuring, capturing, controlling, analyzing and displaying complex information and relationships in link and entity data. iBase is both a database application, as well as a modeling and analysis tool. It uses data pulled from SPD's existing systems for modeling and analysis.	15
Parking Enforcement Systems	Several applications are linked together to comprise the enforcement system and used with ALPR for issuing parking citations. This is in support of enforcing the Scofflaw Ordinance SMC 11.35.	16
Situational Awareness Cameras Without Recording	Non-recording cameras that allow officers to observe around corners or other areas during tactical operations where officers need to see the situation before entering a building, floor or room. These may be rolled, tossed, lowered or throw into an area, attached to a hand-held pole and extended around a corner or into an area. Smaller cameras may be rolled under a doorway. The cameras contain wireless transmitters that convey images to officers.	17
Crash Data Retrieval	Tool that allows a Collision Reconstructionist investigating vehicle crashes the opportunity to image data stored in the vehicle's airbag control module. This is done for a vehicle that has been in a crash and is used with consent or search warrant.	18
Maltego	An interactive data mining tool that renders graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the internet.	19

Please let me know if you have any questions.

Thank you,

Michael Mattmiller

Chief Technology Officer

City of Seattle

2019 Surveillance Impact Report

Computer-Aided Dispatch (CAD)

Seattle Police Department

City of Seattle

Table of Contents

Surveillance Impact Report ("SIR") overview 5

Privacy Impact Assessment..... 6

Financial Information 28

Expertise and References 31

Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet 32

Privacy and Civil Liberties Assessment..... 44

CTO Response..... 48

Appendix A: Glossary..... 54

Appendix B: Meeting Notice(s) 56

Appendix C: Meeting Sign-in Sheet(s) 64

Appendix D: Department of Neighborhood Focus Group Notes..... 89

Appendix E: All Comments Received from Members of the Public..... 121

Appendix F: Department Responses to Public Inquiries 126

Appendix G: Letters from Organizations or Commissions 127

Appendix H: Comment Analysis Methodology..... 151

Appendix I: Supporting Policy Documentation..... 154

Appendix J: CTO Notification of Surveillance Technology 173

City of Seattle

Memo

Date: April 24, 2019
To: City Council
From: Deputy Chief Marc Garth Green, Seattle Police Department
Subject: Computer Aided Dispatch (CAD)

Description

The Seattle Police Department's 9-1-1 Center is the primary Public Safety Answering Point (PSAP) for emergency 9-1-1 calls placed within the City of Seattle. SPD's Computer Aided Dispatch (CAD) system consists of a set of servers and software deployed on dedicated terminals in the 9-1-1 center, on SPD computers, as an application on patrol vehicles' mobile data computers (MDCs), and on some officers' smart phones. It assists 9-1-1 Center call takers and dispatchers process requests for police services, collect information from 9-1-1 callers, and provide dispatchers with real-time patrol unit availability so dispatchers may dispatch appropriate patrol resources to requests for police service. CAD software also provides real-time documentation of the Seattle Police Department's response to calls for service, including relevant information obtained by responding officers. The Seattle Police 9-1-1 Center is staffed 24 hours per day, 365 days per year, receives approximately 900,000 calls resulting in the creation of approximately 250,000 CAD events per year. Approximately 135,000 additional CAD events are initiated by police officers during their normal patrol activities.

Purpose

Developed in the 1960s, Computer Aided Dispatch (CAD) systems are used by virtually all modern police departments. SPD uses the CAD system to assist in the coordination and documentation of the department response to requests for police services. There are two main functions of the CAD system: to initiate and log the appropriate police response, and to document the assignment and response of the correct police resources. CAD is the real-time record-keeping system for officers' response to calls for service, thereby documenting SPD's actions related to each of those requests in an organized and reportable method.

Benefits to the Public

The mission of the Seattle Police Department is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional, and dependable police services. CAD is a technology that supports this mission by ensuring that police resources are efficiently and appropriately dispatched to address emergencies and by documenting the police response to those emergencies. The system allows for increased efficiencies in dispatching responses to emergencies. CAD also provides information that allows SPD to allocate patrol resources effectively while reducing response times.

Privacy and Civil Liberties Considerations

During the privacy review of CAD and the public comment period, the perceived concerns that arose about the system were limited to how long data was kept in the CAD system and how securely. SPD acknowledges the most important unintended possible consequence related to the continued utilization of the CAD system is the unintentional release of privacy data. The policies in place requiring ACCESS and CJIS certification by all CAD users and the data security processes in place mitigate the likelihood of this occurring.

Data entered into SPD's CAD system is retained indefinitely on Seattle IT managed servers dedicated to the CAD system. No data is deleted; however, updates are made as necessary to records. The entire CAD system resides on the SPD's network managed by Seattle ITD and is FBI Criminal Justice Information Services (CJIS) certified.

All authorized users of CAD must be CJIS certified and must maintain Washington State ACCESS certification. SPD Policy 12.050 mandates that all employees receive Security Awareness Training (Level 2), and all employees also receive City Privacy Training. All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), many of which contain specific privacy requirements. Any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

Summary

CAD is a critical component which allows for SPD to act on its mission to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional, and dependable police services. Approximately 385,000 CAD events are created each year by 9-1-1- call takers, dispatchers, and patrol officers in the City of Seattle. The CAD system provides efficient and necessary support to the SPD response to calls for service, providing dispatchers with real-time unit availability, dispatching the appropriate SPD resources, and documenting SPD's response.

City of Seattle

Surveillance Impact Report ("SIR") overview

About the Surveillance Ordinance

The Seattle City Council passed Ordinance 125376, also referred to as the "Surveillance Ordinance," on September 1, 2017. SMC 14.18.020.b.1 charges the City's executive with developing a process to identify surveillance technologies subject to the ordinance. Seattle IT, on behalf of the executive, developed and implemented a process through which a privacy and surveillance review is completed prior to the acquisition of new technologies. This requirement, and the criteria used in the review process, are documented in Seattle it policy pr-02, the "surveillance policy".

How this Document is Completed

This document is completed by the requesting department staff, support and coordinated by the Seattle information technology department ("Seattle it"). As Seattle it and department staff complete the document, they should keep the following in mind.

1. Responses to questions should be in the text or check boxes only; all other information (questions, descriptions, etc.) Should **not** be edited by the department staff completing this document.
2. All content in this report will be available externally to the public. With this in mind, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.

Surveillance Ordinance Review Process

The following is a high-level outline of the complete SIR review process.

Upcoming for Review	Initial Draft	Open Comment Period	Final Draft	Working Group	Council Review
The technology is upcoming for review, but the department has not begun drafting the surveillance impact report (SIR).	Work on the initial draft of the SIR is currently underway.	The initial draft of the SIR and supporting materials have been released for public review and comment. During this time, one or more public meetings will take place to solicit feedback.	During this stage the SIR, including collection of all public comments related to the specific technology, is being compiled and finalized.	The surveillance advisory working group will review each SIR's final draft and complete a civil liberties and privacy assessment, which will then be included with the SIR and submitted to Council.	City Council will decide on the use of the surveillance technology, by full Council vote.

Privacy Impact Assessment

Purpose

A Privacy Impact Assessment ("PIA") is a method for collecting and documenting detailed information collected in order to conduct an in-depth privacy review of a program or project. A PIA asks questions about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. It also requests information about policies, training and documentation that govern use of the technology. The PIA responses are used to determine privacy risks associated with a project and mitigations that may reduce some or all of those risks. In the interests of transparency about data collection and management, the City of Seattle has committed to publishing all PIAs on an outward facing website for public access.

When is a Privacy Impact Assessment Required?

A PIA may be required in two circumstances.

1. When a project, technology, or other review has been flagged as having a high privacy risk.
2. When a technology is required to complete the surveillance impact report process. This is one deliverable that comprises the report.

1.0 Abstract

1.1 Please provide a brief description (one paragraph) of the purpose and proposed use of the project/technology.

The Seattle Police Department's 9-1-1 Center is the primary Public Safety Answering Point (PSAP) for emergency 9-1-1 calls placed within the City of Seattle. Computer Aided Dispatch (CAD) is a software package utilized by the Seattle Police Department's 9-1-1 Center. It assists 9-1-1 Center call takers and dispatchers with receiving requests for police services, collecting information from 9-1-1 callers, and providing dispatchers with real-time patrol unit availability so dispatchers may dispatch appropriate patrol resources to requests for police service. CAD software also enables real-time documentation of the Seattle Police Department's response to calls for service, including relevant information obtained by responding officers.

The Seattle Police 9-1-1 Center, staffed 24 hours per day, 365 days per year, receives approximately 900,000 calls resulting in the creation of approximately 250,000 CAD events per year. Approximately 135,000 additional CAD events are initiated by police officers during their normal patrol activities.

Calls requiring a fire or medical response that do not also require a police response are transferred to the Seattle Fire Alarm Center for appropriate resource deployment and are not entered into SPD's CAD system.

1.2 Explain the reason the project/technology is being created or updated and why the PIA is required.

The CAD system automatically receives the telephone number, name (if available), and location of the caller (if available) from the West VIPER telephone system for calls placed to 9-1-1. Non-emergency calls, and associated phone numbers, are not automatically entered into CAD. If the call is determined to be a request for police services, call takers and dispatchers then manually enter additional information into CAD, such as the nature of the emergency, and create a CAD event to facilitate a police response. Call takers and dispatchers may add supplemental information into CAD regarding scene safety, descriptions of individuals, vehicles, and premises. Much of the privacy-sensitive information entered into CAD is provided by 9-1-1 or non-emergency callers or by officers or dispatchers who input information into the CAD system when responding to a call.

All of the information and data that is entered into CAD is viewable and retrievable. Some information from one call may be used for subsequent calls at the same location or involving the same individuals.

2.0 Project / Technology Overview

Provide an overview of the project or technology. The overview gives the context and background necessary to understand the purpose, mission and justification for the project / technology proposed

2.1 Describe the benefits of the project/technology.

CAD is the system used by SPD to coordinate and document, in real-time, requests for police service and SPD's response to those requests. The technology is used by 9-1-1- call takers to document information reported by a 9-1-1 caller and then assists 9-1-1 dispatchers with prioritizing emergency calls and assigning appropriate police resources to incidents. CAD is also used to document patrol officers' proactive policing ("on-views"), such as initiating a traffic stop. About 250,000 CAD events are created from the approximately 900,000 calls received by the 9-1-1 center annually, and approximately 135,000 CAD events are created annually from patrol officers' on-viewing an incident such as a traffic violation.

Developed in the 1960s, CAD systems are used by virtually all modern police departments. Computer aided dispatch allows for increased efficiencies in dispatching responses to emergencies. CAD also provides information that allows SPD to allocate patrol resources effectively while reducing response times. CAD is the real-time record-keeping system for officers' response to calls for service, thereby documenting SPD's actions related to each of those requests in an organized and reportable method.

2.2 Provide any data or research demonstrating anticipated benefits.

McEwan, Tom. et al. "Computer Aided Dispatch in Support of Community Policing, Final Report." National Institute of Justice. Feb 2004.

> This 2004 research project studied the effects CAD systems have in the support of community policing objectives at several police departments throughout the United States. The benefits provided by CAD outlined in this article include; reporting access to recorded data, location of resource data, data on call types received, better crime analysis, department problem solving information, and resource allocation measures. The article also provided suggestions for enhancements, such as better integration with other data systems and more robust remote access for real-time CAD data by officers in the field, which have largely been implemented by CAD system developers in the years since.

"Versadex PoliceCAD" *Law and Order: The Magazine for Police Management.* Volume:56 Issue:7. July 2008 Pages:38-40,42,43

> The *Versadex PoliceCAD* article details the history of the development of the Computer Aided Dispatch system created by Versadex. The style of CAD they developed was more streamlined and easier to integrate with other law enforcement data systems including records management systems. Effective CAD systems should "improve delivery (of services) and boost the speed and accuracy of the caller's critical information to the emergency responder."

A study by the Illinois Department of Transportation on the impact of CAD systems: https://utc.uic.edu/wp-content/uploads/Strategic-Project-Plan-Computer-Assisted-Scheduleing-and-Dispatch1.pdf

> This study by the Urban Transportation Center at the University of Illinois at Chicago, looks at the impact of CAD systems on the operation and coordination of paratransit services in the state of Illinois. Though this research was not specifically relevant to the dispatch of law enforcement services, the study provides insight into cost-savings and service improvements which are provided by the implementation of CAD systems.

2.3 Describe the technology involved.

CAD (Computer Aided Dispatch) software, made by Versaterm, consists of a set of servers and software deployed on dedicated terminals in the 9-1-1 center, on SPD computers, and as an application on patrol vehicles' mobile data computers (MDCs) and on some officers' smart phones.

When a request for police service is initiated by a 9-1-1 call or an officer on-viewing an incident, a CAD event is created by the 9-1-1 Center staff, and a unique CAD event ID number is automatically generated. Information related to that CAD event is entered into the CAD system. A call taker assigns the CAD event a specific type code and priority associated with the type of police service requested. The location of the event is entered and CAD validates the address, locates the address electronically, and then plots it on a map. Based on this information, the call taker routes the CAD call to the appropriate dispatcher. The dispatcher then assigns patrol officers to the service request and records this information in the CAD event. Each of the assigned patrol officers then log their activities related to that request for service into CAD using established codes. When the request for service is completed, the primary officer assigned closes the CAD call. Based upon the codes used to close the CAD call, the system then automatically routes the information recorded into SPD's Records Management System (RMS) where additional information, such as police reports and supplementary material, is stored.

2.4 Describe how the project or use of technology relates to the department's mission.

The mission of the Seattle Police Department is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional, and dependable police services. CAD is a technology that supports this mission by ensuring that police resources are efficiently and appropriately dispatched to address emergencies and by documenting the police response to those emergencies.

2.5 Who will be involved with the deployment and use of the project / technology?

SPD's authorized users of CAD include all sworn personnel, 9-1-1 Center staff, and other civilian staff whose business needs require access to this data.

Additionally, Seattle IT provides client services and operational support for IT technologies and applications. In supporting SPD systems, operational and application services deploy and service SPD technology systems. Details about the IT department are found in the appendix of this SIR.

All authorized users of CAD are Criminal Justice Information Services (CJIS) certified and maintain Washington State ACCESS (A Central Computerized Enforcement Service System) certification. More information on CJIS compliance may be found at the CJIS Security Policy website. Additional information about ACCESS may be found on the Washington State Patrol's website.

3.0 Use Governance

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities contracting with the City are bound by restrictions specified in the surveillance ordinance and privacy principles and must provide written procedures for how the entity will comply with any restrictions identified.

3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

Access for personnel into the system is predicated on state and federal law governing access to Criminal Justice Information Services (CJIS). This includes pre-access background information, appropriate role-based permissions as governed by the CJIS security policy found in Appendix I, and audit of access and transaction logs within the system. All users of CAD must be CJIS certified and maintain Washington State ACCESS certification.

3.2 List the legal standards or conditions, if any, that must be met before the project / technology is used.

This technology is used each time the 9-1-1 Center receives a request for police service or when a police officer assigns themselves to an incident which was self-initiated (an "on-view") such as a traffic stop. About 250,000 CAD events are created from the approximately 900,000 calls received by the 9-1-1 center annually, and approximately 135,000 CAD events are created annually from patrol officers' on-viewing an incident such as a traffic violation.

3.3 Describe the policies and training required of all personnel operating the project / technology, and who has access to ensure compliance with use and management policies.

Supervisors and commanding officers are responsible for ensuring compliance with policies.

All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

All authorized users of CAD must be CJIS certified and must maintain Washington State ACCESS certification. SPD Policy 12.050 defines the proper use of criminal justice information systems.

Outside of SPD, Seattle Information Technology Department (ITD) client services interaction with SPD systems is governed according to the terms of the 2018 Management Control Agreement (MCA) between ITD and SPD, which states that:

"Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBIs Criminal Justice Information Services, (CJIS) Security Policy."

The MCA document may be found in Appendix I.

Additionally, per the CJIS security policy, records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained. Details of the compliance program in Appendix I.

4.0 Data Collection and Use

4.1 Provide details about what information is being collected from sources other than an individual, including other IT systems, systems of record, commercial data aggregators, publicly available data and/or other City departments.

When an individual places a call to 9-1-1, the telephone number they are calling from, the location they are calling from, the name associated with the phone number (if available from the phone company), and the type of telephone service (landline, cell phone, VOIP phone) are provided by the West VIPER telephone system and automatically entered into CAD when a CAD call is initiated by the call taker.

Additionally, private information may be entered into a CAD call by SPD officers requesting information, such as a warrant check, while responding to a request for service.

4.2 What measures are in place to minimize inadvertent or improper collection of data?

A CAD call is initiated when someone requests police services. All users of the CAD system are trained in its use to ensure the data collected is entered appropriately. Authorized users of the CAD system are required to be CJIS certified and adhere to the CJIS security policy, found in the appendices of this document.

4.3 How and when will the project / technology be deployed or used? By whom? Who will determine when the project / technology is deployed and used?

The Seattle Police 9-1-1 Center is the primary Public Safety Answering Point (PSAP) for emergency 9-1-1 calls placed within the City of Seattle. CAD is in continual use by police communications dispatchers. When a call is entered into CAD, a radio dispatcher communicates to police resources in the field, maintaining contact with those resources and coordinating responses.

4.4 How often will the technology be in operation?

The CAD system is in continuous use 24 hours a day, 365 days a year.

4.5 What is the permanence of the installation? Is it installed permanently, or temporarily?

CAD software is permanently installed.

4.6 Is a physical object collecting data or images visible to the public? What are the markings to indicate that it is in use? What signage is used to determine department ownership and contact information?

The CAD software has no physical or visual indicator that it is in use. The software itself runs 24 hours a day, 7 days a week, 365 days a year.

4.7 How will data that is collected be accessed and by whom?

Within SPD, only authorized users can access the system, technology, or the data. Access to the application requires SPD personnel to log in with password-protected login credentials which are granted to employees with business needs to access CAD. These employees are ACCESS and CJIS certified.

Data is entered into CAD from both the West VIPER telephone system and from information manually entered by SPD personnel. It is accessed and used on SPD's password-protected network with access limited to authorized personnel as described in 2.5, above.

According to the CJIS security policy, "The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.".

All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.

Data with regards to response times, response locations, crime trends, and general statistics is managed by the Data Driven Policing unit within SPD.

Additionally, incidental data access may occur through delivery of technology client services. All ITD employees are required to comply with appropriate regulatory requirements regarding security and background review. Information on the ITD roles associated with client services for City Departments can be found in Appendix I; applicable CJIS compliance policies are found in Appendix I.

ITD client services interaction with SPD systems is governed according to the terms of the 2018 Management Control Agreement between ITD and SPD, which states that:

"Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBIs Criminal Justice Information Services, (CJIS) Security Policy."

The MCA document may be found in Appendix I.

4.8 If operated or used by another entity on behalf of the City, provide details about access, and applicable protocols.

CAD is operated and used primarily by SPD personnel. Seattle IT Department personnel have administrative access to the system for support services as outlined in 4.7.

4.9 What are acceptable reasons for access to the equipment and/or data collected?

Authorized SPD users, as described in 2.5, may have access to the system to document, review, or report on police activity pursuant to law and policy, to extract information for use in court or administrative proceedings as required by law, to respond to appropriate requests for information, to make aggregate information available to the public, and to provide information to oversight bodies on issues such as stop and detention rates, for example.

Incidental access may occur from ITD through delivery of technology client services. All ITD employees are required to comply with appropriate regulatory requirements regarding security and background review. Information on the ITD roles associated with client services for City Departments can be found in Appendix I.

ITD client services interaction with SPD systems is governed according to the terms of the 2018 Management Control Agreement between ITD and SPD, which states that:

"Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBIs Criminal Justice Information Services, (CJIS) Security Policy."

This MCA document between Seattle IT and SPD may be found in Appendix I.

4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

Only authorized SPD users can access the system, technology, or the data. Access to the application is limited to SPD personnel via password-protected login credentials. All activity within CAD (including timeline of commands issued) generates a log that is auditable.

Data is securely input and used on SPD's password-protected network with access limited to authorized users.

The entire system is located on the SPD network that is protect by industry standard firewalls. ITD performs routine monitoring of the SPD network.

The CAD system is CJIS compliant. More information on CJIS compliance may be found at the CJIS Security Policy website.

All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.

SPD's Audit, Policy and Research Section (APRS) can conduct an audit of the any system at any time. The Office of Inspector General and the federal monitor can also access all data and audit for compliance at any time.

ITD client services interaction with SPD systems is governed by the terms of the 2017 Management Control Agreement between ITD and SPD, which states that:

"Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBIs Criminal Justice Information Services, (CJIS) Security Policy."

The MCA document may be found in Appendix I.

Additionally, policy requires the following safeguards to be in place:

- The agency shall establish identifier and authenticator processes.
- Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. 08/16/2018 CJISD-ITS-DOC-08140-5.7 37 password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).
- Unsuccessful login attempts - the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10-minute time period unless released by an administrator.

- When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128-bit strength to protect CJI.
- When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption. When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256-bit strength.
- Intrusion Detection Tools/Techniques such as monitor inbound and outbound communications for unusual or unauthorized activities, send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort, employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.
- Audit - Each agency shall be responsible for complying with all audit requirements for use of CJIS Systems. Each CSO is responsible for completing a triennial audit of all agencies with access to CJIS Systems through the CSO's lines.
- The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.
- A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage.

Publicly accessible computers shall not be used to access, process, store or transmit CJI.

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

All of the data in CAD are held in SPD/ITD servers, located on City premises on SPD networks. Access to these networks is as specified in 4.1. All data that goes to mobile clients are encrypted to FIP 140-2 standards and is therefore CJIS compliant.

Per the CJIS Security Policy (see Appendix I):

"Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history 08/16/2018 CJISD-ITS-DOC-08140-5.7 D-3 records. Additionally, each CSO must ensure that all agencies establish an information security structure that provides for an ISO and complies with the CJIS Security Policy.

Network Diagrams - Network diagrams, i.e. topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the "big picture" – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest."

5.2 How will the owner allow for departmental and other entities, to audit for compliance with legal deletion requirements?

SPD's Audit, Policy and Research Section (APRS) can conduct an audit of the any system at any time. In addition, the Office of Inspector General and the federal monitor can access all data and audit for compliance at any time.

The 2017 Technical Security Audit for CJIS Compliance for SPD can be found in Appendix I

5.3 What measures will be used to destroy improperly collected data?

SPD policy contains multiple provisions to avoid improperly collecting data. SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a GO Report. SPD Policy 7.090 specifically governs the collection and submission of photographic evidence. Evidence is submitted to the Evidence Unit and associated with a specific GO Number and investigation. And, SPD Policy 7.110 governs the collection and submission of audio recorded statements. It requires that officers state their name, the Department name, the General Offense number, date and time of recording, the name of the interviewee, and all persons present at the beginning of the recording.

Additionally, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

Per the CJIS Security Policy:

"5.8.3 Digital Media Sanitization and Disposal The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel."

5.4 Which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

Unit supervisors are responsible for ensuring compliance with data retention requirements within SPD. Audit, Policy & Research Section personnel can also conduct audits of all data collection software and systems. Additionally, any appropriate auditor, including the Office of Inspector General and the federal monitor can audit for compliance at any time.

The CJIS security policy in Appendix I of this SIR includes applicable data retention requirements associated with the CAD system. The MCA between SPD and ITD (see Appendix I) is the inter-departmental agreement that ensures compliance with the CJIS Security Policy.

6.0 Data Sharing and Accuracy

6.1 Which entity or entities inside and external to the City will be data sharing partners?

No person, outside of SPD and Seattle IT, has direct access to the application or the data.

As Seattle IT supports the CAD system on behalf of SPD, a Management Control Agreement exists between SPD and Seattle IT. The agreement outlines the specifications for compliance, and enforcement related to supporting the CAD system through inter-departmental partnership. The MCA can be found in the appendices of this SIR.

Data obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law.

Data may be shared with outside entities in connection with criminal prosecutions:

- Seattle City Attorney's Office
- King County Prosecuting Attorney's Office
- King County Department of Public Defense
- Private Defense Attorneys
- Seattle Municipal Court
- King County Superior Court
- Similar entities where prosecution is in Federal or other State jurisdictions

Data may be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

Discrete pieces of data collected by CAD may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by SPD Policy 12.050 and 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayoral Directive, dated February 6, 2018.

SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the system.

6.2 Why is data sharing necessary?

Data sharing is not an automatic component of the CAD system. Instead, discrete pieces of data may be shared with outside agencies and individuals only within the context of the situations outlined in 6.1. Data sharing may be necessary for SPD to provide coordinated, rapid responses to 911 incidents, particularly reducing the amount of time needed to contact individuals, thereby improving outcomes.

6.3 Are there any restrictions on non-City data use?

Yes ☒ No ☐

6.3.1 If you answered yes, provide a copy of the department's procedures and policies for ensuring compliance with these restrictions.

Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20, regulating criminal justice information systems. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260 (auditing and dissemination of criminal history record information systems), and RCW Chapter 10.97 (Washington State Criminal Records Privacy Act).

Once disclosed in response to PRA request, there are no restrictions on non-City data use; however, applicable exemptions will be applied prior to disclosure to any requestor who is not authorized to receive exempt content.

6.4 How does the project/technology review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?

Research agreements must meet the standards reflected in SPD Policy 12.055. Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

6.5 Explain how the project/technology checks the accuracy of the information collected. If accuracy is not checked, please explain why.

The CAD system documents information provided by the participants and witnesses in the event being reported, as input by SPD personnel. The system itself does not check for accuracy of the information that is provided by personnel. Instead, the Department may later determine that the information provided was not accurate and can provide updated information.

6.6 Describe any procedures that allow individuals to access their information and correct inaccurate or erroneous information.

SPD cannot delete any information in CAD. Updates to information may be added to individual CAD events by SPD personnel with access to CAD.

Individuals may request records pursuant to the PRA, and individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

7.0 Legal Obligations, Risks and Compliance

7.1 What specific legal authorities and/or agreements permit and define the collection of information by the project/technology?

CAD data is not legally constrained at the local, state, or federal level. Instead, retention of data is restricted. SPD retains CAD data that is not case specific (i.e. not related to an investigation) for 90 days.

Case specific data is maintained for the retention period applicable to the specific case type.

7.2 Describe what privacy training is provided to users either generally or specifically relevant to the project/technology.

SPD Dispatchers undergo training on the use of CAD, which includes privacy training.

All authorized users of CAD must be CJIS certified and must maintain Washington State ACCESS certification.

SPD Policy 12.050 mandates that all employees receive Security Awareness Training (Level 2), and all employees also receive City Privacy Training. All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), many of which contain specific privacy requirements. Any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

The CJIS training requirements can be found in the appendices of this document, as well as in question 3.3, above.

7.3 Given the specific data elements collected, describe the privacy risks identified and for each risk, explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

The nature of the Department's mission will inevitably lead it to collect and maintain information many may believe to be private and potentially embarrassing. Minimizing privacy risks revolve around disclosure of personally identifiable information.

SMC 14.12 and SPD Policy 6.060 direct all SPD personnel that "any documentation of information concerning a person's sexual preferences or practices, or their political or religious activities must be for a relevant reason and serve a legitimate law enforcement purpose." Additionally, officers must take care "when photographing demonstrations or other lawful political activities. If demonstrators are not acting unlawfully, police can't photograph them."

Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

Finally, see 5.3 for a detailed discussion about procedures related to noncompliance.

7.4 Is there any aspect of the project/technology that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?

The privacy risks outlined in 7.3 above are mitigated by legal requirements and auditing processes (i.e., activity logs) that allow for any auditor, including the Office of Inspector General and the federal monitor, to inspect use and deployment of CAD.

The largest privacy risk is the un-authorized release of personally identifiable information deemed private or offensive in the RCW. To mitigate this risk, the technology falls under the current SPD policies around dissemination of Department data and information reflected in 6.1.

8.0 Monitoring and Enforcement

8.1 Describe how the project/technology maintains a record of any disclosures outside of the department.

Per SPD Policy 12.080, the Crime Records Unit is responsible to receive and record all requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies." Any subpoenas and requests for public disclosure are logged by SPD's Legal Unit. Any action taken, and data released subsequently in response to subpoenas is then tracked through a log maintained by the Legal Unit. Public disclosure requests are tracked through the City's GovQA Public Records Response System, and responses to Public Disclosure Requests, including responsive records provided to a requestor, are retained by SPD for two years after the request is completed.

8.2 What auditing measures are in place to safeguard the information, and policies that pertain to them, as well as who has access to the audit data? Explain whether the project/technology conducts self-audits, third party audits or reviews.

SPD's Audit, Policy and Research Section is authorized to conduct audits of all investigative data collection software and systems. In addition, the Office of Inspector General and the federal monitor can conduct audits of the software, and its use, at any time. Audit data is available to the public via Public Records Request.

The latest CJIS technical security audit from 2017 can be found in Appendix I of this SIR.

Financial Information

Purpose

This section provides a description of the fiscal impact of the surveillance technology, as required by the surveillance ordinance.

1.0 Fiscal Impact

Provide a description of the fiscal impact of the project/technology by answering the questions below.

1.1 Current or potential sources of funding: initial acquisition costs.

Current ☒ potential ☐

Date of initial acquisition	Date of go live	Direct initial acquisition cost	Professional services for acquisition	Other acquisition costs	Initial acquisition funding source
N/A	N/A	N/A	N/A	N/A	General Obligation Bonds, King County Voter-Approved Levy, Capitol Project Fund, and IT Operating Funds.

Notes:

The existing CAD system has been in place for more than 10 years. The documents related to this legacy technology project were purged after six years, per the City's retention schedule, so we are unable to find specific information related to the initial cost of acquiring CAD. The City appropriated $3,228,000 in 2004 for the acquisition of the existing CAD system.

1.2 Current or potential sources of funding: on-going operating costs, including maintenance, licensing, personnel, legal/compliance use auditing, data retention and security costs.

Current ☒ potential ☐

Annual maintenance and licensing	Legal/compliance, audit, data retention and other security costs	Department overhead	IT overhead	Annual funding source
$333,757	N/A	N/A	N/A	N/A

Notes:

This is funded through the City's General Fund. The King County E 9-1-1 Program Office reimburses the City up to 50% of the initial purchase and maintenance costs for CAD, up to 100% of 9-1-1 call taking modules, and up to 25% of data storage costs are reimbursable.

1.3 Cost savings potential through use of the technology

These are not quantified; however, the use of CAD systems is standard practice in emergency response in the United States and has been for decades. Prior to the development of this type of system, 9-1-1 Center call takers wrote the specifics of emergency calls on paper notecards which were delivered to dispatchers on a conveyer belt. The cost savings provided using CAD technology is measured by its impact on efficiencies.

1.4 Current or potential sources of funding including subsidies or free products offered by vendors or governmental entities

The King County E 9-1-1 Program Office reimburses the City up to 50% of the initial purchase and maintenance costs for CAD, up to 100% of 9-1-1 call taking modules, and up to 25% of data storage costs are reimbursable.

Expertise and References

Purpose

The following information is provided to ensure that Council has a group of experts to reference while reviewing the completed surveillance impact report ("SIR"). Any individuals or agencies referenced must be made aware ahead of publication that their information has been included. All materials must be available for Council to access or review, without requiring additional purchase or contract.

1.0 Other Government References

Please list any other government bodies that have implemented this technology and can speak to the implementation of this technology.

Agency, municipality, etc.	Primary contact	Description of current use
Numerous other agencies use Versaterm, including the Anaheim Police Department, the Austin Police Department, the Bellingham Police Department, the Minneapolis Police Department, the San Jose Police Department, and the Salt Lake City Police Department.	No available	Not available

2.0 Academics, Consultants, and Other Experts

Please list any experts in the technology under consideration, or in the technical completion of the service or function the technology is responsible for.

Agency, municipality, etc.	Primary contact	Description of current use
Versaterm	480-663-7739 infoUSA@versaterm.com	Technical support for SPD's use of Versaterm

3.0 White Papers or Other Documents

Please list any authoritative publication, report or guide that is relevant to the use of this technology or this type of technology.

Title	Publication	Link
Standard Functional Specifications for Law Enforcement Computer Aided Dispatch (CAD) Systems	Law Enforcement Information Technology Standards Council (LEITSC)	https://it.ojp.gov/documents/LEITSC_Law_Enforcement_CAD_Systems.pdf

Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet

Purpose

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit ("RET") in order to:

- Provide a framework for the mindful completion of the SIR in a way that is sensitive to the historic exclusion of vulnerable and historically underrepresented communities. Particularly, to inform the public engagement efforts departments will complete as part of the surveillance impact report.
- Highlight and mitigate any impacts on racial equity from the adoption and the use of the technology.
- Highlight and mitigate any disparate impacts on individuals or vulnerable communities.
- Fulfill the public engagement requirements of the surveillance impact report.

Adaptation of the RET for Surveillance Impact Reports

The RET was adapted for the specific use by the Seattle Information Technology Departments' ("Seattle IT") Privacy Team, the Office of Civil Rights ("OCR"), and Change Team members from Seattle IT, Seattle City Light, Seattle Fire Department, Seattle Police Department, and Seattle Department of Transportation.

Racial Equity Toolkit Overview

The vision of the Seattle Race and Social Justice Initiative ("RSJI") is to eliminate racial inequity in the community. To do this requires ending individual racism, institutional racism and structural racism. The RET lays out a process and a set of questions to guide the development, implementation and evaluation of policies, initiatives, programs, and budget issues to address the impacts on racial equity.

1.0 Set Outcomes

1.1. Seattle City Council has defined the following inclusion criteria in the surveillance ordinance, and they serve as important touchstones for the risks departments are being asked to resolve and/or mitigate. Which of the following inclusion criteria apply to this technology?

☐ The technology disparately impacts disadvantaged groups.

☐ There is a high likelihood that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service.
☒ The technology collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection.
☐ The technology raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice.

1.2 What are the potential impacts on civil liberties through the implementation of this technology? How is the department mitigating these risks?

Some personally identifiable information (PII) gathered during emergency responses could be used to identify individuals, such as their name, home address or contact information. Victims of criminal activity may also be identified during incident responses, whose identities should be protected in accordance with RCW 42.56.240 and RCW 70.02.

1.3 What are the risks for racial or ethnicity-based bias through each use or deployment of this technology? How is the department mitigating these risks?

Include a description of any issues that may arise such as algorithmic bias or the possibility for ethnic bias to emerge in people and/or system decision-making.

The mission of the Seattle Police Department is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional and dependable police services. While race and ethnicity information of individuals is recorded in the CAD system, there are no means within the system through which and ethnic bias may emerge. CAD is the real-time record-keeping system for officers' response to calls for police service and its users are subject to SPD's existing policies prohibiting bias-based policing. Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

1.4 Where in the City is the technology used or deployed?

☒ all Seattle neighborhoods

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont

☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County.

If possible, please include any maps or visualizations of historical deployments / use.

N/A

1.4.1 What are the racial demographics of those living in this area or impacted by these issues?

City of Seattle demographics: White - 69.5%; Black or African American - 7.9%; Amer. Indian & Alaska Native - 0.8%; Asian - 13.8%; Native Hawaiian & Pacific Islander - 0.4; Other race - 2.4%; Two or more races - 5.1%; Hispanic or Latino ethnicity (of any race): 6.6%; Persons of color: 33.7%.

King County demographics: White – 70.1%; Black or African American – 6.7%; American Indian & Alaskan Native – 1.1%; Asian, Native Hawaiian, Pacific Islander – 17.2%; Hispanic or Latino (of any race) – 9.4%

1.4.2 How does the Department to ensure diverse neighborhoods, communities, or individuals are not specifically targeted through the use or deployment of this technology?

The CAD system is used to assist in the dispatch of police resources and document SPDs response to requests for service throughout the city of Seattle. There is no distinction in the levels of service this system provides to the various and diverse neighborhoods, communities, or individuals within the city.

1.5 How do decisions around data sharing have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

The Aspen Institute on Community Change defines *structural racism* as "…public policies, institutional practices, cultural representations and other norms [which] work in various, often reinforcing ways to perpetuate racial group inequity."[1] Data sharing has the potential to be a contributing factor to structural racism and thus creating a disparate impact on historically targeted communities. In an effort to mitigate this possibility, SPD has established policies regarding the dissemination of data in connection with criminal prosecutions, Washington Public Records Act (Chapter 42.56 RCW), and other authorized researchers.

Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

Data entered into CAD may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law. See section 6.0 for more details about data sharing.

1.6 How do decisions around data storage and retention have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

Like decisions around data sharing, data storage and retention have similar potential for disparate impact on historically targeted communities. CAD is the real-time record-keeping system for officers' response to calls for police service and its users are subject to SPD's existing policies prohibiting bias-based policing. Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

1.7 What are potential unintended consequences (both negative and positive potential impact)? What proactive steps can you can / have you taken to ensure these consequences do not occur.

The most important unintended possible consequence related to the continued utilization of the CAD system by SPD is the unintentional release of privacy data. The policies in place requiring ACCESS and CJIS certification by all CAD users and the data security processes in place mitigate the likelihood of this occurring.

2.0 Public Outreach

2.1 Organizations who received a personal invitation to participate.

Please include a list of all organizations specifically invited to provide feedback on this technology.

1. ACLU of Washington	2. Ethiopian Community Center	3. Planned Parenthood Votes Northwest and Hawaii
4. ACRS (Asian Counselling and Referral Service)	5. Faith Action Network	6. PROVAIL
7. API Chaya	8. Filipino Advisory Council (SPD)	9. Real Change
10. API Coalition of King County	11. Friends of Little Saigon	12. SCIPDA
13. API Coalition of Pierce County	14. Full Life Care	15. Seattle Japanese American Citizens League (JACL)
16. CAIR	17. Garinagu HounGua	18. Seattle Neighborhood Group
19. CARE	20. Helping Link	21. Senior Center of West Seattle
22. Central International District Business Improvement District	23. Horn of Africa	24. Seniors in Action
25. Church Council of Greater Seattle	26. International ImCDA	27. Somali Family Safety Task Force
28. City of Seattle Community Police Commission (CPC)	29. John T. Williams Organizing Committee	30. South East Effective Development
31. City of Seattle Community Technology Advisory Board	32. Kin On Community Health Care	33. South Park Information and Resource Center SPIARC
34. City of Seattle Human Rights Commission	35. Korean Advisory Council (SPD)	36. STEMPaths Innovation Network
37. Coalition for Refugees from Burma	38. Latina/o Bar Association of Washington	39. University of Washington Women's Center
40. Community Passageways	41. Latino Civic Alliance	42. United Indians of All Tribes Foundation
43. Council of American Islamic Relations - Washington	44. LELO (Legacy of Equality, Leadership, and Organizing)	45. Urban League
46. East African Advisory Council (SPD)	47. Literacy Source	48. Wallingford Boys & Girls Club
49. East African Community Services	50. Millionair Club Charity	51. Washington Association of Criminal Defense Lawyers
52. Education for All	53. Native American Advisory Council (SPD)	54. Washington Hall
55. El Centro de la Raza	56. Northwest Immigrant Rights Project	57. West African Community Council
58. Entre Hermanos	59. OneAmerica	60. YouthCare
61. US Transportation expertise	62. Local 27	63. Local 2898
64. (SPD) Demographic Advisory Council	65. South Seattle Crime Prevention Coalition (SSCPC)	66. CWAC
67. NAAC		

2.2 Additional Outreach Efforts

Department	Outreach Area	Description
SPD	Meeting: South Seattle Crime Prevention Council	Deputy Chief GarthGreen presented the three SPD Group 2 surveillance technologies. One-page summaries and event flyer were distributed. DC GarthGreen and Policy Advisor fielded questions about the technologies. Attendees were directed to the public BKL event and seattle.gov/privacy to provide comment. No physical comment sheets were collected at the event.
SPD	Meeting: Fabulous Forum	Officer Ritter presented this meeting to approximately 40 members of the public. The public meeting flyer was distributed, paired with a brief introduction to the information around SPD's technologies currently open for public comment through 3-5. The Fabulous Forums are designed to provide valuable educational information to the public regarding a variety of topics ranging from the SPD's cultural history, to how the SPD works at enhancing the relationships between Seattle's police and population it serves, employment opportunities, hate crimes education, self defense and much more.
SPD	Meeting: East African Advisory Council	A brief presentation on SPD's group 2 surveillance technologies was given. One-page overviews of the technologies were handed out as resources in both English and translated into Somali. Attendees were directed to seattle.gov/privacy to provide comments on the technologies.
SPD	Meeting	East African Community Senior Lunch
SPD	Meeting: East Precinct Advisory Council at Seattle University	A high level overview of the Surveillance Ordinance was provided. A brief introduction to SPD's group 2 technologies (CopLogic, CAD, 911 Logging Recorder) was also provided. One page overviews of each technology were distributed and attendees were directed to seattle.gov/privacy to provide public comment on the technology.
ITD	Social Media Outreach Plan: Twitter	Directed Tweets and Posts related to Open Public Comment Period for Group 2 Technologies, as well as the BKL event.
SPD, SFD, OPCD, OCR, SPL, SDOT, SPR, SDCI, SCL, OLS, Seattle City Council	Social Media Outreach Plan: Twitter	Tweets and Retweets regarding Group 2 comment period and/or BKL event.
ITD	Press Release	Press release sent to several Seattle media outlets.

ITD	Ethnic Media Press Release	Press Release sent to specific ethnic media publications.
ITD	Social Media Outreach Plan: Facebook Event Post	Seattle IT paid for boosted Facebook posts for their BKL event.
ITD	CTAB	Presented and utilized the Community Technology Advisory Board (CTAB) network and listserv for engaging with interested members of the public
ITD	Blog	Wrote and published a Tech Talk blog post for Group 2 technologies, noting the open public comment period, BKL event, and links to the online survey/comment form.
ITD	Technology Videos	Seattle IT worked with the Seattle Channel to produce several short informational/high level introductory videos on group 2 technologies, which were posted on seattle.gov/privacy. And used at a number of Department of Neighborhoods-led focus groups.

2.3 Scheduled public meeting(s).

Meeting notes, sign-in sheets, all comments received, and questions from the public will be included in Appendix B, C, D, E, F, G, H and I. Comment analysis will be summarized in section 3.0 Public Comment Analysis.

Location	Bertha Knight Landes Room, 1st Floor City Hall 600 4th Avenue, Seattle, WA 98104
Time	February 27, 2018; 6 p.m. – 8 p.m.
Capacity	100+
Link to URL Invite	BKL Event Invitation

2.4 Scheduled focus Group Meeting(s)

Meeting 1

Community Engaged	Council on American-Islamic Relations - Washington (CAIR-WA)
Date	Thursday, February 21, 2019

Meeting 2

Community Engaged	Entre Hermanos
Date	Thursday, February 28, 2019

Meeting 3

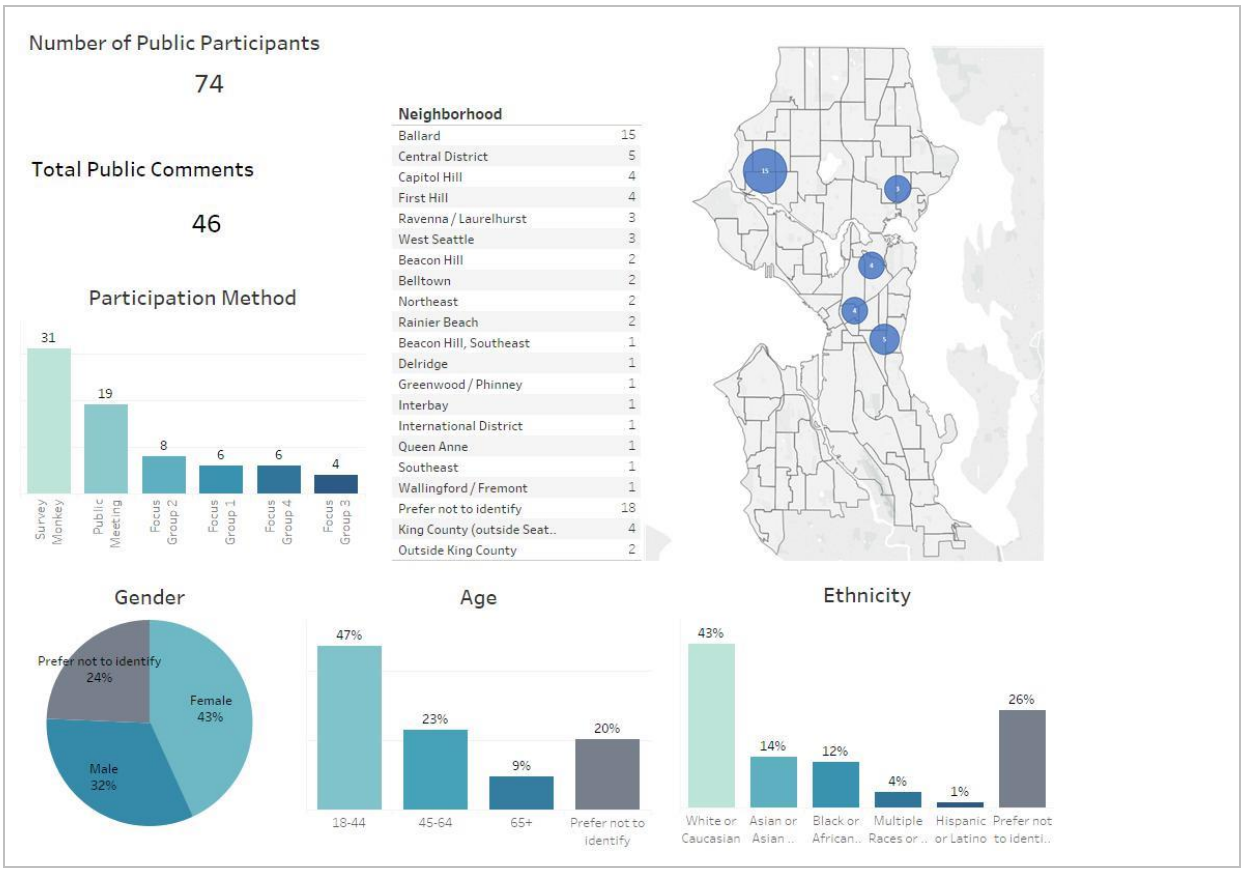
Community Engaged	Byrd Barr Place
Date	Thursday, February 28, 2019

Meeting 4

Community Engaged	Friends of Little Saigon
Date	Wednesday, February 27, 2019

3.0 Public Comment Analysis

3.1 Summary of Response Volume



3.2 Question One: What concerns, if any, do you have about the use of this technology?

Due to the low volume of responses received about this technology, a comment analysis was not able to be completed. Please see Appendix E for all comments received from the public about this technology.

3.3 Question Two: What value, if any, do you see in the use of this technology?

Due to the low volume of responses received about this technology, a comment analysis was not able to be completed. Please see Appendix E for all comments received from the public about this technology.

3.4 Question Three: What do you want City leadership to consider about the use of this technology?

Due to the low volume of responses received about this technology, a comment analysis was not able to be completed. Please see Appendix E for all comments received from the public about this technology.

3.5 Question Four: Do you have any other comments?

Due to the low volume of responses received about this technology, a comment analysis was not able to be completed. Please see Appendix E for all comments received from the public about this technology.

4.0 Equity Annual Reporting

4.1 What metrics for this technology be reported to the CTO for the annual equity assessments?

Respond here.

Privacy and Civil Liberties Assessment

Purpose

This section shall be completed after public engagement has concluded and the department has completed the racial equity toolkit section above. The privacy and civil liberties assessment is completed by the community surveillance working group ("working group"), per the surveillance ordinance which states that the working group shall:

"Provide to the executive and the City Council a privacy and civil liberties impact assessment for each SIR that must be included with any departmental request for surveillance technology acquisition or in-use approval. The impact assessment shall include a description of the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities. The CTO shall share with the working group a copy of the SIR that shall also be posted during the period of public engagement. At the conclusion of the public engagement period, the CTO shall share the final proposed SIR with the working group at least six weeks prior to submittal of the SIR to Council for approval. The working group shall provide its impact assessment in writing to the executive and the City Council for inclusion in the SIR within six weeks of receiving the final proposed SIR. If the working group does not provide the impact assessment before such time, the working group must ask for a two-week extension of time to City Council in writing. If the working group fails to submit an impact statement within eight weeks of receiving the SIR, the department and City Council may proceed with ordinance approval without the impact statement."

Working Group Privacy and Civil Liberties Assessment

The Working Group's Privacy and Civil Liberties Impact Assessment for this technology is below, and is also included in the Ordinance submission package, available as an attachment.

From: Seattle Community Surveillance Working Group (CSWG) To: Seattle City Council

Date: June 4, 2019

Re: Privacy and Civil Liberties Impact Assessment for Computer-Aided Dispatch (Seattle Police Department)

Executive Summary

On April 25, 2019, the CSWG received the Surveillance Impact Report (SIR) on Computer-Aided Dispatch (CAD), a surveillance technology used by the Seattle Police Department (SPD) included in Group 2 of the Seattle Surveillance Ordinance technology review process. This document is CSWG's Privacy and Civil Liberties Impact Assessment for this technology as set forth in SMC 14.18.080(B)(1), which we provide for inclusion in the final SIR submitted to the City Council.

This document first provides recommendations in this executive summary, then provides background information, key concerns, and outstanding questions on CAD technology (SPD).

Our assessment of CAD (SPD) focuses on three major issues rendering protections around this technology inadequate:

(1) No specific policies defining purpose of use.
(2) Lack of clarity on data retention in CAD system.
(3) Lack of clarity on internal and third party access to CAD data.

Recommendations

We recommend that SPD adopt clear and enforceable rules that ensure, at a minimum, the following:

(1) The purpose of use must be clearly defined as emergency operations, and the operation and data collected by the tool must be explicitly restricted to that purpose only.
(2) Data retention within CAD, to the extent there is any, must be limited to the time needed to effectuate the emergency operations purpose defined.
(3) Data sharing with third parties, if any, must be limited to those held to the same restrictions.
(4) Clear policies must govern operation, and all operators should be trained in those policies.

Background on Computer-Aided Dispatch (CAD) (Versaterm)– Seattle Police Department (SPD)

CAD[1] is a software package, provided by Versaterm,[2] utilized by the SPD's 9-1-1 Center to assist 9-1-1 Center call takers and dispatchers with receiving requests for police services, collecting information from 9-1-1 callers, and providing dispatchers with real-time patrol unit availability. The technology consists of a set of servers and software deployed on dedicated terminals in the 9-1-1 center, in SPD computers, and as an application on patrol vehicles' mobile data computers and on some officers' smart phones. The CAD system automatically receives the telephone number, and if available, the name and location of the caller from the West VIPER telephone system[3] for calls placed to 9-1-1. Non-emergency calls and associated phone numbers are not automatically entered into CAD. If the call is determined to be a request for police services, call takers and dispatchers then manually enter additional information into CAD, such as the nature of the emergency, and create a CAD event to facilitate a police response.

The system automatically routes the information recorded by CAD into SPD's Records Management System (RMS) where additional information, such as police reports and supplementary material, is stored.[4]

Overall, our major concerns focus on the use of CAD and/or collected data for purposes other those intended, over-retention of data, and data sharing with third parties (e.g., law enforcement agencies).

[1] https://www.versaterm.com/vcad

[2] https://www.versaterm.com/

[3] https://www.west.com/safety-services/public-safety/call-handling-suite/

[4] 2019 Surveillance Impact Report SPD Computer-Aided Dispatch, Section 2.3, page 9.

Key Concerns

(1) **There is no policy defining the purpose of the technology and limiting its use to that purpose.** SPD appears to have no specific policy defining the purpose of use for CAD and limiting its use to that purpose.

(2) **It is unclear whether and what data is retained within CAD and SPD's Records Management System (RMS).** While the SIR makes clear that CAD data is automatically transferred to SPD's RMS, it is unclear what data, if any, the CAD system itself retains and for how long. If the CAD system does retain some data (for example, call logs) independent of the RMS, and that data is accessible to the vendor, appropriate data protections should be put in place.

(3) **It is unclear which internal and third parties have access to SPD's CAD data.** Section 2.5 of the SIR states: "SPD's authorized users of CAD include all sworn personnel, 9-1-1 Center staff, and other civilian staff whose business needs require access to this data." "Other civilian staff" and the "business needs" requiring access to CAD data are not clearly defined, and it would be helpful to ensure access to CAD data (to the extent any is stored in CAD) clearly tracks with personnel who have a defined need to access such data. In addition, if any third parties access that data, those third parties are not delineated, nor are any parameters or restrictions for their access and/or use laid out.

Outstanding Questions

- Does the CAD system itself store data? If so, what data and for how long? Who can access that data?
- Which third parties have access to SPD's CAD data, and for what purposes may they use it?
- Why are public comments from ACLU-WA and CTAB not included in the SIR transmitted to the CSWG?

Depending on the answers to the questions above, the recommendations above may be modified and/or additional recommendations added.

City of Seattle

CTO Response

Memo

Date: 11/17/2020

To: Seattle City Council, Transportation and Utilities Committee

From: Saad Bashir

Subject: CTO Response to the Surveillance Working Group SPD Computer Aided Dispatch (CAD) SIR Review

---

To the Council Transportation and Utilities Committee Members,

I look forward to continuing to work together with Council and City departments to ensure continued transparency about the use of surveillance technologies and finding a mutually agreeable means to use technology to improve City services while protecting the privacy and civil rights of the residents we serve.

As provided in the Surveillance Ordinance, SMC 14.18.080, this memo outlines the Chief Technology Officer's (CTO's) response to the Surveillance Working Group assessment on the Surveillance Impact Report for Seattle Police Department's Computer Aided Dispatch (CAD).

Background

The Information Technology Department (ITD) is dedicated to the Privacy Principles and Surveillance Ordinance objectives to provide oversight and transparency about the use and acquisition of specialized technologies with potential privacy and civil liberties impacts. All City departments have a shared mission to protect lives and property while balancing technology use and data collection with negative impacts to individuals. This requires ensuring the appropriate use of privacy invasive technologies through technology limitations, policy, training and departmental oversight.

The CTO's role in the SIR process has been to ensure that all City departments comply with Surveillance Ordinance requirements. As part of the review work for surveillance technologies, ITD's Privacy Office has facilitated the creation of the Surveillance Impact Report documentation, including collecting comments and suggestions from the Working Group and members of the public about these technologies. IT and City departments have also worked collaboratively with the Working Group to answer additional questions that came up during their review process.

Technology Purpose

The Seattle Police Department's 9-1-1 Center is the primary Public Safety Answering Point (PSAP) for emergency 9-1-1 calls placed within the City of Seattle. Computer Aided Dispatch (CAD) is a software package utilized by the Seattle Police Department's 9-1-1 Center. It assists 9-1-1 Center call takers and dispatchers with receiving requests for police services, collecting information from 9-1-1 callers, and providing dispatchers with real-time patrol unit availability so dispatchers may dispatch appropriate patrol resources to requests for police service. CAD software also enables real-time documentation of

the Seattle Police Department's response to calls for service, including relevant information obtained by responding officers.

The CAD system automatically receives the telephone number, name (if available), and location of the caller (if available) from the West VIPER telephone system for calls placed to 9-1-1. Non-emergency calls, and associated phone numbers, are not automatically entered into CAD. If the call is determined to be a request for police services, call takers and dispatchers then manually enter additional information into CAD, such as the nature of the emergency, and create a CAD event to facilitate a police response. Call takers and dispatchers may add supplemental information into CAD regarding scene safety, descriptions of individuals, vehicles, and premises. Much of the privacy-sensitive information entered into CAD is provided by 9-1-1 or non-emergency callers or by officers or dispatchers who input information into the CAD system when responding to a call.

Working Group Concerns

In their review, the Working Group has raised concerns about:

(1) No specific policies defining purpose of use.
(2) Lack of clarity on data retention in CAD system.
(3) Lack of clarity on third party access to CAD data.

I have addressed each of these concerns individually below, providing the overall assessment and references to the appropriate responses in the SIR documentation.

Response to Specific WG Concerns: SPD Computer Aided Dispatch

Concern: Defining purpose and policies of data use

CTO Assessment: SPD policies and limitations pertaining to the purpose and use of data collected through the CAD system are clearly outlined in the SIR response, the details of which are provided in the SIR excepts below. The purpose of the data collected by the CAD system is clearly stated in the SIR. In summary, the information collected by the SPD CAD system provides dispatchers with information to enable appropriate resources as needed. CAD software also enables real-time documentation of the Seattle Police Department's response to calls for service, including relevant information obtained by responding officers that may be used for internal and external audit review, legal action, and public records requests. Details of this is provided below:

SIR Response:
Section 4.1: Provide details about what information is being collected from sources other than an individual, including other IT systems, systems of record, commercial data aggregators, publicly available data and/or other City departments.

When an individual places a call to 9-1-1, the telephone number they are calling from, the location they are calling from, the name associated with the phone number (if available from the phone company), and the type of telephone service (landline, cell phone, VOIP phone) are provided by the West VIPER telephone system and automatically entered into CAD when a CAD call is initiated by the call taker. Additionally, private information may be entered into a CAD call by SPD officers requesting information, such as a warrant check, while responding to a request for service.

Section 4.2: What measures are in place to minimize inadvertent or improper collection of data?

A CAD call is initiated when someone requests police services. All users of the CAD system are trained in its use to ensure the data collected is entered appropriately. Authorized users of the CAD system are required to be CJIS certified and adhere to the CJIS security policy, found in the appendices of the SIR.

Concern: Lack of clarity about data retention

CTO Assessment: It is our assessment that SPD has established adequate and clear policy and procedure to adhere to all applicable legal obligations around data retention. Data retention and data handling requirements are dictated by state and municipal law and further based on regulatory Criminal Justice Information Security (CJIS) policy requirements. The specifics about retention of data collected by law enforcement are clearly provided in the SIR. SPD does not have authority to change or adjust these requirements. In summary, unit supervisors are responsible for ensuring compliance and SPD internal and external agencies are part of the audit process to provide oversight. The State of Washington retention schedule for law enforcement agencies may be found online https://www.sos.wa.gov/_assets/archives/recordsmanagement/law-enforcement-records-retention-schedule-v.7.2-(january-2017).pdf .

SIR Response:

Section 5.4: Which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

Unit supervisors are responsible for ensuring compliance with data retention requirements within SPD. To ensure compliance with these legal obligations, SPD's Audit, Policy & Research Section personnel can also conduct audits of all data collection software and systems. Additionally, any appropriate auditor, including the Office of Inspector General and the federal monitor can audit for compliance at any time.
The Criminal Justice Information Security (CJIS) security policy provided in Appendix I of the SIR includes applicable data retention requirements associated with the CAD system. The MCA between SPD and ITD (see Appendix I) is the inter-departmental agreement that ensures compliance with the CJIS Policy.

Concern: Lack of clarity about third party access and data sharing

CTO Assessment: Access to CAD data is limited to authorized SPD personnel, those agencies involved in incident response, and as allowed by the State Public Records Act RCW 42.56. Details about legal obligations, SPD policy and technology access controls for data access and sharing are provided in the SIR, and follow below:

SIR Response:
Section 4.10: What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

- Only authorized SPD users can access the system, technology, or the data collected by the CAD system. Access to the application itself is limited to SPD personnel via password-protected login credentials. All activity within CAD (including timeline of commands issued) generates an auditable log providing detail about user access.
- Data is securely input and used on SPD's password-protected network with access limited to authorized users.
- The entire system is located on the SPD network that is protect by industry standard firewalls. ITD performs routine monitoring of the SPD network.

Criminal Justice Information Security (CJIS) Compliance

The CAD system is CJIS compliant, requirements that outline access control for the data collected. More information on CJIS compliance may be found at the CJIS Security Policy website. CJIS policy requires the following safeguards to be in place:

- All SPD employees must undergo a background check and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.
- The agency shall establish identifier and authenticator processes.

- Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. 08/16/2018 CJISD-ITS-DOC-08140-5.7 37 password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).
- Unsuccessful login attempts - the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10-minute time period unless released by an administrator.
- When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128-bit strength to protect CJI.
- When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption. When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256-bit strength.
- Intrusion Detection Tools/Techniques such as monitor inbound and outbound communications for unusual or unauthorized activities, send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort, employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.

Audit

There are extensive provisions for auditability of the CAD system, including:

- Each CJIS compliant agency using the CAD system is responsible for complying with all audit requirements for use of CJIS Systems. Each CSO is responsible for completing a triennial audit of all agencies with access to CJIS Systems through the CSO's lines.
- SPD's Audit, Policy and Research Section (APRS) can conduct an audit of the any system at any time. The Office of Inspector General and the federal monitor can also access all data and audit for compliance at any time.
- The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.
- A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage.
- Publicly accessible computers shall not be used to access, process, store or transmit CJI.

Section 6.1: Which entity or entities inside and external to the City will be data sharing partners?

Data access and sharing are governed by the following legal and policy agreements:

- No person, outside of SPD and Seattle IT, has direct access to the application or the data.
- As Seattle IT supports the CAD system on behalf of SPD, a Management Control Agreement exists between SPD and Seattle IT. The agreement outlines the specifications for compliance, and enforcement related to supporting the CAD system through inter-departmental partnership.
  "Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBIs Criminal Justice Information Services, (CJIS) Security Policy." The MCA document may be found in Appendix I of the SIR.

- Data obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law.
- Data may be shared with outside entities in connection with criminal prosecutions:
  - Seattle City Attorney's Office
  - King County Prosecuting Attorney's Office
  - King County Department of Public Defense
  - Private Defense Attorneys
  - Seattle Municipal Court
  - King County Superior Court
  - Similar entities where prosecution is in Federal or other State jurisdictions
- Data may be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.
- Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."
- Discrete pieces of data collected by CAD may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by SPD Policy 12.050 and 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayoral Directive, dated February 6, 2018.
- SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the system.

Appendix A: Glossary

Accountable: (taken from the racial equity toolkit.) Responsive to the needs and concerns of those most impacted by the issues you are working on, particularly to communities of color and those historically underrepresented in the civic process.

Community outcomes: (taken from the racial equity toolkit.) The specific result you are seeking to achieve that advances racial equity.

Contracting equity: (taken from the racial equity toolkit.) Efforts to achieve equitable racial outcomes in the way the City spends resources, including goods and services, consultants and contracting.

DON: "department of neighborhoods."

Immigrant and refugee access to services: (taken from the racial equity toolkit.) Government services and resources are easily available and understandable to all Seattle residents, including non-native English speakers. Full and active participation of immigrant and refugee communities exists in Seattle's civic, economic and cultural life.

Inclusive outreach and public engagement: (taken from the racial equity toolkit.) Processes inclusive of people of diverse races, cultures, gender identities, sexual orientations and socio-economic status. Access to information, resources and civic processes so community members can effectively engage in the design and delivery of public services.

Individual racism: (taken from the racial equity toolkit.) Pre-judgment, bias, stereotypes about an individual or group based on race. The impacts of racism on individuals including white people internalizing privilege, and people of color internalizing oppression.

Institutional racism: (taken from the racial equity toolkit.) Organizational programs, policies or procedures that work to the benefit of white people and to the detriment of people of color, usually unintentionally or inadvertently.

OCR: "Office of Civil Rights."

Opportunity areas: (taken from the racial equity toolkit.) One of seven issue areas the City of Seattle is working on in partnership with the community to eliminate racial disparities and create racial equity. They include: education, health, community development, criminal justice, jobs, housing, and the environment.

Racial equity: (taken from the racial equity toolkit.) When social, economic and political opportunities are not predicted based upon a person's race.

Racial inequity: (taken from the racial equity toolkit.) When a person's race can predict their social, economic, and political opportunities and outcomes.

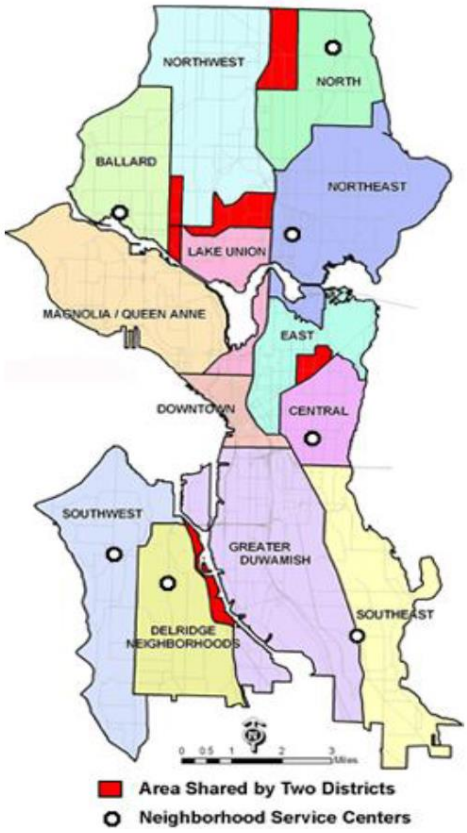
RET: "racial equity toolkit"

Seattle neighborhoods: (taken from the racial equity toolkit neighborhood.) Boundaries defined for the purpose of understanding geographic areas in Seattle.

Stakeholders: (taken from the racial equity toolkit.) Those impacted by proposed policy, program, or budget issue who have potential concerns or issue expertise. Examples might include: specific racial/ethnic groups, other institutions like Seattle housing authority, schools, community-based organizations, change teams, City employees, unions, etc.

Structural racism: (taken from the racial equity toolkit.) The interplay of policies, practices and programs of multiple institutions which leads to adverse outcomes and conditions for communities of color compared to white communities that occurs within the context of racialized historical and cultural conditions.

Surveillance ordinance: Seattle City Council passed ordinance 125376, also referred to as the "surveillance ordinance."



SIR: "surveillance impact report", a document which captures the fulfillment of the Council-defined surveillance technology review process, as required by ordinance 125376.

Workforce equity: (taken from the racial equity toolkit.) Ensure the City's workforce diversity reflects the diversity of Seattle.

City of Seattle

Appendix B: Meeting Notice(s)

City Surveillance Technology Fair

February 27, 2018

6:00 p.m. – 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Join us for a public meeting to comment on a few of the City's surveillance technologies:

Seattle City Light
- Binoculars
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation
- Acyclica

Seattle Fire Department
- Computer Aided Dispatch

Seattle Police Department
- 911 Call Logging Recorder
- Computer Aided Dispatch
- CopLogic

Can't join us in person?

Visit www.seattle.gov/privacy to leave an online comment or send your comment to **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** The Open Comment period is from **February 5 - March 5, 2019.**

Please let us know at Surveillance@seattle.gov if you need any accommodations. For more information, visit Seattle.gov/privacy.

Surveys, sign-in sheets and photos taken at this event are considered a public record and may be subject to public disclosure. For more information see the Public Records Act RCW Chapter 42.56 or visit Seattle.gov/privacy. All comments submitted will be included in the Surveillance Impact Report.

City of Seattle

Giám Sát Thành Phố
Hội Chợ Công Nghệ

ngày 27 tháng 2 năm 2019
6 :00 giờ chiều – 8:00 giờ chiều
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Hãy tham gia cuộc họp công cộng cùng chúng tôi để nhận xét về một số công nghệ giám sát của Thành phố:

Seattle City Light
- Ống nhòm quan sát
- Sensorlink Ampstik
- Đồng hồ đo máy biến áp của Sensorlink

Seattle Department of Transportation (Sở Giao Thông Vận Tải Seattle)
- Acyclica

Seattle Fire Department (Sở Phòng Cháy Chữa Cháy Seattle)
- Hệ Thống Thông Tin Điều Vận Có Máy Tính Trợ Giúp

Seattle Police Department (Sở Cảnh Sát Seattle)
- Hệ Thống Ghi Âm Cuộc Gọi 911
- Hệ Thống Thông Tin Điều Vận Có Máy Tính Trợ Giúp
- CopLogic

Quý vị không thể tới tham dự trực tiếp cùng chúng tôi?

Hãy truy cập www.seattle.gov/privacy và để lại nhận xét trực tuyến hoặc gửi ý kiến của quý vị tới **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** Giai đoạn Góp Ý Mở từ **Ngày 5 tháng 2 - Ngày 5 tháng 3 năm 2019.**

Vui lòng thông báo cho chúng tôi tại Surveillance@seattle.gov nếu quý vị cần bất kỳ điều chỉnh nào. Để có thêm thông tin, hãy truy cập Seattle.gov/privacy.

Các khảo sát, danh sách đăng ký và ảnh chụp tại sự kiện này được coi là thông tin công cộng và có thể được tiết lộ công khai. Để biết thêm thông tin, hãy tham khảo Public Records Act (Đạo Luật Hồ Sơ Công Cộng) RCW Chương 42.56 hoặc truy cập Seattle.gov/privacy. Tất cả các ý kiến đóng góp mà quý vị gửi đến sẽ được đưa vào Báo Cáo Tác Động Giám Sát.

City of Seattle

Eksibisyon ng Teknolohiya Sa Pagmamatyag sa Lungsod

Pebrero 27, 2019

6:00 p.m. - 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Samahan kami para sa isang pampublikong pagpupulong upang magbigay ng komento sa ilan sa mga teknolohiya sa pagmamanman ng Lungsod:

Seattle City Light
- Mga Binocular
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation (Departamento ng Transportasyon ng Seattle)
- Acyclica

Seattle Fire Department (Departamento para sa Sunog ng Seattle)
- Pagdispatsa sa Tulong ng Computer

Seattle Police Department (Departamento ng Pulisya ng Seattle)
- Rekorder ng Pagtawag sa 911
- Pagdispatsa sa Tulong ng Computer
- CopLogic

Hindi kami masasamahan nang personal?

Bumisita sa www.seattle.gov/privacy upang mag-iwan ng online na komento o ipadala ang iyong komento sa **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** Ang panahon ng Bukas na Pagkomento ay sa **Pebrero 5 - Marso 5, 2019.**

Mangyaring ipaalam sa amin sa Surveillance@seattle.gov kung kailangan mo ng anumang tulong. Para sa higit pang impormasyon, bumisita sa Seattle.gov/privacy.

Itinuturing na pampublikong rekord ang mga survey, papel sa pag-sign-in at mga larawan na makukuha sa pangyayaring ito at maaaring mapasailalim sa paghahayag sa publiko. Para sa higit pang impormasyon, tingnan ang Public Records Act (Batas sa Mga Pampublikong Rekord) RCW Kabanata 42.56 o bumisita sa Seattle.gov/privacy. Isasama ang lahat ng isinumiteng komento sa Surveillance Impact Report (Ulat sa Epekto ng Pagmamanman).

City of Seattle

Feria de tecnología de vigilancia ciudadana

27 febrero de 2019

De 6:00 p. m. a 8:00 p. m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Acompáñenos en la reunión pública para dar su opinión sobre algunas de las tecnologías de vigilancia de la ciudad:

Seattle City Light
- Binoculars
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation (Departamento de Transporte de Seattle)
- Acyclica

Seattle Fire Department (Departamento de Bomberos de Seattle)
- Computer Aided Dispatch

Seattle Police Department (Departamento de Policía de Seattle)
- 911 Call Logging Recorder
- Computer Aided Dispatch
- CopLogic

¿No puede asistir en persona?

Visite www.seattle.gov/privacy para dejar un comentario en línea o enviar sus comentarios a **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** El período de comentarios abiertos es desde el **5 de febrero al 5 de marzo de 2019.**

Avísenos en Surveillance@seattle.gov si necesita adaptaciones especiales. Para obtener más información, visite seattle.gov/privacy.

Las encuestas, las planillas de asistencia y las fotos que se tomen en este evento se consideran de dominio público y pueden estar sujetas a la difusión pública. Para obtener más información, consulte la Public Records Act (Ley de Registros Públicos), RCW capítulo 42.56, o visite Seattle.gov/privacy. Todos los comentarios enviados se incluirán en el Informe del efecto de la vigilancia.

City of Seattle

Kormeerida Bandhigga Tiknoolajiyada ee Magaalada

Feebaraayo 27, 2019
6:00 p.m. - 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Nagulasoo biir bandhigga dadweynaha si fikir looga dhiibto dhawr kamid ah aaladaha tiknoolajiyada ee City surveillance:

Seattle City Light
- Binoculars
- Sensorlink Ampstik
- Sensorlink Cabiraha mitirka Gudbiyaha

Seattle Department of Transportation
(Waaxda Gaadiidka ee Seattle)
- Acyclica

Seattle Fire Department
(Waaxda Dab damiska ee Seattle)
- Adeeg Qaybinta Kumbuyuutarka loo adeegsado

Seattle Police Department
(Waaxda Booliiska ee Seattle)
- Qalabka Duuba Wicitaanada 911
- Computer Aided Dispatch
- CopLogic

Nooguma imaan kartid miyaa si toos ah?

Booqo barta www.seattle.gov/privacy si aad fikirkaaga oonleen ahaan uga dhiibato **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.**
Mudada Fikrad Dhiibashadu furantahay waxay kabilaabanaysaa **Feebaraayo 5 - Maarso 5, 2019.**

Fadlan noogusoo gudbi ciwaankaan Surveillance@seattle.gov hadaad ubaahantahay hooy laguusii qabto. Wixii macluumaad dheeri ah, booqo Seattle.gov/privacy.

Xog aruurinada, waraaqaha lasaxixaayo iyo sawirada lagu qaado munaasabadaan waxaa loo aqoonsanayaa diiwaan bulsho waxaana suuragal ah in bulshada lagu dhex faafiyo. Wixii macluumaad dheeri ah kafiiri Public Records Act (Sharciga Diiwaanada Bulshada) RCW Cutubkiisa 42.56 ama booqo Seattle.gov/privacy. Dhammaan fikradaha ladhiibto waxaa lagusoo darayaa Warbixinta ugu danbaysa ee Saamaynta Qalabka Muraaqabada.

City of Seattle

城市监控技术博览会

2019 年 2 月 27 日
下午 6:00 至下午 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 9810

加入我们的公众会议，留下您对纽约市监控技术的意见：

Seattle City Light
- 望远镜
- Sensorlink Ampstik
- Sensorlink 变压器表

Seattle Department of Transportation（西雅图交通局）
- Acyclica

Seattle Fire Department（西雅图消防局）
- 计算机辅助调度

Seattle Police Department（西雅图警察局）
- 911 通话记录录音器
- 计算机辅助调度
- CopLogic

无法亲自前来？

访问 www.seattle.gov/privacy 发表在线评论或将您的意见发送至 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124。开放评论期：2019 年 2 月 5 日至 3 月 5 日。

如果您需要任何住宿服务，请通过 Surveillance@seattle.gov 联系我们。要获得更多信息，请访问 Seattle.gov/privacy。

此次活动中的调查、签到表和照片被视为公共记录，可能会被公开披露。有关更多信息，请参阅 Public Records Act（信息公开法）RCW 第 42.56 章或访问 Seattle.gov/privacy。提交的所有意见都将包含在监控影响报告内。

City of Seattle

도시 감시 기술 박람회

2019 년 2 월 27 일
오후 6:00 – 오후 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

공개모임에 참여하시고, 도시 감시 기술과 관련한 의견을 공유해 주십시오.

Seattle City Light
- 쌍안경
- Sensorlink Ampstik
- Sensorlink 변압기 미터

Seattle Department of Transportation(시애틀 교통국)
- Acyclica

Seattle Fire Department(시애틀 소방국)
- 컴퓨터 지원 출동 지시

Seattle Police Department(시애틀 경찰국)
- 911 전화 기록 녹음기
- 컴퓨터 지원 출동 지시
- CopLogic

현장 참여가 어려우신가요?

www.seattle.gov/privacy 를 방문하셔서 온라인 의견을 남기시거나 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124 로 의견을 송부해 주시기 바랍니다. 공개 의견 수렴 기간은 2019 년 2 월 5 일 – 3 월 5 일입니다.

편의사항이 필요하신 경우 Surveillance@seattle.gov 로 문의해 주시기 바랍니다.
자세한 정보는 Seattle.gov/privacy 를 참조해 주십시오.

본 행사에서 수집된 설문 조사, 참가 신청서 및 사진은 공개 기록으로 간주되며 일반에 공개될 수 있습니다. 자세한 사항은 Public Records Act(공공기록물법) RCW 챕터 42.56 을 참조하시거나, Seattle.gov/privacy 를 방문하시기 바랍니다. 제출된 모든 의견은 감시 영향 보고서에 수록됩니다.

City of Seattle

城市監視技術展覽會

2019 年 2 月 27 日
下午 6:00 至下午 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

加入我們的公眾會議，留下您對紐約市監視技術的意見：

Seattle City Light
- 望遠鏡
- Sensorlink Ampstik
- Sensorlink 變壓器表

Seattle Department of Transportation（西雅圖交通局）
- Acyclica

Seattle Fire Department（西雅圖消防局）
- 電腦輔助發送

Seattle Police Department（西雅圖警察局）
- 911 通話紀錄錄音機
- 電腦輔助發送
- CopLogic

無法親自前來？

造訪 www.seattle.gov/privacy 發表線上評論或將您的意見傳送至 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124。開放評論期：2019 年 2 月 5 日至 3 月 5 日。

如果您需要任何便利服務，請透過 Surveillance@seattle.gov 聯絡我們。要獲得更多資訊，請造訪 Seattle.gov/privacy。

此次活動中的調查、簽入表和照片被視為公共紀錄，可能會被公開披露。有關更多資訊，請查閱 Public Records Act（資訊公開法）RCW 第 42.56 章或造訪 Seattle.gov/privacy。提交的所有意見都將包含在監視影響報告內。

City of Seattle

Appendix C: Meeting Sign-in Sheet(s)

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☒ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☒ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

☐ Include Middle Eastern

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☒ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☒ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☑ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☑ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☑ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☒ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☒ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☑ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☒ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☒ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☑ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☑ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☑ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

2

Queen Anne

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☑ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☑ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☒ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- [x] Ballard
- [ ] Belltown
- [ ] Beacon Hill
- [ ] Capitol Hill
- [ ] Central District
- [ ] Columbia City
- [ ] Delridge
- [ ] First Hill
- [ ] Georgetown
- [ ] Greenwood / Phinney
- [ ] International District
- [ ] Interbay
- [ ] North
- [ ] Northeast
- [ ] Northwest
- [ ] Madison Park / Madison Valley
- [ ] Magnolia
- [ ] Rainier Beach
- [ ] Ravenna / Laurelhurst
- [ ] South Lake Union / Eastlake
- [ ] Southeast
- [ ] Southwest
- [ ] South Park
- [ ] Wallingford / Fremont
- [ ] West Seattle
- [ ] King county (outside Seattle)
- [ ] Outside King County

Race/Ethnicity

- [ ] American Indian or Alaska Native
- [ ] Asian
- [ ] Black or African American
- [ ] Hispanic or Latino
- [ ] Native Hawaiian or other Pacific Islander
- [x] White
- [ ] Prefer not to Identify

Age

- [ ] Under 18
- [x] 18-44
- [ ] 45-64
- [ ] 65+
- [ ] Prefer not to identify

Gender

- [x] Female
- [ ] Male
- [ ] Transgender
- [ ] Prefer not to identify

Neighborhood

- [ ] Ballard
- [ ] Belltown
- [ ] Beacon Hill
- [ ] Capitol Hill
- [ ] Central District
- [ ] Columbia City
- [ ] Delridge
- [ ] First Hill
- [ ] Georgetown
- [ ] Greenwood / Phinney
- [ ] International District
- [ ] Interbay
- [ ] North
- [ ] Northeast
- [ ] Northwest
- [ ] Madison Park / Madison Valley
- [ ] Magnolia
- [ ] Rainier Beach
- [ ] Ravenna / Laurelhurst
- [ ] South Lake Union / Eastlake
- [ ] Southeast
- [ ] Southwest
- [ ] South Park
- [x] Wallingford / Fremont
- [ ] West Seattle
- [ ] King county (outside Seattle)
- [ ] Outside King County

Race/Ethnicity

- [ ] American Indian or Alaska Native
- [ ] Asian
- [ ] Black or African American
- [ ] Hispanic or Latino
- [ ] Native Hawaiian or other Pacific Islander
- [x] White
- [ ] Prefer not to Identify

Age

- [ ] Under 18
- [x] 18-44
- [ ] 45-64
- [ ] 65+
- [ ] Prefer not to identify

Gender

- [ ] Female
- [x] Male
- [ ] Transgender
- [ ] Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☑ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☑ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

X

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☒ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☒ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☒ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☒ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☒ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☒ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☑ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

leighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
] Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☒ 18-44
☐ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☒ Female
☐ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☑ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
] Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☐ 45-64
☑ 65+
☐ Prefer not to identify

Gender

☐ Female
☑ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

☑ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
] Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☑ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☑ Female
☐ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

SE KING COUNTY

☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☑ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
✓ Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☑ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☐ Female
☑ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☒ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☒ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☒ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☒ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☒ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☑ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☑ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☑ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☑ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☑ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☑ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Appendix D: Department of Neighborhood Focus Group Notes

Friends of Little Saigon (FOLS)

Please select which technology you wish to comment on:

☐SCL: Binoculars ☐SCL: Sensorlink Transformer Meter (TMS) ☐SFD: Computer-Aided Dispatch ☐SPD:9-11 Call Recorder

☐SCL: Sensorlink Ampstik ☐SDOT: Acyclica ☐SPD: Computer-Aided Dispatch ☒SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

- Will they keep the data safe on coplogic?
- Can it be hacked?
- What if you report your neighbour and your neighbour hacks the system and find out?
- What is the money amount limit for coplogic / Why is there a limit for coplogic?: (a community member says that she believes that the limit $500 or under, but it's hard to have a limit because a lot of packages cost more than $500 such as electronics get stolen and you won't be able to report it online)
- The departement is having all these technologies being used but not letting the public aware of it
- Coplogic is not clear and is confusing to use (what you can report and what you can't report)
- If coplogic is known by the community would they use it ? (Community members agreed that no one would use coplogic because it's not in Vietnamese. Not even people who speak english fluently even use it.
- Many community members don't trust the system)

What value, if any, do you see in the use of this technology?

- Coplogic has been going on for a few years it's not very effective. The only effective thing is that coplogic is doing saving police hours and time.

What do you want City leadership to consider about the use of this technology?

- Most of the time, our community don't report things because they don't trust the system, they often tell someone that they trust a friend. Is there an option that someone and report a crime for someone else?

Other comments:

- The government should be more transparent with the technology system with the public.

- The translation is much far removed from the actual Vietnamese language.
- The translation is very hard to understand, the language is out of context (The flyer is poorly translate)
- Is there resources to support these technologies? Is there translations so that it is accessible for everyone? Will this accommodate everyone?
- Police should have a software that connects them to translation and interpretation right away instead of having to call a translator
- How will other people know of the technology if they can't come to focus group meetings? Such as flyers? Social media? Etc.
- Besides face to face meetings, are there plans to execute this information of the technology and surveillance to the community?
- Will the City of Seattle go to community events, temple, the church to reach out to the community and explain the technologies?
- These technologies are taking a part of our taxes, so everyone should know. It should be for everyone to know, not only catered to one group or population.

Are there any questions you have, or areas you would like more clarification?

- How effective are the tools/technology?
- How many people know of these technologies? Provide statistics
- What are the statistics of the coplogic?
- What is the data and statistics for coplogic and what are people reporting?
- What is the most common crime that they are reporting?
- And how effective is coplogic based on the statistics and data?

City of Seattle

Friends of Little Saigon (FOLS)

Please select which technology you wish to comment on:

☐SCL: Binoculars ☐SCL: Sensorlink Transformer Meter (TMS) ☐SFD: Computer-Aided Dispatch ☒SPD:9-11 Call Recorder

☐SCL: Sensorlink Ampstik ☐SDOT: Acyclica ☒SPD: Computer-Aided Dispatch ☐SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

- CAD did not work from experience. A community member said that they reported that they needed assistance at 10:00pm and no one showed up, then had to call 911 at 12:00am and someone finally showed up at 4:30am
- Why create more options and technologies if the police department and government can not support it? It's a waste of time and money (taxes). Should have enough personals before they implement technology.
- Government should have enough personals to support translation if they choose to translate.

What do you want City leadership to consider about the use of this technology?

- The city should focus on having the community review the technologies that are yet to be implemented.
- The Vietnamese community is not getting the information we need to report crimes

Other comments:

- Engagement is very important. Engaging the community and engaging different demographics.
- Friday night, Saturdays, and Sunday afternoon work the best for the Vietnamese community.
- If the city wants to involve the vietnamese community and engage the Vietnamese community, it is important to accommodate with our community It is important to proofread the translation, have 3 people proofread. Someone
  pre 1975, post 1975 and current Vietnamese language. The government clearly does not proofread the translation.

Council on American Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington
Thursday, Feb. 21, 2019
Technology Discussed: CopLogic

1. Do you have concerns about this specific technology or how it's used?
    - Having used the system myself the one thing I noted was the type of report you can file, they ask questions like if you knew the suspect, and if you're saying no I don't know who did it. and you check a box that says I understand that no one is going to investigate this
        - What is the point of having a system in place than If no one is going to investigate it
        - It is for common things like my car is broken into and stuff was taken out of my car, you can file it if you need a report for insurance. But if you were to call that and report to the police, they wouldn't come for days
    - So for example if I can be a straight up Islamophobe and I can see a Muslim woman and make a bunch of false reports online, and how long would it take for someone to say I see you making all these reports. Because people can make so many different reports, how do you deal with that
        - There are very limited types of reports that it will accept. So if someone wanted to report graffiti and they were reporting more hate crime related graffiti an officer will review the report
        - So I think the review process would be really important
    - Another barrier is that it's an online system so we need to think about wifi access and there is this assumption that everyone has access to internet and computers. And what I'm hearing is that people can just file a report at a click of their finger. And if these people can do that on their computer what stops them from being able to file all these cases about certain groups and individuals.
    - Additional there have been cases in the past where people are abusing reporting system. This one doesn't allow you to report against known suspect but I could see that happening in the future so I wanted that to be mentioned. The other thing under protection is says all activity can be stored and the data Is monitored by lexis nexus… and this company does a lot of research on crime mapping which brings up some of the concerns on like CVE
        - But what you are saying is that lexis nexus does other mapping that it can use this information for
        - Yes, because I want to clarify what is the technological ambition of SPD because I don't think this would work well in the communities that SPD is supposed to served. And I would want a contract review of what lexis nexus does. Will the info stay on the data and server of lexis nexus, what happens to it
    - Another thing is has SPD given Lexis nexus to use this in any of the research data they do, because they put out a lot of information regarding mapping, and crime control. And what information are they allowed to take
    - We have seen recently people doing interesting things when reporting crimes. I think its important to realize that when reporting crime people have a different perception when

reporting crime. People will see you in a certain neighborhood and might think they stole that car, or are doing something bad here. So when we give people the ability to report online we need to be concerned with accessibility about people being able to report freely… and we saw for a year that if an African American person came to use a swimming pool someone can call and say they don't live here. I think SPD is trying alleviate some of those calls they are getting, but I don't think this is the solution to the problem
    - What is the logic behind this overall, because is seems like it presents more cons than pros, and what is analytics database you use to look at these reports. Because when I am using government data base I can see where I need more surveillance etc. so we are getting all these open wholes in the system. Is this a right wing Donald trump agenda to watch neighbors of color and surveillance
    - I think im more concerned with where does this information end up and how is it used
    - What is the usefulness of the information that is not followed up on. And how does it help the people it's actually serving? So for example someone works for an anti-Muslim white supremacy group and they have people in different areas report issues about different Muslim groups in Seattle how do you prove the validity of these information and make sure they aren't just causing harm
2. What value do you think this brings to our city?
    - I think technology saves time, money, makes filing a report easy, I had to do that once it takes a lot of time.
    - I appreciate that it is easier so something like a hit or run or a car breaking in, that's fine.
3. What worries you about how this is used?
    - The only issues I can think of right now is it seems like it would be very easy to make a fraudulent report or a report that is for a small thing that you can make into a big thing, like the things you see go viral on the internet. So now it seems like the barrier to making a police report is smaller
    - I agree I think the bar is lowered and different people are perceived differently. And we have seen how SPD criminalizes different communities for behaviors that don't need to be criminalizing
    - A lot of different kinds of reports have to do with peoples perceived notion, so my concern comes from how do we make sure that this kind of technology isn't used to map our where Muslims live/are, and there types of religious belief. Or isn't being used to monitor them. How do we ensure that this isn't used to map our communities
    - The only comment I have that in the forms I have filled out is it won't allow you to fill out the form if you are naming a specific individual, you can name a group, but a not a person. The following criteria is there no known suspects, it happens in Seattle, so things like thefts. So you can report, graffiti, identity theft, credit card fraud, simple shop lift. So when I click report it says if you have a suspect it says please call. And when I press report it allows me to report anonymously, so I could report against a community with no follow up
        - Well that doesn't stop them from targeting al-Noor masjid, or Safeway in new holly, or new holly gathering hall, and it can target the people in that

community. And people don't feel comfortable with increase police presences, so it targets area if not targeting people

- When I was buying the house in Dallas (participant currently still lives/works/plays in Seattle) one of the first things I did was looking at a crime map and based off of that if someone is making a lot of reports can that be used for crime mapping because than that can lower the property value. And if the police isn't following up then how is it being used
- Its definitely possible for people to report inaccurate information

4. What recommendations would you give policy makers at the City about this technology?
    a. But my concern is reporting someone that can really target people of color. And that happens much more threatening to people. So the concept of an upset black women is more intimidating than an upset women that is another race and how many times will behavior like that be reported. Or how many times will a black man be reported against because it seems scary. So I think it lowers the bar when you don't have to talk to an individual when you don't have to talk to a police
    b. My questions are, how accessible are cop logic to people who don't read or speak English. How is SPD going to do what they can to make sure that this doesn't negatively impact communities they are already having issues with like the Sea Tac community that already feels threaten and criminalized by communities.

5. Can you imagine another way to solve the problem this technology solves?
    - So the SPD is very data driven these days and the one thing we repeat is report report report, call 911 and report online whatever you thinking is happening because all of that goes into their data base and is used for them to use resources and put police based off of where there is more crime. The report report report mentality assumes there are good relationships between the community and police, so even if someone doesn't do something bad, I don't know that they would feel comfortable reporting, even if online
    - From the community I have come from I am almost certain that they haven't even used online reporting so how do we make sure that we are giving everyone access to use online reporting. And there are certain crimes that are so common in areas that they don't even report it because they think the police should already know about it
    - I think the department should solely rely on the technology only as a way of collecting info they should still use in personal resources to actively participant in local community and make connections you can't rely only on this technology alone to do this

6. Other comments
    a. Also in this day in age we need to consider that immigration is a issue, and this administrative has blended the different agencies so people have a hard time knowing where SPD starts and ICE starts and those lines have been blurred and that is a real concern for many families

Council on Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington

Thursday, Feb. 21, 2019

Technology Discussed: Binoculars/Spotting Scope

1. Do you have concerns about this specific technology or how it's used?
    . People in our community don't have the access to say or be apart of these conversation. A lot of these people are literate, and might not have the same cultural values. For Muslim women there are a type of consent that you have when you walk outside and are covered in a certain away versus when you are in the privacy of your own home. And people might not have that cultural and religious awareness
    a. I had one quick concerns, as far as the data that is collected using these binoculars, who has access to it
        - Seattle City Light: Information goes into the billing system, which customers can access if they have the automated reader but do not have access to under the current system
    - I know the focus is on binoculars but my mind is on new technologies and when people who are consumers and feel like I am overcharged how do I follow up and get those issues resolved. For systems that are completed based off of technologies how will I know if that data is being altered.
    b.
2. What value do you think this brings to our city?
    . I would just add this is more my general comments I think its good that Seattle city lights is providing notifications to people when this is happening. Are they wearing something visible that show people they are from Seattle city lights? And is there a way for people to complain?
        - Yes they are wearing vests that are very visible. Yes we have a couple different avenues the easiest is to call the customer service line and to submit a complaint there
3. What worries you about how this is used?
    . My primary concerns on my end is if someone is looking into my home with binoculars its a privacy concern. Most Muslim women wear hijab and I don't feel comfortable if someone is using binoculars looking from the outside when we are not wearing the hijab. My concern is that it is a huge invasion of privacy
    a. I have a question as the women expressed the feeling of people reading the meters with binoculars, if the meter has abnormal behavior or is in a different place of the house. Have there been situations where someone sees the person looking at someone house with binoculars, and they might not have gotten

notified. Or the meter might be on the opposite side of where they are looking. Are they getting background checks? Or are complaints being followed up

- Seattle City Light: Yes all city employees have background checks, and if a complaint gets called in they will go through disciplinary actions
- What are the average times for disciplinary actions. How long is the process for a full investigation
- Seattle City Light: It's a multiple step process in terms of different levels. There are warnings, and if there was undo actions. Timeline really depends, I'm not sure
- Cause I think that people who go through the different nuances of how privacy can be breach that is just the end all be all of how privacy can breach so I think there needs to be policy put in place so that people don't have their privacy breach and they are being monitored by a pedophile

4. What recommendations would you give policy makers at the City about this technology?
   . When I look at the Seattle city of light they do a lot of estimated guesses and as a consumer they might give you a $500 fee based off of the estimated guesses so I think it is important to have some sort of device that better clearly shows how much you use

5. Can you imagine another way to solve the problem this technology solves?
   . My other question is if its actually not efficient why do you get the option to opt out (of the new automated system). If there is an old school way of doing it that involves a breach of privacy because these are human beings using the binoculars, so If this other option is better why are people having the ability to opt out.
6. Other comments: (Many comments were discussed over Seattle City Light's upcoming change from binocular use to automated meter readers)
   . Who opted out was it home owners?
   a. When we go to a place with 12 tenements do all 12 of them have the ability to opt out or in, or just the owners of the building?
   b. Each home owner has a schedule provided to them and it is a 3 day period which they can come in and look at the system
   c. Is there a cost to them to have the new meter.
      - Seattle City Light: There is no cost with getting the new meter, but there is still a cost If we have to send someone out there to read it
      - What I don't understand is why the new practice is not to just use the new system since that is more accurate and it is doesn't require binoculars
      - What is the cost of opting out

    - Seattle City Light: There is a flat rate
- I was gonna reiterate when we talk about equity and equitable practices. You can opt out (of the automated system) but there is a fee. And it makes me think how much of It is a choose if one of these you have to pay for and the other one is free. So that sounds a little problematic when looking at choices of equity. I think choices are great, but also people need to be well informed. Like people within the community need to have more clear information to make the best decision for themselves
- Going back to people who make the decision. I want the person who are living in the house to know what decision is being made. So not just the person who owns the house, but the person living in the home. And not everyone it literate and not everyone speaks English. And its really important that you are giving them information they can actually consume. Instead of giving them notices they cant read

Council on Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington
Thursday, Feb. 21, 2019
Technology Discussed: Acyclica

1. Do you have concerns about this specific technology or how it's used?
    - Where does this data go? Does it go to SDOT? Google maps?
    - My other question is, it said whatever is being transferred is encrypted. All encrypted means to me is getting data from one device to another will be transferred without it being intercepted. What I don't know is, how much information are people getting
    - My concern is related to data, yeah we like to use gps. But what is the perimeter, what is the breach of access. Where is the data being used, and what can that turn into. we might be okay if the data is only being used for traffic related updates, but they might use it for more
    - I also would like to see how acyclica actually does what they do. They are using a lot of words that normally don't know. So I want to know how exactly they are hashing and salting. So for them to be clear about how they doing it. like when whatsapp encrypted they didn't give us the exact code but told us how they are doing it
    - Asking for a greater transparency for how they are doing this
    - I think the purpose of it is really important but the biggest concern is collecting all of this information without consent of passersby.
    - So the specific identifier that acyclica uses it mac addresses? You could potentially use that number to track that phone for the lifetime of the phone, for as long as that phone is on and being used. And that is very concerning.
    - Also I want to understand more where is this data going, and I want to know if this data is going to be used for future projects.
    - I want to ask is this something people opt into
    - People don't even know this is being used

2. What value do you think this brings to our city?
    - I like getting places and I like getting traffic information.
3. What worries you about how this is used?
    - What I don't like is you using my phone to get that information. I want whatever is in my cellphone to be protected. And I wanna know what you can access
    - I think based on Seattle and Seatac's higher up wanting to monitor and map out Muslims and where they are, and I don't like people being able to use our phone to track our location or actions they might think is violent. So based off of Seattle's track record and law enforcement agencies I don't like it
    - People who live outside of Seattle are also being impacted by it anytime they drive in Seattle
    - Could someone "opt out" by having wifi disabled on their device? I don't know if this covers cell towers. Because if it covers cell towers the only thing you could is having your phone on airplane mode

4. What recommendations would you give policy makers at the City about this technology?
    - I think the big question is why aren't we using other vendors, like I mentioned google maps, or waze, in fact komo 4 uses ways. Where other options we're looked at, and what were the trade off there's. And I want to see some transparency between the decision-making processes
    - I don't think this data should be shared with other private agencies, or other interagency programs
    - If all you're looking at is traffic flow, why are you not using the sensors in the road to give traffic flow updates.
    -
5. Can you imagine another way to solve the problem this technology solves?
    - I don't know if this already exists but something that makes it that data can't be used from one technology and use it for a different purposes
    - I think speaking from an industry perspective that is really important to have a processes for. Because all of this data is being used regardless of if you live in Seattle, or people live in different countries even who are visiting. That data is being collected. My understanding is that SDOT doesn't get the data directly. So my concern is how long can acyclica keep this data, use this data. Why wasn't a different option used, one in which some sort of consent can be used, so something like waze, google maps where people can opt in can get that information.
    - Road sensors or ways to count cars
    - I think its better to count cars than phones, because there is some expectation that your car will be monitored.
    - Using vehicle level granularity

City of Seattle

Entre Hermanos

Please select which technology you wish to comment on:

☐SCL: Binoculars	☐SCL: Sensorlink Transformer Meter (TMS)	☐SFD: Computer-Aided Dispatch	☐SPD:9-11 Call Recorder
☐SCL: Sensorlink Ampstik	☒SDOT: Acyclica	☐SPD: Computer-Aided Dispatch	☐SPD: CopLogic

1) What concerns, if any, do you have about the use of this technology?

El uso de wifi en Acyclica porque pueden obtener toda la información de los teléfonos.

Si vale la pena la inversión

Enfocando al grupo: La tecnología ya está instalada. que les preocupa de su uso?

El tráfico sigue igual.

Quien usa o almacena la información.

La preocupación es la colección de data.

Colección y almacenamiento de información es la mayor preocupación.

No es la colección de data lo alarmante sino los recursos (dinero utilizado) ya que o la tecnología no están funcionando porque el tráfico sigue igual. No hay cambio con la nueva tecnología, esos gastos no son válidos ya que no hay resultados. Esos gastos pudieran ser utilizados para la comunidad.

También tienen que ver si la tecnología emite radiación o alguna otra cosa dañina; perjudicial a la salud.

El gobierno tiene todos los datos.

No necesitan esta tecnología para tener los datos porque ya existen métodos para eso, incluso aplicaciones o alguna otra cosa.

La otra preocupación del grupo es que no haya un cambio al problema que se quiere resolver. En el caso de Acrylica sería el mejorar el tráfico.

- Tecnologías como esta necesitan recolectar más opiniones de expertos.
- Sería bueno que la información sea compartida con la comunidad. (Transparencia en fines y objetivos de la tecnología y datos guardados, tácticas implementadas.)

2) What do you want City leadership to consider about the use of this technology?

Hay lugares donde no se necesitan. En algunas partes de Magnolia, Queen Anne, Northgate, no se ocupan.

Seguimiento de pregunta: En las comunidades donde viven los latinos que tanto se ocupa Acyclica?

Participante no cree que allí se ocupan.

Hablaron sobre la necesitad de puntos estratégicos y calles con más necesidad de ayuda por causa del tráfico.

What do you think about this technology in particular ?

Bien, la tecnología ayuda con la velocidad o el movimiento de los coches.

La información se guarda y analizan por donde viajas o cuantas veces cruzas este rastreo.

Si es solo para ver el tráfico está bien.

Está bien en algunas partes. Puede que sea algo bueno. Pero puede que esta tecnología pueda compartir información personal que puede ser utilizada de otra forma en especial si hay Hacking (forma negativa, uso de datos).

La tecnología en sí no es tan grande (de tamaño) para ser algo visualmente desagradable. La información captada a través de estos medios puede que ayude a conducir el tráfico de mejor manera pero también puede que tome información personal.

Are there any questions you have, or areas you would like more clarification? ●

La tecnología no es un router, sino colección de data para planeaciones urbanas.

Participante: “quiero creer” “convencerme” que los sensores están allí para ayudar con el tráfico.

No se sabe cuándo las instalaron, los resultados deberían de ser públicos. Si la tecnología es para aliviar el flujo de tráfico entonces por qué no extienden el programa? O por qué no hay mejoramiento del tráfico?

Alternatives to this technology

- Alguna pantalla que indique cuáles vías son alternativas puede reemplazar esto.
- Cambios al límite de velocidad puede que alivie el flujo del tráfico.
- Dejar de construir tanto.
- Rediseño de calles ayudaría flujo de tráfico.
- El rediseñar las vías servirá para las futuras generaciones.

City of Seattle

Entre Hermanos

Please select which technology you wish to comment on:

☒SCL: Binoculars ☒SCL: Sensorlink Transformer Meter (TMS) ☐SFD: Computer-Aided Dispatch ☐SPD:9-11 Call Recorder

☐SCL: Sensorlink Ampstik ☐SDOT: Acyclica ☐SPD: Computer-Aided Dispatch ☐SPD: CopLogic

1) What concerns, if any, do you have about the use of this technology?

Los binoculares son preocupantes si la persona no tiene ética. Es preocupante que una persona vea a través de binoculares a que una tecnología mida el uso de la electricidad

Al grupo le incomoda el uso de binoculares

Sensorlynk específicamente la preocupación sería que le quita el trabajo a una persona.

Si es para detectar robo el grupo cree que hay otras maneras de saber quien roba

que no tan solo será para leer la electricidad sino para obtener otros tipos de información si cámaras fueran usadas

2) What value, if any, do you see in the use of this technology?

Ahorro de energía

Record y datos mas precisos

Oportunidad de trabajo a quien utiliza los binoculares

Estabiliza los precios de la electricidad

3) What do you want City leadership to consider about the use of this technology?

: Usar background check, uso de uniforme por trabajadores, cámara en binoculares.

What do you think about this technology in particular ?

Sensorlink Si

Binoculares son invasivos

Are there any questions you have, or areas you would like more clarification? ●

La confianza en estos medidores serán confiables? Serán efectivos?

El uso de binoculares se puede acompañar de una cámara añadida

Alternatives to this technology

Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad

City of Seattle

Entre Hermanos

Please select which technology you wish to comment on:

☐SCL: Binoculars ☐SCL: Sensorlink Transformer Meter (TMS) ☐SFD: Computer-Aided Dispatch ☐SPD:9-11 Call Recorder

☐SCL: Sensorlink Ampstik ☐SDOT: Acyclica ☐SPD: Computer-Aided Dispatch ☒SPD: CopLogic

1) What concerns, if any, do you have about the use of this technology?

Las fallas electrónicas son preocupantes especialmente en reportes policiacos.

Las preocupaciones es que el reporte no salió, no llegó por cualquier razón.

No todos podrán o saben usar las computadoras.

Fallas de los algoritmos de cada demanda es alarmante.

Que y cuando determina la urgencia de respuesta

Las personas le temen a los policías. Y este medio puede ayudar a que el miedo disminuya.

La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

2) What value, if any, do you see in the use of this technology?

La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

El uso de computadora está bien para las denuncias.

Si personas usan esta tecnología y es analizada en tiempo real por otras personas no hay problema.

Es otro método para denunciar

Está de acuerdo con el uso de computadoras para denunciar solo que no todos son capaz de usar este método/tecnología.

3) What do you want City leadership to consider about the use of this technology?
Que sea multi-idioma, implementar audio, implementar sistemas que ayuden a múltiples personas con diversas capacidades/necesidades

Si es usada de manera adecuada y como han dicho está bien.

El uso de la tecnología es bueno para dar respuesta para todas las cosas y personas

What do you think about this technology in particular ?

Grupo están de acuerdo con su uso.

Puede salvar una vida.

Los riesgos y acciones determinan la urgencia de la intermisión policiaca.

Alguna gente se siente más capaz de presentar una queja a través de este sistema, la tecnología en uso tiene validez.

Bueno para la violencia doméstica.

Are there any questions you have, or areas you would like more clarification?

La computadora decidirá la importancia/urgencia del reporte/emergencia dando a llevar acciones de emergencia.

Gravedad de emergencia es determina por tecnología.

La definición de emergencia es diferente con cada persona.

Cada uno tiene la definición de vigilancia, pero ¿que tal la definición de emergencia?

SITUATIONS TO APPLY ITS USE

Una pelea en la calle, un malestar corporal, cuestiones de vida, abuso doméstico

Si nos basamos en la definición de emergencia sólo en cuanto estemos en peligro inmediato o en tiempos mínimos/ de transcurrencia alarmante/peligrosa el uso de será implementado o limitado solo a instantes inmediatos de peligro.

Para reportar algo que ya sucedió o que son recurrentes.

Basado en el concepto de emergencia, las personas pueden tomar el método adecuado para reportar su caso y a través del medio necesario.

Los reportes no son anónimos.

Los datos son recolectados aun, a pesar de la opción escogida.

Alternatives to this technology

Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad

Entre Hermanos

City of Seattle
Surveillance

Inicio

Resumen: El departamento de vecindarios quiere saber la opinión de este grupo. Ellos verán videos de un minuto y medio y encontrarán folletos en sus mesas donde encontraran más información sobre lo visto.

Demográficos:

Ocho personas participaron, una de West Seattle, una de First Hill, dos de Ravenna/Laurelhurst y cuatro de King County (outside Seattle).

Cuatro personas se consideraron hispano o latino, una como india americana o nativa de Alaska, y tres no opinaron.

Cinco personas marcaron 18-44 como su rango de edad, dos marcaron 45-64 como el suyo y una no opinó.

Cinco personas marcaron masculino como género, una como transgénero, una como femenino, y otra no opinó.

Otra Información Importante:

- Preguntas serán hechas.
- Habrá una hoja para poder conversar sobre videos de interés
- Se les agradeció por venir.
- El concepto de vigilancia será manejado como la ciudad de Seattle lo maneja.
- Tom: Agradeció a los invitados por venir

Surveillance. In 2017 city council passed an ordinance to see what technology fit the definition of surveillance. The information gathered by these surveillance technologies are as follows: to “observe or analyze the movements, behaviors, or actions of identifiable individuals in a manner” which "is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice.”

Presentador: Preguntó si la conversación en inglés fue entendida.

Grupo: Concordó.

Tom: Do not let information on videos stop you from making comments or raising questions.

Presentador: Dio a entender el concepto de vigilancia como ha sido interpretada por la ciudad de Seattle. Fue analizada de esta manera: “La vigilancia es definida como tecnologías que observan o analizan los movimientos, comportamientos, o acciones de individuales identificables de una manera que razonablemente levanta inquietudes sobre libertades civiles, la libertad de expresión o asociación, igualdad racial o justicia social.”

- Los movimientos de la gente son observados a través de esta tecnología y puede que para algunas personas esto sea incómodo.
- Las cámaras de policía no califican como tecnologías de vigilancia en este tema.
- La presentación mostrada en la pantalla a través de los videos será transmitida en inglés.
- Se pidió que todos se traten con respeto y que opinen y que su nombre sea mencionado e incluso la vecindad donde viven.

El Grupo

Participante vino porque quiere obtener más información y dar su opinión. Es de Seattle.

Participante viene de Shoreline/Seattle para ver cuánto la tecnología entra afecta

Participante vino porque quiere saber qué información es colectada por el gobierno y para qué usan esa información. Puede que la información obtenida a través de la tecnología sea usada para perseguir a personas de color/minorías/personas marginadas.

Participante vino de First Hill, porque quiere ver el punto de vista de la ciudad y ver que opiniones surgirán.

Participante viene de Seatac porque tiene interés en el tema y porque la seguridad es importante y quiere saber a dónde llega la información.

Participante vine en Ravenna/Northgate, quiere ver que tan confiable es la tecnología y para qué es utilizada. Perjudicial o beneficial?

Participante vine en Seatac y vino porque es un tema muy interesante ya que se tiene que saber/mantener informado de lo que hacen los gobernantes.

Participante vino de Burien por la importancia del tema y la privacidad.

Presentador: La tecnología no es nueva. Ya está siendo usada. Y quieren saber el formato para que las futuras tecnologías tengan.

El video de Seattle Department of Transportation de Acyclica fue mostrado

Esta tecnología es un sensor que detecta el wifi. Es un sensor que detecta la tecnología wifi.

Seattle Metering Tool fue mostrada

Nadie del grupo sabe del tema más el presentador no hablará a fondo de esto para no influenciar opiniones.

Video de Fire Department's Computer Aided Dispatch fue mostrado

El 9-1-1 logging recorder video fue mostrado

Aclaración: Información impresa fue entregada explicando cada una de las tecnologías.

Video de Coplogic fue mostrado

El grupo no conocía que se puede reportar a la policía a través de su página/en línea.

El video de Seattle Police Computer Aided Dispatch fue mostrado

Esta tecnología es similar a la de los bomberos.

Se preguntó cuál video era de interés para analizar

Se acordó el análisis de Acyclica, Binoculares/Sensorlink, y Coplogic

Las Preguntas que sea harán serán las siguientes:

¿Qué piensan de este sistema de tecnología en específico y el motivo de usarla?
¿Cuál creen que sea el aporte de esta tecnología a la cuidad?
¿Qué preocupación les causa el uso que se le dará a este sistema?
¿Qué recomendarían a el grupo de políticos de la cuidad responsables de tomar las decisiones de implementar estas tecnologías?
¿Qué otra manera habría de resolver el problema que esta tecnología esta designada a resolver?

La Acyclica

Pregunta: ¿Qué piensan de este sistema de tecnología en específico y el motivo de usarla? (Como se usa y cuál es el uso)

- Bien, la tecnología ayuda con la velocidad o el movimiento de los coches.
- La información se guarda y analizan por donde viajas o cuantas veces cruzas este rastreo.
- Si es solo para ver el tráfico está bien.

- Está bien en algunas partes. Puede que sea algo bueno. Pero puede que esta tecnología pueda compartir información personal que puede ser utilizada de otra forma en especial si hay Hacking (forma negativa, uso de datos).

- La tecnología en sí no es tan grande (de tamaño) para ser algo visualmente desagradable. La información captada a través de estos medios puede que ayude a conducir el tráfico de mejor manera pero también puede que tome información personal.

Pregunta: Qué es lo que aporta esta tecnología a la ciudad?

- Seria algo bueno el aporte por la agilidad del tráfico solo si la tecnología está sincronizada con los semáforos, de otra manera no es útil si no aporta para el mejoramiento del tráfico.

- Participante dice que hay alternativas para esquivar el tráfico.

- Participante opina que la tecnología es interesante ya que usa google maps y está de acuerdo con el mejoramiento del tráfico.

- Si el objetivo es de mejorar el tráfico está de acuerdo. Pero también quiere saber en qué lugar(es) estarán los aparatos, si algunas personas serán beneficiadas más que otras.

Pregunta: Qué preocupaciones tienen con posible uso/uso potencial de esta tecnología?

- Le preocupa el uso de wifi en Acyclica porque pueden obtener toda la información de los teléfonos.

- Si el potencial puede ser aplicada a la inversión.

Enfocando al grupo: La tecnología ya está instalada, que les preocupa de su uso?

- El tráfico sigue igual.

- Quien usa o almacena la información.

- La preocupación es la colección de data.

Más de la mitad de grupo opina que esa (el almacén y colección de información) es la preocupación.

- Participante no está de acuerdo. No es la colección de data lo alarmante sino los recursos (dinero utilizado) ya que o la tecnología no están funcionando porque el tráfico

sigue igual. No hay cambio con la nueva tecnología, esos gastos no son válidos ya que no hay resultados. Esos gastos pudieran ser utilizados para la comunidad.

- También tienen que ver si la tecnología emite radiación o alguna otra cosa dañina; perjudicial a la salud.

- El gobierno tiene todos los datos.

- Opinión de otro participante: No necesitan esta tecnología para tener los datos porque ya existen métodos para eso, incluso aplicaciones o alguna otra cosa.

La otra preocupación del grupo es que no haya un cambio al problema que se quiere resolver. En el caso de Acrylica sería el mejorar el tráfico.

- Tecnologías como esta necesitan recolectar más opiniones de expertos.

- Sería bueno que la información sea compartida con la comunidad. (Transparencia en fines y objetivos de la tecnología y datos guardados, tácticas implementadas.)

Pregunta: Le dirían algo a los políticos algo del lugar donde se encuentran estos aparatos?

- Hay lugares donde no se necesitan. En algunas partes de Magnolia, Queen Anne, Northgate, no se ocupan.

Seguimiento de pregunta: En las comunidades donde viven los latinos que tanto se ocupa Acyclica?

- Participante no cree que allí se ocupan.

Hablaron sobre la necesitad de puntos estratégicos y calles con más necesidad de ayuda por causa del tráfico.

Presentrador: Crees que Acylica es como el router de google?

- La tecnología no es un router, sino colección de data para planeaciones urbanas.

- Participante: “quiero creer” “convencerme” que los sensores están allí para ayudar con el tráfico.

- No se sabe cuándo las instalaron, los resultados deberían de ser públicos. Si la tecnología es para aliviar el flujo de tráfico entonces por qué no extienden el programa? O por qué no hay mejoramiento del tráfico?

Otra pregunta: Alguna otra tecnología que pueda ser utilizada en vez de Acyclica?

Alternativas:

- Alguna pantalla que indique cuáles vías son alternativas puede reemplazar esto.
- Cambios al límite de velocidad puede que alivie el flujo del tráfico.
- Dejar de construir tanto.
- Rediseño de calles ayudaría flujo de tráfico.
- El rediseñar las vías servirá para las futuras generaciones.

Tecnologia #2

Sensorlink/Binoculares

Pregunta: Que opina el grupo de la tecnología?

- Los binoculares son preocupantes si la persona no tiene ética. Es preocupante que una persona vea a través de binoculares a que una tecnología mida el uso de la electricidad.

- Un sensor que detecta la electricidad sería mejor.

- Al grupo le incomoda el uso de binoculares.

Pregunta: Qué opinas sobre la tecnología medidora de electricidad (sensorlink) y que sea usada en tu casa?

- No le incomoda o afecta a dos participantes.

- La preocupación sería que le quita el trabajo a una persona.

- Los binoculares son invasivos.

- Para que usar binoculares si es que se puede llegar a el hogar y ver el medidor en persona, pidiendo permiso? Si la tecnología es usa para ver que las personas se roban la electricidad, creen que no saben quiénes roban?

- El grupo cree que si saben.

Pregunta: Cual creen que sea el aporte que esta tecnología?

- El video dice que 3 millones de dólares son ahorrados.

Pregunta: De qué manera beneficia esto a la cuidad/ciudadanos/comunidad?

- El robo de la luz es preocupante.
- Si ya llevan el record y datos y le hacen saber a la comunidad puede que ahorren dinero.
- Uso de binoculares puede dar trabajo a una persona y dinero puede ser ahorrado con esta tecnología.
- La tecnología trae gasto de electricidad para poder ver gastos de luz? Si pretende evitar el robo entonces los gastos de la factura eléctrica deberían de seguir estables.

Pregunta: La confianza en estos medidores serán confiables? Serán efectivos?

- Ayuda a la precisión, a bajar precios.
- Que quiten los binoculares sería una sugerencia, o usar binoculares que graban con video.
- Si ya tienen récord sobre la energía (consumo, gastos, etc.), el robo de energía no es suficiente para establecer este tipo de tecnología ya que puede ser identificado el robo o alguna otra anomalía dependiendo en el nivel alto o bajo o repentino analizado/visto/detectado por métodos convencionales ya establecidos.
- Otra recomendación: Usar background check, uso de uniforme por trabajadores, cámara en binoculares.
- Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad
- .La preocupación es que no tan solo será para leer la electricidad sino para obtener otros tipos de información si cámaras fueran usadas.

Tecnologia #3 Coplogic

- Esta tecnología no solo el ahorro de tiempo, sino el ahorro de tiempo policial ya que ellos trabajarían en otras cosas
- El uso de computadora está bien para las denuncias.
- Si personas usan esta tecnología y es analizada en tiempo real por otras personas no hay problema.

Enfoque: Lo que estamos queriendo dialogar es el uso del internet y las denuncias.

- Es otro método para denunciar
- Está de acuerdo con el uso de computadoras para denunciar solo que no todos son capaz de usar este método/tecnología.

Pregunta: En que ayuda a la comunidad?

- Por qué usar estos métodos?
- Grupo están de acuerdo con su uso.
- Puede salvar una vida.
- Los riesgos y acciones determinan la urgencia de la intermisión policiaca.
- Alguna gente se siente más capaz de acudir a través de este sistema la tecnología en uso tiene validez.
- Bueno para la violencia doméstica.
- Las fallas electrónicas son preocupantes especialmente en reportes policiacos.
- Las preocupaciones es que el reporte no salió, no llegó por cualquier razón.

- No todos podrán o saben usar las computadoras.
- Fallas de los algoritmos o cuando o que promueve urgencia de cada demanda es alarmante.
- Criterio de demandas y que clase de preocupación de parámetros son confiables tienen que ser cuestionados/analizados, y que/quien es digno de prioridad o importancia o de ayuda.

Pregunta: De qué manera este uso beneficiaria a la comunidad?

- Personas pueden ser discriminadas
- Las personas le temen a los policías. Y este medio puede ayudar a que el miedo disminuya.
- La computadora decidirá la importancia/urgencia del reporte/emergencia dando a llevar acciones de emergencia.

- Gravedad de emergencia determina uso de tecnología.

Pregunta: Alguna inquietud sobre el uso de esta tecnología?

- La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

Pregunta: En qué situación usarán esta tecnología?

- Una pelea en la calle, un malestar corporal, cuestiones de vida, abuso doméstico
- Cada uno tiene la definición de vigilancia, pero que tal la definición de emergencia?
- La definición de emergencia es diferente con cada persona.
- Si nos basamos en la definición de emergencia sólo en cuanto estemos en peligro inmediato o en tiempos mínimos/ de transcurrencia alarmante/peligrosa el uso de será implementado o limitado solo a instantes inmediatos de peligro

Pregunta: Para qué sirve el reporte de la computadora?

- Para reportar algo que ya sucedió o que son recurrentes.
- Basado en el concepto de emergencia, las personas pueden tomar el método adecuado para reportar su caso y a través del medio necesario.
- Los reportes no son anónimos.
- Los datos son recolectados aun, a pesar de la opción escogida.

Pregunta: Qué les recomendarían a los políticos?

- Que sea multi-idioma, implementar audio, implementar sistemas que ayuden a múltiples personas con diversas capacidades/necesidades

Pregunta: Algún otro comentario en general sobre la tecnología de vigilancia?

- Si es usada de manera adecuada y como han dicho está bien.

- El uso de la tecnología es bueno para dar respuesta para todas las cosas y personas.

Consejo:

- Den información más información sobre lo que están haciendo. (transparencia/divulgación de información)

- Que haya más transparencia.

Ser transparentes sobre la colección de datos, para que haya discusiones y decisiones

Informadas, en todas las tecnologías implementadas/por implementar.

Byrd Barr Place

2/28/2019 Surveillance Technology Focus Group

Thursday, February 28, 2019
1:42 PM

Disclaimer: some of these notes are written in first-person. These should not be considered direct quotes

Videos:

- Acyclica: sensors recognize when a wifi enabled device is in range of it. Attached to street lights
- 911 recorder: records the conversation with the person calling 911, and conversation with the dispatched officers
- CopLogic: Online police report, treated as a regular policy report
- Computer Aided Dispatch
- Seattle City Light: Binoculars for meter readers; sensor to see if someone is stealing electricity

Tom: Read definition of surveillance

Craig: invasion of privacy?

- Electric one: I never even know they had the sensor one.

Community Member: used to be in the tech industry for thirty years. Writing a book about surveillance and technology
Wanda: I like the online police report. If someone is experiencing a crisis or trauma, you can go ahead and report it.

- Surveillance, I understand the concern, but overall I think it's a good thing. There is good and bad in any location, you'll find people who are taking advantage of it, but hopefully there are systems in place.
- Used to work nights, and catching the bus at night is scary. Having the cameras and police out when catching the bus helps, I appreciate that. No one likes to be watched, but if it's gonna keep people safe, that's a good thing.

Mercy: security is a great safety issue
Craig: there are some parts of the neighborhood/city that need to be watched, and some that need to be left alone
Wanda: as long as it's even
Craig: Sometimes it's not even
Both: There are hot spots though

Which of the surveillance technologies do you think could be abused to pinpoint specific communities?

IG: The Computer Aided Dispatch

Talking about the International District:

- Lots of businesses and residential crammed together in a larger space
- Talking about a great community member who died; if they had surveillance technology them, maybe they would have found his killer

"Some neighborhoods need to be watched"
- Gangs; drug use

Tom: getting back to CAD, how do we feel about the information that is stored
- Craig: there are concerns, but who is allowed to see it, how is it stored? That's a concern
    - Is it used for BOLOs? Is it everyone who is in the area, all of the police officers? Or is there some discretion as to which police officers would be given the information?
- Wanda: plenty of people are arrested who "fit a description"
    - Discussion about the racial discrimination: how people who think that "all [insert race here] look alike".
    - Individuals may think like that, but police officers have the capability to ruin someone's life.
- Marjorie: just recently got a smart phone, and it's new to me that someone could know where I'm going and I wouldn't be aware of it
    - Without my consent.
- Mercy: grew up with the idea that big brother is watching you
    - Tracking how many times I go to the library seems like a waste of money
    - People who are not law abiding citizens, they are the ones to be worried
- Craig: What about selling weed, coke, etc. Should they be worried?
    - Mercy: well at least in Seattle, it's ok to sell
- Mercy: big brother is watching. We already know that, it's just more obvious now
- There is a lot of technology that we are not made aware of

Tom: So acyclica, is it worth it? Some people worried it's tracking, is it something that we can live without?
- Should we put up signs that this road is tracked?
    - Viron: Maybe
    - Mercy: let people out there know that you're on camera.
    - Viron: does it work if your device is not turned on?

Tom: what do you want to tell the city council about tech that is collecting personal information?
- Wanda: they should get our individual consent
- Martha: putting it on the ballot doesn't mean that you are getting individual consent, because if you vote no but it still passes, you didn't give your consent
- Deana: there are some places around Capitol Hill that I don't feel safe at at night
    - Talking about fire department responding to a fire in her building: when one building alarm system goes off, it goes directly to the fire department - affects multiple buildings.
        - Response time is very good.

    - I choose to turn off the GPS tracking, because I don't need people to know where I'm at
        - If others are watching where I'm at, that's an invasion of privacy. I should be able to walk out my front door and go wherever I want without anyone knowing.
- Location privacy: you can tell a lot about a person based on where they go, and tracking that can build a pretty extensive profile of who you are
- IG: now that I know they are tracking, I will turn it off.

Mr. Surveillance: Surveillance is always secret, and it's an aggressive act. It's meant to exert power over others.

Do you think any individual could raise enough concern that it would change anything?

- Resounding no
- Maybe with a larger group
    - Maybe with the whole city

SCL binoculars:

- Craig: they should warn their customers and let them know they are coming into their yard/looking through binoculars.
- Wanda: as long as they aren't looking in people's windows.
    - When we're walking down the street, it's a little different. Certain neighborhoods do need more surveillance than others

Regarding being watched in public:

- Eydie: in public, it depends on how long. If it's a short period of time, that's one thing, but if you're tracked the whole time you're out, it's unreasonable.
    - I don't know what the solutions would be.
    - Even when the meter read just walks into your yard, it's unnerving.
    - What’s the purpose of tracking it this way?
- Mercy: (referring to the acyclica) Why are they doing it all the time? Have they not gotten the information yet?
    - They should already know what the traffic flow would be.
    - We lost a lane to the bicyclist
- Craig: facial recognition used on the street is bad.
- Vyron: sometimes you can't walk down the street and shake someone's hand without getting in trouble
- Mr. Surveillance: The technology has gotten ahead of the law, and it means they have to pay less people

Tom: Are we willing to accept more technology to have less police?

- Craig: how about just making it even? Police have an image to people of color; they are afraid of why they are going to be there. We can police ourselves

- Wanda: I disagree. There are some who think there should be less, but there are also a lot of people who worry about walking down the street
    - As a woman and DV survivor, I appreciate the police and appreciate living in a country where I can call a number for help.
    - I have a big problem with the shooting of unarmed black men, but as an individual I still appreciate the police.
    - But I have a problem being tracked, and I have a problem being watched in my home.
- General comment: The number of police being on the corner is a touchy situation
    - Knowing the police that are on your corner makes a difference. They can police the community better if there is more of a relationship between the two.
- Craig: it has to be both, even. You can't trade off the technology for the police.
- Mr. Surveillance: The trend is they want to go to more technology and less police.

Tom: If right now we have lots of technology, and we want a balance, then how do we do that?

- Craig: keep it the way it is but clean up the police department. Make sure the people who are working there are good at their jobs, not biased or discriminating

CopLogic: making police reports online

- Craig: I think it's stupid.
    - Would use that technology for stupid crimes
- Mercy: you could report your neighbor for silly things
    - Anonymous reporting of crimes that could target people for things they might not call 911 for
- Wanda: there were some lines of traffic where I saw cars lined up with their windows smashed in; nothing taken, but glass all over the place.
    - Police response when called: maybe you should get a cheaper type of car
    - Would he have said that to us if we were a different skin color, or lived in a different neighborhood?
- IG: I think it's a bad thing: someone could make up a story and the officer didn’t have to check it.
- Marjorie: I think the online reporting could be abused

City of Seattle

Appendix E: All Comments Received from Members of the Public

ID: 10617659831
Submitted Through: Survey Monkey
Date: 3/25/2019 1:18:11 PM
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SPD: Computer-Aided Dispatch (CAD)
What concerns, if any, do you have about the use of this technology?
Concerns: 1) Accidental release of personal information of citizens via PRA requests. However, per the SPD rep at the SIR tech fair, SPD redacts names, addresses, phone numbers, building access codes, etc. as a matter of practice when responding to PRA requests, so the likelihood of release seems low here. 2) No 2-step-verification/2-factor-authentication (2SV/2FA) for login to Versaterm vCAD; however, an individual would need to first logon to an SPD workstation and then login to vCAD. That being said, page 14 of the SIR implies that 2FA is in place.
What value, if any, do you see in the use of this technology?
It meets a functional need that likely is more accurate and efficient than a paper-based workflow.
What do you want City leadership to consider about the use of this technology?
The draft SIR did not specify what (if any) other vendors SPD/IT considered before deploying Versaterm vCAD. Is this the optimal CAD solution for the City of Seattle? Is there perhaps another CAD software provider that is more competitive and perhaps has better security/privacy/audit features?
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

ID: 10617346709
Submitted Through: Survey Monkey
Date: 3/25/2019 11:16:33 AM
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SPD: Computer-Aided Dispatch (CAD)
What concerns, if any, do you have about the use of this technology?
None at all
What value, if any, do you see in the use of this technology?
Gets help where it's most needed faster.
What do you want City leadership to consider about the use of this technology?
Allow it.
Do you have any other comments?
I can't believe this is even an issue.
Are there any questions you have, or areas you would like clarification?
Don't you have better things to do with your time and our money?

ID: 4
Submitted Through: Focus Group
Date: 2/27/2019
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SPD: CAD
What concerns, if any, do you have about the use of this technology?
Dispatching softwares should have "detail options" on language callers speak that may be different than English
What value, if any, do you see in the use of this technology?
convenience and effective and accountable
What do you want City leadership to consider about the use of this technology?
allow enough trial times - testing times- before applying
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?
Again, how to keep data safe

ID: 3
Submitted Through: Focus Group
Date: 2/27/2019
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SCL: Binoculars, SCL: CheckMeter, SCL: AmpFork, SFD: CAD, SPD: CAD, SPD: 911 Logging Recorder
What concerns, if any, do you have about the use of this technology?
That would be good with advanced technology
What value, if any, do you see in the use of this technology?
Yes, around the city.
What do you want City leadership to consider about the use of this technology?
Need good train to people who use new technologies
Do you have any other comments?
Are there any questions you have, or areas you would like clarification?

ID: 10529127076
Submitted Through: Survey Monkey
Date: 2/13/2019
Which surveillance technology that is currently open for public comment, do you wish to comment on?
SPD: CAD
What concerns, if any, do you have about the use of this technology?
Why isn't Geotime and Maltego on this list? This is what I have the most concern about.
What value, if any, do you see in the use of this technology?
Geotime and Maltego - I want to know where it get it's data and how it's collected.
What do you want City leadership to consider about the use of this technology?
Geotime should NOT exist
Do you have any other comments?
Why don't you have Maltego and Geotime. I think the public should know more about this technology and how it's used. Disregard question 1
Are there any questions you have, or areas you would like clarification?
Maltego and Geotime. -- Disregard question 1

Appendix F: Department Responses to Public Inquiries

Community Comment Responses:

FG	2/27/2019	SPD: CAD	How do we keep the data safe?

Only authorized SPD users can access the system, technology, or the data. Access to the application is limited to SPD personnel via password-protected login credentials. All activity within CAD (including timeline of commands issued) generates a log that is auditable. The entire system is located on the SPD network that is protect by industry standard firewalls and is CJIS compliant.

FOLS FG	2/27/2019	SPD: CAD	Who is allowed to see the information that is stored in CAD?

The information in CAD is accessible only by CJIS certified personnel who have been granted access by SPD with unique usernames and passwords. No person, outside of SPD and Seattle IT, has direct access to CAD or the data stored in the CAD system. Data may be shared with outside entities in connection with criminal prosecutions. Data may also be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester.

FOLS FG	2/27/2019	SPD: CAD	Is it used for BOLOs? Is it everyone who is in the area, all of the police officers? Or is there some discretion as to which police officers would be given the information?

BOLOs are distributed to SPD officers through a variety of methods including, radio broadcasts, CAD notifications, emails, and SPD cell phones. Officers who are on duty and logged in to the CAD system receive active BOLO notifications through the CAD system.

Appendix G: Letters from Organizations or Commissions

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

March 12th, 2019

Seattle City Council
600 4th Ave
Seattle, WA 98104

Re: Surveillance Ordinance Group 2 Public Comment

We would like to first thank City Council for passing one of the strongest surveillance technology policies in the country, and thank Seattle IT for facilitating this public review process.

These public comments were prepared by volunteers from the Community Technology Advisory Board (CTAB) Privacy & Cybersecurity Committee, as part of the surveillance technology review defined in Ordinance 125376. These volunteers range from published authors, to members of the Seattle Privacy Coalition, to industry experts with decades of experience in the information security and privacy sectors.

We reviewed and discussed the Group 2 Surveillance Impact Reports (SIRs) with a specific emphasis on privacy policy, access control, and data retention. Some recurring themes emerged, however, that we believe will benefit the City as a whole, independent of any specific technology:

- **Interdepartmental sharing of privacy best practices**: When we share what we've learned with each other, the overall health of the privacy ecosystem goes up.
- **Regular external security audits**: Coordinated by ITD (Seattle IT), routine third-party security audits are invaluable for both hosted-service vendors and on-premises systems.
- **Mergers and acquisitions**: These large, sometimes billion-dollar ownership changes introduce uncertainty. Any time a vendor, especially one with a hosted service, changes ownership, a thorough review of any privacy policy or contractual changes should be reviewed.
- **Remaining a Welcoming City**: As part of the Welcoming Cities Resolution, no department should comply with a request for information from Immigration and Customs Enforcement (ICE) without a criminal warrant. In addition, the privacy of all citizens should be protected equally and without consideration of their immigration status.

Sincerely,

Privacy & Cybersecurity Committee volunteers
Torgie Madison, Co-Chair
Smriti Chandashekar, Co-Chair
Camille Malonzo
Sean McLellan
Kevin Orme
Chris Prosser
Rabecca Rocha
Adam Shostack
T.J. Telan

Community Technology Advisory Board
Steven Maheshwary, CTAB Chair
Charlotte Lunday, CTAB Co-Vice Chair
Torgie Madison, CTAB Co-Vice Chair
Smriti Chandashekar, CTAB Member
Mark DeLoura, CTAB Member
John Krull, CTAB Member
Karia Wong, CTAB Member

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SFD: Computer-Aided Dispatch (CAD)

Comments

The use of a centralized Computer-Aided Dispatch (CAD) system is essential to protecting the health and safety for all Seattle citizens. The National Fire Protection Association (NFPA) standards outline specific alarm answering, turnout, and arrival times[1] that could only be accomplished in a city of this size with a CAD system.

In addition, with over 96,000 SFD responses per year (2017)[2], only a computerized system could meet the state's response reporting guidelines established in RCW 35A.92.030[3].

CentralSquare provides the dispatch service used by SFD. CentralSquare is a new entity resulting from the merger of Superion, TriTech, Zuercher, and Aptean[4] in September 2018.

Recommendations

- Tritech, the underlying technology supplying SFD with CAD services, has been in use since 2003 [SIR 4.3], making it 16 years old. As with any technology, advancements in security, speed, usefulness, and reliability come swiftly. Due to the age of the technology, we recommend conducting a survey into the plausibility of replacing Tritech as SFD's CAD solution.

- Tritech was merged very recently into CentralSquare in one of the largest-ever government technology mergers to date. Due diligence should be exercised to ensure that this vendor is keeping up to date with industry best practices for security and data protection, and that their privacy policies are still satisfactory after the CentralSquare merger. We recommend ensuring that the original contracts and privacy policies have remained unchanged as a result of this merger.

---

[1] "NFPA Standard 1710." https://services.prod.iaff.org/ContentFile/Get/30541
[2] "2017 annual report - Seattle.gov." https://www.seattle.gov/Documents/Departments/Fire/FINAL%20Annual%20Report_2017.pdf
[3] "RCW 35A.92.030: Policy statement—Service ... - Access WA.gov." https://app.leg.wa.gov/rcw/default.aspx?cite=35A.92.030
[4] "Superion, TriTech, Zuercher, and Aptean's Public Sector Business to " 5 Sep. 2018, https://www.tritech.com/news/superion-tritech-zuercher-and-apteans-public-sector-business-to-form-centr a

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SDOT: Acyclica

Comments

Traffic congestion is an increasingly major issue for our city. Seattle is the fastest-growing major city in the US this decade, at 18.7% growth, or 114,00 new residents[5]. Seattle ranks sixth in the nation for traffic congestion[6]. The need for intelligent traffic shaping and development has never been greater. Acyclica, a service provided by Western Systems and now owned by FLIR[7], is an implementation of surveillance technology specifically designed to address this problem.

We were happy to see the 2015 independent audit of Acyclica's systems [SIR 8.2]. This is an excellent industry best practice, and one that we'll be recommending to other departments throughout this document.

In addition, we are pleased to see the hashing function's salt value rotated every 24-hours [SIR 4.10]. This ensures that even the 10-year retention policy [SIR 5.2] cannot be abused to correlate multiple commute sessions and individually identify a person.

Recommendations

- FLIR Systems' acquisition of Acyclica is a recent development (September 2018). We recommend verifying that the Western Systems terms [SIR 3.1] still apply. If they have been superseded by new terms from FLIR Systems, those should be subject to an audit by SDOT and Seattle IT. Specifically, section 2.5.1 of Western Systems' terms must still apply:

  > 2.5.1. It is the understanding of the City that the data gathered are encrypted to fully eliminate the possibility of identifying individuals or vehicles. In no event shall City or Western Systems and its subcontractors make any use of the data gathered by the devices for any purpose that would identify the individuals or vehicles included in the data.

- FLIR Systems is known primarily as an infrared technology vendor. Special care should be taken if FLIR/Acyclica attempt to couple IR scanning with WiFi/MAC sniffing. Implementation of an IR system would necessitate a new public surveillance review.

---

[5] "114,000 more people: Seattle now decade's fastest-growing big city in ...." 24 May. 2018, https://www.seattletimes.com/seattle-news/data/114000-more-people-seattle-now-this-decades-fastest-growing-big-city-in-all-of-united-states/
[6] "INRIX Global Traffic Scorecard." http://inrix.com/scorecard/
[7] "FLIR Systems Acquires Acyclica | FLIR Systems, Inc.." 11 Sep. 2018, http://investors.flir.com/news-releases/news-release-details/flir-systems-acquires-acyclica

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SCL: Binoculars, Check Meter, SensorLink

Comments

As these three technologies are serving the same team and mission objectives, we will review them here in a combined section.

The mission of the Current Diversion Team (CDT) is to investigate and gather evidence of illegal activity related to the redirection and consumption of electricity without paying for its use. As such, none of these technologies surveil the public at large. They instead target specific locations and equipment, albeit without the associated customer's knowledge.

It appears as though all data collected through the Check Meter Device and SensorLink Amp Fork are done without relying on a third-party service, so the usual scrutiny of a vendor's privacy policies does not apply.

Recommendations

- **Binoculars**: We have no recommendations for the use of binoculars.
- **Check Meter Device & SensorLink Amp Fork**: As noted in the comments above, we have no further recommendations for the use of the Check Meter Device and SensorLink Amp Fork technologies.
- **Racial Equity**: As with any city-wide monitoring practice, it can be easy to more closely scrutinize one neighborhood over another. Current diversion may be equally illegal (and equally prevalent) across the city, but the enforcement of this law may be unevenly applied. This could introduce racial bias by disproportionately burdening specific neighborhoods with a higher level of surveillance.

  As described, DPP 500 P III-416 section 5.2[8] asserts that all customers shall receive uniform consideration [SIR RET 1.7]. To ensure this policy is respected, we encourage City Light to track and routinely review the neighborhoods where CDT performs investigations, with a specific emphasis on racial equity. This information should be made publicly available.

  When asked at the February 27th Surveillance Technology public meeting, SDOT indicated that no tracking is currently being done on where current diversion is enforced.

[8] "SCL DPP 500 P III-416 Current Diversion - Seattle.gov." 11 Jan. 2012, http://www.seattle.gov/light/policies/docs/III-416%20Current%20Diversion.pdf

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: 911 Logging Recorder

Comments

This is a technology that the general public would likely already assume is in place. Some of the more sensational 911 call logs have been, for example, played routinely on the news around the country. Since it would not alarm the public to know that 911 call recording is taking place, our recommendations will focus primarily on data use, retention, and access control.

Call logging services are provided by NICE Ltd., an Israeli company founded in 1986. This vendor has had a troubling history with data breaches. For example, a severe vulnerability discovered in 2014 allowed unauthorized users full access to a NICE customer's databases and audio recordings[9]. Again, in 2017, a NICE-owned server was set up with public permissions, exposing phone numbers, names, and PINs of 6 million Verizon customers[10].

Recommendations

- SIR Appendix K includes a CJIS audit performed in 2017. SIR section 4.10 also mentions that ITD (Seattle IT) periodically performs routine monitoring of the SPD systems.

  However, given the problematic history with the quality of the technology vendor, if any of the NICE servers, networks, or applications were installed by the vendor (or installation was overseen/advised by the vendor), we recommend an external audit of the implementation of the call logging technology.

- SIR sections 3.3 and 4.2 outline the SPD-mandated access control and data retention policies, however it is not apparent if there is a policy that strictly locks down the use of this technology to a well-defined list of allowed cases. We recommend formally documenting the allowed 911 Logging use cases, and creating a new SIR for any new desired applications of this technology.

  With a 90-day retention policy [SIR 4.2], and with SPD receiving 900,000 calls per year[11], there are about 220,000 audio recordings existing at any given time. This is enough for a data mining, machine learning, or voice recognition project.

---

[9] "Backdoor in Call Monitoring, Surveillance Gear — Krebs on Security." 28 May. 2014, https://krebsonsecurity.com/2014/05/backdoor-in-call-monitoring-surveillance-gear/
[10] "Nice Systems exposes 14 million Verizon customers on open AWS ...." 12 Jul. 2017, https://www.techspot.com/news/70106-nice-systems-exposes-14-million-verizon-customers-open.html
[11] "9-1-1 Center - Police | seattle.gov." https://www.seattle.gov/police/about-us/about-policing/9-1-1-center

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: Computer-Aided Dispatch (CAD)

Comments

As mentioned in the section "SFD: Computer-Aided Dispatch (CAD)" and the section "SPD: 911 Logging Recorder", these dispatch technologies are mandatory for functional emergency services of a city this size. No other system would be able to meet the federal- and state-mandated response times and reporting requirements.

SIR section 4.10 mentions that ITD (Seattle IT) performs routine inspections of the Versaterm implementation.

Versaterm, founded in 1977, provides the technology used by SPD's CAD system. SPD purchased this technology in 2004. In September of 2016, there was a legal dispute between Versaterm and the City of Seattle over a Public Records Act (PRA) disclosure of certain training and operating manuals[12]. The court ruled in favor of Versaterm.

Recommendations

- It is not immediately clear what use cases are described in SIR 2.5 describing data access by "other civilian staff whose business needs require access to this data". All partnerships and data flows between SPD and businesses should be explicitly disclosed.

- This system has been in place for 15 years. As with any technology, advancements in security, speed, usefulness, and reliability come swiftly. Due to the age of the technology, and the potential damaged relationship between Seattle and Versaterm due to the aforementioned legal dispute, we recommend conducting a survey into the plausibility of replacing Versaterm as SPD's CAD solution.

- As mentioned in the introduction to this document, Seattle has adopted the Welcoming Cities Resolution[13]. In honoring this resolution, we recommend that SPD never disclose identifying information, from CAD or any system, to Immigrations and Customs Enforcement (ICE) without a criminal warrant.

[12] "Versaterm Inc. v. City of Seattle, CASE NO. C16-1217JLR | Casetext." 13 Sep. 2016, https://casetext.com/case/versaterm-inc-v-city-of-seattle-2
[13] "Welcoming Cities Resolution - Council | seattle.gov." http://www.seattle.gov/council/issues/past-issues/welcoming-cities-resolution

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: CopLogic

Comments

Track 1 - Public reporting of no-suspect, no-evidence, non-emergency crimes

CTAB understands that in cases where no evidence or suspect is available, a crime should be reported (for statistical or insurance purposes) but does not require the physical appearance of an SPD officer.

Track 2 - Retail Loss Prevention

This track is more problematic, as it could be used by retailers as a method to unreasonably detain, intimidate, or invade the privacy of a member of the public accused of, but not proven guilty of, shoplifting.

Recommendations

- **Track 2**: If not already done, retailers should be trained and informed that having a CopLogic login does not allow them to act as if they are law enforcement officers. Members of the public suspected of shoplifting need to have an accurate description of their rights in order to make informed decisions before providing identifying information. Retailers are also held to a lower standard than SPD regarding racial bias. It is virtually guaranteed that people of color are disproportionately apprehended and entered into the retail track of CopLogic.

  We recommend discontinuing Track 2 entirely.

- **Track 1 & 2**: If not already done, SPD, in coordination with Seattle IT, should perform or hire a company to perform an audit of the vendor's systems. If this audit has not been performed in the 8 years since purchasing this system, it should absolutely be done before the 10-year mark in 2020.
- **Track 1 & 2**: It is not immediately clear in the SIR or LexisNexis's Privacy Policy what CopLogic does with these records long-term, after SPD has imported them into their on-premises system. A written statement from LexisNexis on how this data is used, mined, or sold to affiliates/partners should be acquired by SPD.
- **Track 1 & 2**: We recommend migrating CopLogic to an on-premises solution. We found the LexisNexis privacy policy to be obfuscated and vague[14]. Such sensitive information should not be protected by trust alone.

[14] "Privacy Policy | LexisNexis." 7 May. 2018, https://www.lexisnexis.com/en-us/terms/privacy-policy.page

City of Seattle

March 20, 2019

RE: ACLU-WA Comments Regarding Group 2 Surveillance Technologies

Dear Seattle IT:

On behalf of the ACLU of Washington, I write to offer our comments on the surveillance technologies included in Group 2 of the Seattle Surveillance Ordinance process. We are submitting these comments by mail and electronically because they do not conform to the specific format of the online comment form provided on the CTO's website, and because the technologies form groups in which some comments apply to multiple technologies.

These comments should be considered preliminary, given that the Surveillance Impact Reports (SIR) for each technology leave a number of significant questions unanswered. Specific unanswered questions for each technology are noted in the comments relating to that technology, and it is our hope that those questions will be answered in the updated SIR provided to the Community Surveillance Working Group and to the City Council prior to their review of that technology. In addition to the SIR, our comments are also based on independent research relating to the technology at hand.

The 8 technologies in Group 2 are covered in the following order.

I. Acyclica (SDOT)

II. CopLogic (SPD)

III. Computer-Aided Dispatch & 911 Logging Recorder Group

1. Computer-Aided Dispatch (SPD)
2. Computer-Aided Dispatch (SFD)
3. 911 Logging Recorder (SPD)

IV. Current Diversion Technology Group

1. Check Meter Device (Seattle City Light)
2. SensorLink Amp Fork (Seattle City Light)
3. Binoculars/Spotting Scope (Seattle City Light)

ACLU
AMERICAN CIVIL LIBERTIES UNION
Washington

901 Fifth Ave, Suite #630
Seattle, WA 98164
(206) 624-2184
aclu-wa.org

Tana Lin
Board President

Michele Storms
Executive Director

Shankar Narayan
Technology & Liberty Project Director

I. Acyclica - SDOT

Background

Acyclica technology is a powerful location-tracking technology that raises a number of civil liberties concerns because of its ability to uniquely identify individuals and their daily movements. Acyclica (via its hardware vendor, Western Systems), manufactures Intelligent Transportation System (ITS) sensors called RoadTrend that are used by the Seattle Department of Transportation for the stated purpose of traffic management. These RoadTrend sensors collect encrypted media access control (MAC) addresses, which are transmitted by any Wi-Fi enabled device including phones, cameras, laptops, and vehicles. Collection of MAC addresses, even when hashed (a method of de-identifying data irreversibly),[1] can present locational privacy challenges.

Experts analyzing a dataset of 1.5 million individuals found that just knowing four points of approximate spaces and times that individuals were near cell antennas or made a call were enough to uniquely identify 95% of individuals.[2] In the case of Acyclica's operation in Seattle, the dataset is comprised of MAC addresses recorded on at least 301 intersections,[3] which allows Acyclica to generate even more precise location information about individuals. Not only do the RoadTrend sensors pick up the MAC addresses of vehicle drivers and riders, but these sensors can also pick up the MAC addresses of all nearby individuals, including pedestrians, bicyclists, and people in close structures (e.g., apartments, offices, and hospitals). Acyclica technology's location tracking capabilities means that SDOT's use of Acyclica can not only uniquely identify individuals with ease, but can also create a detailed map of their movements. This raises privacy concerns for Seattle residents, who may be tracked without their consent by this technology while going about their daily lives.

These location-tracking concerns are exacerbated by the lack of clarity around whether SDOT has a contract with Acyclica (see below). Without a contract, data ownership and scope of data sharing and repurposing by Acyclica is unclear. For example, without contractual restrictions, Acyclica

[1] Hashing is a one-way function that scrambles plain text to produce a unique message digest. Unlike encryption—which is a two-way function, allowing for decryption—what is hashed cannot be un-hashed. However, hashed location data can still be used to uniquely identify individuals. While it is infeasible to compute an input given only its hash output, pre-computing a table of hashes is possible. These types of tables consisting of pre-computed hashes and their inputs are called rainbow tables. With a rainbow table, if an entity has a hash, then they only need to look up that hash in their table to then know what the original MAC address was.
[2] Montjoye, Y., Hidalgo, C., Verleysen, M., and Blondel, V. 2013. Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports.* 3:1375.
[3] The SIR states that SDOT has 301 Acyclica units installed throughout the City. However, an attached location excel sheet in Section 2.1 lists 389 Acyclica units, but only specifies 300 locations.

would be able to share the raw data (i.e., the non-aggregated, hashed data before it is summarized and sent to SDOT) with any third parties, and these third parties would be able to use the data in any way they see fit, including combining the data with additional data such as license plate reader or facial recognition data. Acyclica could also share the data with law enforcement agencies that may repurpose the data, as has happened with other City data. For example, in 2018, U.S. Immigration and Customs Enforcement (ICE) approached Seattle City Light with an administrative subpoena demanding information on a particular customer location, including phone numbers and information on related accounts.[4] ICE also now has agency-wide access to a nationwide network of license plate readers controlled by Vigilant Solutions,[5] indicating the agency may seek additional location data for immigration enforcement purposes in the future. Data collected via Acyclica should never be used for law enforcement purposes.

The uncertainty around the presence or absence of a contract contributes to two key issues: (1) lack of a clearly defined purpose of use of Acyclica technology; and (2) lack of clear restrictions on the use of Acyclica technology that track that purpose. With no contract, SDOT cannot enforce policies restricting the use of Acyclica technology to the intended purpose.

There are also a number of contradictory statements in the SIR concerning the operation of Acyclica technology,[6] as well as discrepancies between the SIR, the information shared at the technology fair (the first public meeting to discuss the Group 2 technologies),[7] and ACLU-WA's conversation with the President of Acyclica, Daniel Benhammou. All these leave us with concerns over whether SDOT fully understands (and the SIR reflects) the capabilities of the technology. In addition, there remain a number of critical unanswered questions that the final SIR must address (set forth below).

Of additional concern is the recent acquisition of Acyclica by FLIR Systems, an infrared and thermal imaging company funded by the U.S. Department of Defense.[8] As of March 2019, FLIR has discontinued Acyclica RoadTrend sensors.[9] Neither the implications of the FLIR acquisition nor the discontinuation of the RoadTrend sensors are mentioned in the SIR—but if the sensors used will change, the SIR should make clear how that will impact the technology.

a. Specific Concerns

- *Inadequate Policies Defining Purpose of Use.* Policies cited in the SIR are vague,

[4] https://crosscut.com/2018/02/immigration-officials-subpoena-city-light-customer-info
[5] https://www.theverge.com/2018/3/1/17067188/ice-license-plate-data-california-vigilant-solutions-alpr-sanctuary
[6] Explained in further detail in 1. Acyclica – SDOT *Major Concerns* below.
[7] http://www.seattle.gov/tech/initiatives/privacy/events-calendar#/?i=3
[8] https://www.crunchbase.com/acquisition/flir-systems-acquires-acyclica--e6043a1a#section-overview
[9] https://www.flir.com/support/products/roadtrend#Specifications

short, and impose no meaningful restrictions on the purposes for which Acyclica devices may be used.[10] Section 1.1 of the abstract set forth in the SIR states that Acyclica is used by over 50 agencies to "to help to monitor and improve traffic congestion." Section 2.1 is similarly vague, providing what appear to be examples of some types of information the technology produces (e.g., calculated average speeds) in order to facilitate outcomes (correcting traffic signal timing, providing information to travelers about expected delays, and allowing SDOT to meet traffic records and reporting requirements)—but it's not clear this list is exhaustive. Section 2.1 fails to describe the purpose of use, all the types of information Acyclica provides, and all the types of work that Acyclica technology facilitates. All these must be clarified.

- *Lack of Clarity on Whether Acyclica and SDOT have a Written Contract.* The SIR does not state that any contract exists, and in the 2018 conversation ACLU-WA had with Benhammou, he stated that there was no contract between the two parties. However, at the 2019 technology fair, the SDOT representative affirmatively stated that SDOT has a contract with Acyclica. As previously mentioned, the lack of a contract limits SDOT's ability to restrict the scope of data sharing and repurposing. The only contractual document provided appears to be a terms sheet in Section 3.0 detailing SDOT's terms of service with Western Systems (the hardware vendor that manufactures the Acyclica RoadTrend sensors), which states that Western Systems only deals with the maintenance and replacement of the hardware used to gather the data, and not the data itself.

- *Lack of Clarity on Data Ownership.* At the technology fair, the SDOT representative stated that SDOT owns all the data collected (including the raw data), but the SIR only states that the aggregated traffic data is owned by SDOT. In the 2018 conversation, Benhammou stated that Acyclica owns all the raw data. There is an apparent lack of clarity between SDOT and Acyclica concerning ownership of data that must be addressed.

- *Data Retention Periods are Unclear.* Section 5.2 of the SIR states that there is a 10-year internal deletion requirement for the aggregated traffic data owned by SDOT, but pg. 37 of the SIR states that "the data is deleted within 24 hours to prevent tracking devices over time." In the 2018 interview, Benhammou stated that Acyclica retains all non-aggregated data indefinitely. It is unclear whether the different retention periods stated in the SIR are referring to different types of data. The lack of clarity on data retention periods also relates to the lack of clarity on data ownership given that data retention periods may depend on data ownership.

[10] As noted in 1. Acyclica – SDOT *Background* above.

- *Inaccurate Descriptions of Anonymization/Data Security Practices.* The SIR appears to use the terms "encryption" and "hashing" interchangeably in some parts of the SIR, making it difficult to clearly understand Acyclica's practices in this area. For example, Section 7.2 states: "Contractually, Acyclica guarantees that the data gathered is encrypted to fully eliminate the possibility of identifying individuals or vehicles." But by design, encryption allows for decryption with a key, meaning anyone with that key and access to the data can identify individuals. (Also, if there is no contract between SDOT and Acyclica, the use of 'contractually' is misleading). This language is also used in the terms sheet detailing SDOT's contract with Western Systems (in Section 2.5.1 in the embedded contract). The SIR compounds this confusion with additional contradictory statements. For example, the SIR states in multiple sections that the data collected by the RoadTrend sensors are encrypted and hashed on the actual sensor. However, according to a letter from Benhammou provided by SDOT representatives at the technology fair,[11] the data is never hashed on the sensor—the data is only hashed after being transmitted to Acyclica's cloud server. These contradictory descriptions cause concern.

- *No Restrictions on Non-City Data Use.* Section 6.3 of the SIR states that there are no restrictions on non-City data use. However, there are no policies cited making clear the criteria for such use, any inter-agency agreements governing sharing of Acyclica data with non-City parties, or why the data must be shared in the first place.

- *Not All Locations of Acyclica Devices are Specified.* Section 2.1 of the SIR states that there are 301 Acyclica locations in Seattle. However, in the embedded excel sheet detailing the serial numbers and specific intersections in which Acyclica devices are installed, there are 389 serial numbers, but only 300 addresses/locations specified. The total number and the locations of Acyclica devices collecting data in Seattle is unclear. This gives rise to the concern that there are unspecified locations in which Acyclica devices are collecting MAC addresses.

- *No Mention of RoadTrend Sensor Discontinuation.* As noted in the background,[12] Acyclica has been acquired by FLIR, an infrared and thermal imaging company. As of March 2019, FLIR's product webpage states that the Acyclica RoadTrend sensors (those currently used by SDOT) have been discontinued.[13] From the information we have, it is unclear if SDOT will be able to continue using the RoadTrend sensors described in the 2019 SIR. Given that FLIR sensors, such as the TrafiOne, have capabilities that go much farther than those of the

[11] Included in Appendix 1.
[12] As noted in 1. Acyclica – SDOT *Background* above.
[13] https://www.flir.com/support/products/roadtrend#Specifications

RoadTrend sensors (e.g., camera technology and thermal imaging)[14] as well as potentially different technical implementations, their use would give rise to even more serious privacy and misuse concerns. Neither the implications of the FLIR acquisition nor the discontinuation of the RoadTrend sensors are mentioned in the SIR.

- *No Mention of Protecting MAC Addresses of Non-Drivers/Riders (e.g., people in nearby buildings).* The Acyclica sensors will pick up the MAC addresses of all nearby individuals, regardless of whether they are or are not driving or riding in a vehicle. The SIR does not mention any steps taken to reduce the privacy infringements on non-drivers/riders.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- For what specific purpose or purposes will Acyclica be used, and what policies state this?
- Does SDOT have a contract with Acyclica, and if so, why is the contract not included in the SIR?
- Who owns the raw, non-aggregated data collected by Acyclica devices?
- What is the retention period for the different types of collected data (aggregated and non-aggregated)—for both SDOT and Acyclica?
- Provide accurate descriptions of Acyclica's data security practices, including encryption and hashing, consistent with the letter from Daniel Benhammou, including any additional practices that prevent reidentification.
- What third parties will access Acyclica's data, for what purpose, and under what conditions?
- Why are 89 locations not specified in the embedded Acyclica locations sheet in Section 2.1 of the SIR?
- Will SDOT continue to use Acyclica RoadTrend Sensors, and for how long? If SDOT plans to switch to other sensors, which ones, and how do their capabilities differ from the RoadTrend Sensors?
- Did SDOT consider any other alternatives when deciding to acquire Acyclica? Did SDOT consider other, more privacy protective traffic management tools in use (for example, inductive-loop detectors currently used by the Washington State Department of Transportation and the US

[14] https://www.flir.com/support/products/trafione#Resources

Department of Transportation)?[15]

- How does SDOT plan to reduce the privacy infringements on non-drivers/riders?

c. Recommendations for Regulation:

At this stage, pending answers to the questions set forth above, we can make only preliminary recommendations for regulation of Acyclica. We recommend that the Council adopt, via ordinance, clear and enforceable rules that ensure, at a minimum, the following:

- There must be a binding contract between SDOT and Acyclica.
- The contract between SDOT and Acyclica must include the following minimum provisions:
  - A data retention period of 12 hours or less for any data Acyclica collects, within which time Acyclica must aggregate the data, submit it to SDOT, and delete both non-aggregated and aggregated data.
  - SDOT receives only aggregated data.
  - SDOT owns all data, not Acyclica.
  - Acyclica cannot share the data collected with any other entity besides SDOT for any purpose.
- The ordinance must define a specific purpose of use for Acyclica technology, and all use of the tool and its data must be restricted to that purpose. For example: Acyclica may only be used for traffic management purposes, defined as activities concerning calculating average travel times, regulating traffic signals, controlling traffic disruptions, determining the placement of barricades or signals for the duration of road incidents impeding normal traffic flow, providing information to travelers about traffic flow and expected delays, and allowing SDOT to meet traffic records and reporting requirements.
- SDOT must produce an annual report detailing its use of Acyclica, including details how SDOT used the data collected, the amount of data collected, and for how long it was retained and in what form.

II. CopLogic – SPD

[15] https://www.fhwa.dot.gov/publications/research/operations/its/06108/03.cfm

Background

CopLogic (LexisNexis's Desk Officer Reporting System-DORS)[16] is a technology owned by LexisNexis and used by the Seattle Police Department to allow members of the public and retailers to submit online police reports regarding non-emergency crimes. Members of the public and retailers can submit these reports through an online portal they can access via their phone, tablet, or computer. Community members can report non-emergency crimes that have occurred within the Seattle city limits, and retail businesses that participate in SPD's Retail Theft Program may report low-level thefts that occur in their businesses when they have identified a suspect. This technology is used by SPD for the stated purpose of freeing up resources in the 9-1-1 Center, reducing the need for a police officer to be dispatched for the sole purpose of taking a police report.

This technology gives rise to potential civil liberties concerns because it allows for the collection of information about community members, unrelated to a specific incident, and without any systematic method to verify accuracy or correct inaccurate information. In addition, there is lack of clarity surrounding data retention and data sharing by LexisNexis, and around how CopLogic data will be integrated into SPD's Records Management System.

a. Concerns

- *Lack of Clarity on CopLogic/LexisNexis Data Collection and Retention.* There is no information in the SIR or in the contract between SPD and LexisNexis detailing the data retention period by LexisNexis (Section 5.2 of the SIR). This lack of clarity stems in part from an unclear description of what's provided by LexisNexis—it's described as an online portal, but the SIR and the contract provided appears to contemplate in Section 4.8 that LexisNexis will indeed access and store collected data. If true, the nature of that access should be clarified, and data restrictions including clear access limitations and retention periods should accordingly be put in place. Once reports are transferred over to SPD's Records Management System (RMS), the reports should be deleted by CopLogic/LexisNexis.

- *Lack of Clarity on LexisNexis Data Sharing with Other Agencies or Third Parties.* If LexisNexis does access and store data, it should do so only for purposes of fulfilling the contract, and should not share that data with third parties. But the contract between SPD and LexisNexis does not make clear whether LexisNexis is prohibited entirely from sharing data with other entities (it does contain a restriction on "transmit[ting]" the data, but without reference to third parties.

[16] https://risk.lexisnexis.com/products/desk-officer-reporting-system

- *No Way to Correct Inaccurate Information Collected About Community Members.* Community members or retailers may enter personally-identifying information about third parties without providing notice to those individuals, and there is no immediate, systematic method to verify the accuracy of information that individuals provide about third parties. There are also no stated measures in the SIR to destroy improperly collected data.

- *Lack of clarity on how the CopLogic data will be integrated with and analyzed within SPD's RMS.* At the technology fair, SPD stated that completed complaints will go into Mark43[17] when it is implemented. ACLU-WA has previously raised concerns about the Mark43 system, and it should be made clear how CopLogic data will enter that system, including to what third parties it will be made available.[18]

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What data does LexisNexis collect and store via CopLogic? What are LexisNexis's data retention policies for CopLogic data?

- Are there specific policies restricting LexisNexis from sharing CopLogic data with third parties? If so, what are they?

- Is there any way to verify or correct inaccurate information collected about community members?

- How will CopLogic data be integrated with Mark43?

c. Recommendations for Regulation:

Pending answers to the questions set forth above, we can make only preliminary recommendations for regulation of CopLogic. SPD should adopt clear and enforceable policies that ensure, at a minimum, the following:

- After CopLogic data is transferred to SPD's RMS, LexisNexis must delete all CopLogic data.

- LexisNexis is prohibited from using CopLogic data for any purpose other than those set forth in the contract, and from sharing CopLogic data with third parties.

[17] https://www.aclu-wa.org/docs/aclu-letter-king-county-council-regarding-mark-43
[18] A Records Management System (RMS) is the management of records for an organization throughout the records-life cycle. New RMSs (e.g., Mark43) may have capabilities that allow for law enforcement agencies to track and analyze the behavior of specific groups of people, leading to concerns of bias in big data policing, particularly for communities of color.

- Methods are available to the public to correct inaccurate information entered in the CopLogic portal.
- Measures are implemented to delete improperly collected data.

III. Computer-Aided Dispatch & 911 Logging Recorder Group

Overall, concerns around the Computer-Aided Dispatch (CAD) and 911 Logging Recorder technologies focus on use of the technologies and/or collected data them for purposes other than those intended, over-retention of data, and sharing of that data with third parties (such as federal law enforcement agencies). Therefore, for all of these technologies as appropriate, we recommend that the responsible agency should adopt clear and enforceable rules that ensure, at a minimum, the following:

- The purpose of use must be clearly defined, and its operation and data collected must be explicitly restricted to that purpose only.
- Data retention must be limited to the time needed to effectuate the purpose defined.
- Data sharing with third parties, if any, must be limited to those held to the same restrictions.
- Clear policies must govern operation, and all operators should be trained in those policies.

Specific comments follow:

1. Computer-Aided Dispatch – SPD

Background

CAD is a software package (made by Versaterm) utilized by the Seattle Police Department's 9-1-1 Center that consists of a set of servers and software deployed on dedicated terminals in the 9-1-1 center, in SPD computers, and as an application on patrol vehicles' mobile data computers and on some officers' smart phones. The stated purpose of CAD is to assist 9-1-1 Center call takers and dispatchers with receiving requests for police services, collecting information from callers, and providing dispatchers with real-time patrol unit availability. Concerns include lack of clarity surrounding data retention and data sharing with third parties.

a. Concerns:

- *Lack of clarity on data retention within CAD v. RMS.* While the SIR makes clear that at some point, CAD data is transferred to SPD's RMS, it is unclear what data, if any, the CAD system itself retains and for how long. If the CAD system does retain some data (for example, call logs)

independent of the RMS, and that data is accessible to the vendor, appropriate data protections should be put in place. But because the SIR usually references "data collected by CAD," it is unclear where that data resides.

- *Lack of a policy defining purpose of the technology and limiting its use to that purpose*: Unlike SFD's similar system, SPD appears to have no specific policy defining the purpose of use for CAD and limiting its use to that purpose.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- Does the CAD system itself store data? If so, what data and for how long? Who can access that data?

c. Recommendations for Regulation:

Depending on the answer to the question above, appropriate data protections may be needed as described above. In addition, SPD should adopt a policy similar to SFD's, clearly defining purpose and limiting use of the tool to that purpose.

2. Computer-Aided Dispatch – SFD

Background

Computer Aided Dispatch (CAD) is a suite of software packages used by SFD and made by Tritech that provide unit recommendations for 911 emergency calls based on the reported problem and location of a caller. The stated purpose of CAD is to allow SFD to manage emergency and non-emergency call taking and dispatching operations. The technology allows SFD to quickly enable personnel to execute rapid aid deployment.

Generally and positively, SFD clearly defines the purpose of use, restricts CAD operation and data collection to that purpose only, limits sharing with third parties, and specifies policies on operation and training. However, SFD must clarify what data is retained within CAD, data retention policies, and provide information about its data sharing partners.

d. Concerns

- *Lack of clarity on data retention within CAD*. It is unclear what data, if any, the CAD system itself retains and for how long. If the CAD system does retain some data (for example, call logs) and that data is accessible to the vendor, appropriate data protections should be put in place.
- *Lack of clarity on data retention policies*. At the technology fair, we learned that CAD data is retained indefinitely. It is not clear what justifies indefinite retention of this data.

- *Lack of clarity on data sharing partners.* In Section 6.3 of the SIR, SFD states that in rare case where CAD data is shared with partners other than those specifically named in the SIR, a third-party nondisclosure agreement is signed. However, there are no examples or details of who those partners are and the purposes for which CAD data would be shared.

e. Outstanding Questions That Must be Addressed in the Final SIR:

- Does the CAD system itself store data? If so, what data and for how long? Who can access that data?
- Who are SFD's data sharing partners? For what purpose is data shared with them?

f. Recommendations for Regulation:

Depending on the answer to the question regarding if the CAD system itself stores data, appropriate data protections may be needed as described above. SFD should adopt a clear policy requiring deletion of CAD data no longer needed. In addition, depending on how data is shared, SFD should adopt a policy that clearly limits what for what purposes CAD data would be shared, and with what entities.

3. 911 Logging Recorder – SPD

Background

The NICE 911 logging recorder is a technology used by SPD to audio-record all telephone calls to SPD's 9-1-1 communications center and all radio traffic between dispatchers and patrol officers. The stated purpose of the 9-1-1 Logging Recorder is to allow SPD to provide evidence to officers and detectives who investigate crimes and the prosecutors who prosecute offenders. These recordings also provide transparency and accountability for SPD, as they record in real time the interactions between 9-1-1 call takers and callers, and the radio traffic between 9-1-1 dispatchers and police officers. The NICE system also supports the 9-1-1 center's mission of quickly determining the nature of the call and getting the caller the assistance they need as quickly as possible with high quality, consistent and professional services.

Concerns include lack of clarity surrounding data retention schedules and data sharing with third parties.

a. Concerns

- *Lack of clarity on data retention.* Section 4.2 of the SIR states: "Recordings

requested for law enforcement and public disclosure are downloaded and maintained for the retention period related to the incident type." Similar to other technologies noted above, it is unclear whether the 9-1-1 system itself stores these recordings, or if they are stored on SPD's RMS. If the former, it should be made clear how the technology vendor accesses these recordings and for what purpose, if at all.

- *More clarity needed on data sharing with third parties.* There are no details or examples of the "discrete pieces of data" that are shared outside entities and individuals as referenced in Section 6.0 of the SIR.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What is SPD's data retention schedule for data stored in the NICE system, if any?
- What "discrete pieces of data" does SPD share with third parties?

c. Recommendations for Regulation:

SPD should adopt a clear policy requiring deletion of data no longer needed. In addition, depending on how data is shared, SPD should adopt a policy that clearly limits what for what purposes data would be shared, and with what entities.

IV. Current Diversion Technology Group – Seattle City Light

The technologies in this group—the Check Meter device (SensorLink TMS), the SensorLink Amp Fork, and the Binoculars/Spotting Scope raise civil liberties concerns primarily due to lack of explicit, written policies imposing meaningful restrictions on use of the technologies. While the purpose of the current diversion technologies appears clear—to assess whether suspected diversions of current have occurred and/or are continuing to occur—there are no explicit policies in the SIR detailing restrictions on what can and cannot be recorded by these technologies.

Below are short descriptions of the technologies, followed by concerns and recommendations.

Background

1. Check Meter Device (SensorLink TMS)

The SensorLink TMS device measures the amount of City Light-provided electrical energy flowing through the service-drop wire over time, digitally capturing the instantaneous information on the device for later retrieval by the Current Diversion Team via the use of a secure wireless protocol.

The stated purpose of use is to allow Seattle City Light to maintain the integrity of its electricity distribution system, to determine whether suspected current diversions have taken place, and to provide the valuation of the diverted energy to proper authorities for cost recovery.

2. SensorLink Amp Fork

The SensorLink Amp Fork is an electrical device mounted on an extensible pole allowing a circular clamp to be placed around the service-drop wire that provides electrical service to a customer location via its City Light-provided meter. The device then displays instantaneous readings of the amount of electrical energy (measured in amperage, or "amps") that the Current Diversion Team may compare against the readings displayed on the meter, allowing them to determine if current is presently being diverted.

The stated purpose of use of the Amp Fork is to allow Seattle City Light to assess whether suspected diversions of current have occurred and/or are continuing to occur. The Amp Fork allows the Utility to determine the valuation of the energy illegally diverted, which supports City Light's mission of recovering this value for ratepayers via a process called "back-billing."

3. Binoculars/Spotting Scope

The binoculars are standard, commercial-grade, unpowered binoculars. They do not contain any special enhancements requiring power (e.g., night-vision or video-recording capabilities). They are used to read a meter from a distance when the Current Diversion Team is otherwise unable to access physically the meter for the purpose of inspection upon suspected current diversion.

The stated purpose of the binoculars is to allow Seattle City Light to inspect meters and other implicated electrical infrastructure at a distance. If a determination of diversion is sustained, data may be used to respond to lawful requests from the proper law enforcement authorities for evidence for recovering the value of the diverted energy.

a. Concerns Regarding all Three Current Diversion Technologies

- *Absence of explicit, written policies imposing meaningful restrictions on use.* At the technology fair, a Seattle City Light representative stated that these technologies are used only for the purpose of checking current diversions, but could not confirm that Seattle City Light had clear, written policies for what data could and could not be recorded (e.g., an employee using the binoculars to view non-meter related information). The absence of written, specific policies increases the risk of unwarranted surveillance of individuals. There is also no mention in the SIRs of

specific data protection policies in place to safeguard the data (e.g., encryption, hashing, etc.).

- *Seattle City Light's records retention schedule is mentioned in the SIRs, but details about it are omitted.* It is unclear how long Seattle City Light retains data collected, and for what reason.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What enforceable policies, if any, apply to use of these three technologies?
- What is Seattle City Light's data retention schedule?

c. Recommendations for Regulation:

Seattle City Light must create clear, enforceable policies that, at a minimum:

- Define purpose of use for each technology and restrict its use to that purpose.
- Clearly state what clear data protection policies exist to safeguard stored data, if any, and ensure the deletion of data collected by the technology immediately after the relevant current diversion investigation has closed.

Thank you for your consideration, and please don't hesitate to contact me with questions.

Best,

Shankar Narayan
Technology and Liberty Project Director

Jennifer Lee
Technology and Liberty Project Advocate

15

Appendix 1: Benhammou Letter

City of Seattle

Acyclica

February 6th, 2015

RE: Acyclica data privacy standards

To whom it may concern:

The purpose of this letter is to provide information regarding the data privacy standards maintained by Acyclica. Acyclica is a traffic information company specializing in traffic congestion information management and analysis. Among the various types of data sources which make of Acyclica's traffic data portfolio including GPS probe data, video detection and inductive loops, Acyclica also utilizes our own patent-pending technology for the collection of Bluetooth and Wifi MAC addresses. MAC or Media Access Control addresses are unique 48-bit numbers which are associated with devices with Bluetooth and/or Wifi capable devices.

While MAC addresses themselves are inherently anonymous, Acyclica goes to great lengths to further obfuscate the original source of data through a combination of hashing and encryption to all but guarantee that information derived from the initial data bears no trace of any individual.

Acyclica's technology for collecting MAC addresses for congestion measurement operates by detecting nearby MAC addresses. The MAC addresses are then encrypted using GPG encryption before being transmitted to the cloud for processing. Encrypting the data prior to transmission means that no MAC addresses are ever written where they can be retrieved from the hardware. Once the data is received by our servers, the data is further anonymized using a SHA-256 algorithm which makes the raw MAC address nearly impossible to decipher from the hashed output. Furthermore, any customer seeking to download data for further investigation or integration through our API can only ever view the hashed MAC address.

Acyclica occasionally provides data to partners to help enhance the quality of congestion information. The information which is provided to such partners is received through API calls which only return aggregated information about traffic data over a given period such as the average travel-time over a 5-minute period. Aggregating the data provides a final layer of anonymization by reporting on the collective trend of all vehicles rather than the specific behavior of a single vehicle.

As always questions, comments and concerns are welcome. Please do let me know if we can provide further clarity and transparency on our internal operations with regards to data processing and privacy standards. We take the privacy of the public very seriously and always treat our customers and the data with the utmost respect.

Regards,

Daniel Benhammou
President
Acyclica Inc.

Appendix H: Comment Analysis Methodology

Overview

The approach to comment analysis includes combination of qualitative and quantitative methods. A basic qualitative text analysis of the comments received, and a subsequent comparative analysis of results, were validated against quantitative results. Each comment was analyzed in the following ways, to observe trends and confirm conclusions:

1. Analyzed collectively, as a whole, with all other comments received
2. Analyzed by technology
3. Analyzed by technology and question

A summary of findings are included in Appendix B: Public Comment Demographics and Analysis. All comments received are included in Appendix E: All Individual Comments Received.

Background on Methodological Framework

A modified Framework Methodology was used for qualitative analysis of the comments received, which "*…approaches [that] identify commonalities and differences in qualitative data, before focusing on relationships between different parts of the data, thereby seeking to draw descriptive and/or explanatory conclusions clustered around themes" (Gale, N.K., et.al, 2013).* Framework Methodology is a coding process which includes both inductive and deductive approaches to qualitative analysis.

The goal is to classify the subject data so that it can be meaningfully compared with other elements of the data and help inform decision-making. Framework Methodology is "not designed to be representative of a wider population, but purposive to capture diversity around a phenomenon" (*Gale, N.K., et.al, 2013).*

Methodology

Step One: Prepare Data

1. Compile data received.
    a. Daily collection and maintenance of 2 primary datasets.
        i. Master dataset: a record of all raw comments received, questions generated at public meetings, and demographic information collected from all methods of submission.
        ii. Comment analysis dataset: the dataset used for comment analysis that contains coded data and the qualitative codebook. The codebook contains the qualitative codes used for analysis and their definitions.
2. Clean the compiled data.
    a. Ensure data is as consistent and complete as possible. Remove special characters for machine readability and analysis.
    b. Comments submitted through SurveyMonkey for "General Surveillance"

remained in the "General Surveillance" category for the analysis, regardless of content of the comment. Comments on surveillance generally, generated at public meetings, were categorized as such.

c. Filter data by technology for inclusion in individual SIRs.

Step Two: Conduct Qualitative Analysis Using Framework Methodology

1. Become familiar with the structure and content of the data. This occurred daily compilation and cleaning of the data in step one.
2. Individually and collaboratively code the comments received, and identify emergent themes.
   I. Begin with deductive coding by developing pre-defined codes derived from the prescribed survey and small group facilitator questions and responses.
   II. Use clean data, as outlined in Data Cleaning section above, to inductively code comments.
      A. Each coder individually reviews the comments and independently codes them.
      B. Coders compare and discuss codes, subcodes, and broad themes that emerge.
      C. Qualitative codes are added as a new field (or series of fields) into the Comments dataset to derive greater insight into themes, and provide increased opportunity for visualizing findings.
   III. Develop the analytical framework.
      A. Coders discuss codes, sub-codes, and broad themes that emerge, until codes are agreed upon by all parties.
      B. Codes are grouped into larger categories or themes.
      C. The codes are be documented and defined in the codebook.
   IV. Apply the framework to code the remainder of the comments received.
   V. Interpret the data by identifying differences and map relationships between codes and themes, using R and Tableau.

Step Three: Conduct Quantitative Analysis

1. Identify frequency of qualitative codes for each technology overall, by questions, or by themes:
   I. Analyze results for single word codes.
   II. Analyze results for word pair codes (for context).
2. Identify the most commonly used words and word pairs (most common and least common) for all comments received.
   I. Compare results with qualitative code frequencies and use to validate codes.
   II. Create network graph to identify relationships and frequencies between

words used in comments submitted. Use this graph to validate analysis and themes.

3. Extract CSVs of single word codes, word pair codes, and word pairs in text of the comments, as well as the corresponding frequencies for generating visualizations in Tableau.

Step Four: Summarization

1. Visualize themes and codes in Tableau. Use call out quotes to provide context and tone.
2. Included summary information and analysis in the appendices of each SIR.

Appendix I: Supporting Policy Documentation

Management Control Agreement

Management Control Agreement Between
Seattle Police Department and
City of Seattle Information Technology Department

The City of Seattle Police Department ("SPD"), also referred to as the Criminal Justice Agency, and the City of seattle Information Technology Department ("ITD") are departments of the municipal corporation of the City of Seattle.

Pursuant to Seattle Municipal Code ("SMC") 3.23, ITD provides information technology systems, services, and support to SPD and is therefore required to support, enable, enforce, and comply with SPD policy requirements, including the FBI's Criminal Justice Information Services ("CJIS") Security Policy.

Pursuant to the CJIS Security Policy, it is agreed that with respect to the administration of computer systems, network infrastructure, devices, and services interfacing directly or indirectly with A Central Computerized Enforcement System ("ACCESS") for the exchange of criminal history/criminal justice information, the Criminal Justice Agency shall have the authority, via managed control, to set and enforce:

Priorities that guarantee the priority, integrity, and availability of service needed by the criminal justice community.

Requirements for the selection, authorization, supervision, and termination of physical and logical access to Criminal Justice Information ("CJI").

Policy governing operation of justice systems, data, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a communications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.

Restriction of unauthorized physical and logical access to or use of systems and equipment accessing CJI.

Compliance with all rules and regulations of the Criminal Justice Agency policies and CJIS Security Policy in the operation of, access to, or control over any CJI systems, data, or infrastructure.

The responsibility for management control of the criminal justice function remains solely with the Criminal Justice Agency. ITD will not enter into any agreements or allow any access to, possession of, or control over any SPD CJI systems, data, or infrastructure without explicit authorization from at least one SPD Authorized Party. SPD Authorized Parties must be SPD employees and include:
Chief of Police
Chief Operating Officer

This agreement covers the overall supervision of all Criminal Justice Agency systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, administration, and maintenance of any Criminal Justice Agency system to include NCIC Programs that may be subsequently designed and/or implemented within the Criminal Justice Agency.

Additional agreements, such as a Memorandum of Agreements, Service Level Agreements, and/or Continuity Plans, may be established and maintained to further delineate, define, and assign roles, responsibilities, and requirements of and agreements between SPD and ITD, and other City of Seattle Departments and/or agencies.

Tracye Cantrell

Tracye Cantrell
Interim Chief Technology Officer
Seattle Information Technology Department

Date Feb 2, 2018

Carmen Best

Carmen Best
Interim Chief of Police |
Seattle Police Department

Date 2-7-2018

Reference: CJIS Security Policy, Version 5.5, dated June 1, 2016 (CJISD-ITS-DOC-08140-5 .5)

IT Support Services for City Technology

Engineering and Operations

This division designs, implements, operates, and supports technology solutions and resources in accordance with city wide architecture and governance. Responsibilities for this division include:

- Primary communications networks that provide public safety and constituent access to and from City government; the telephone system, the data network, and Public Safety Radio System. Responsible for sustaining all three systems operating as close to 100% availability as possible 24 hours a day, seven days a week.
- Design, acquisition, installation, maintenance, repair and management of fiber optic cables on behalf of City departments and approximately 20 other local, state and federal agencies.
- Procurement requests, allocation, operation and maintenance of city wide and departmental servers, virtual enterprise computing and SAN storage environments for large scale mission critical applications in a secure, reliable, 24/7 production environment for enterprise computing.
- Allocation, operation and maintenance of enterprise level services like messaging services, web access, file sharing, user management and remote access solutions.
- Collaborate with Enterprise Architecture team to develop standards for information technology equipment and software.
- Service Desk and technical support services for City's computers, peripherals, electronic devices and mobile device management.
- Centralized IT asset management to include research, procurement request, surplus and asset transfer.
- Facility management for a reliable production computing environment to the City departments.
- Support for other enterprise services and tools.

Compute System Technologies

This team manages the operations and maintenance of computing infrastructure, including servers, storage, backup and recovery, and enterprise support systems (e.g., Active Directory, VPN, etc.). The team is also responsible for safeguarding systems and data by performing required security patches, updates, and backups to ensure systems operate at as close to 100% availability as possible 24x7. Units within this group include:

Systems Operations. The team is focused on delivering the computing environment across multiple departments. The team has technical expertise to design, integrate, and operate a secure, reliable computing environment. Key technologies include Windows, Solaris, IBM AIX, and Linux.

Enterprise Services. Enterprise Services (ES) are large scale infrastructure and application services used by the City of Seattle end user community. This includes both SaaS and NGDC hosted infrastructure and application services. The team is responsible for EA vendor management, system administration, upgrades and technical support. Key technologies

includes Microsoft Active Directory (AD), Distributed File System (DFS), Exchange Online, Office 365 and SharePoint Online infrastructure.

Infrastructure Tools. The team provides a single focus for the design, planning, deployment and maintenance of standard enterprise infrastructure monitoring and management tools. This includes system performance (Solarwinds, SCOM), configuration management (SCCM, WSUS), and monitoring and system management (Trend Micro, CRM, Vipre).

Virtual and Data Infrastructure. This team engineers and operates reliable, flexible, performant virtualized Windows, UNIX and Linux platforms and their related technologies in direct support of critical business applications. Key technologies include Solaris, Unix, Linux, Windows, and vmWare, and the associated virtualization Nutanix, IBM LPAR, and Solaris hardware.

The team also engineers and operates reliable, flexible, performant storage and data protection solutions to host and protect critical business data of all types, leveraging SAN, NAS, object, and cloud technologies. Key technologies include Dell Compellent, Quantum, Hitachi, NetApp, Cloud storage, Brocade fiber channel switching, and Commvault.

Network And Communications Technologies

This team is responsible for designing, installing, operating, and maintaining data, voice, radio, fiber optic, and structured cabling infrastructure that integrates with other technologies to provide access to resources used by City departments and the public we serve. Units within this group include:

Network Engineering & Operations. The Network Services team engineers, operates and maintains the City's data network, including data center core networks, the internet perimeter, the network backbone, and local area networks that support systems and users across the City. This group designs, acquires, installs, maintains, repairs, and manages an enterprise data network that aligns with City architectures and standards. This group also participates in development of those standards and provides tier 2 and 3 end user support. This team supports technologies that include routing, switching, load balancing, enterprise Wi-Fi, DNS/DHCP/NTP, and network security (including firewalls, VPN appliances, certificate infrastructure, network access control, and web filtering.)

Telecommunication Engineering & Operations. The Telecommunications Services team engineers, operates, and maintains a highly-reliable enterprise telephone and contact center infrastructure. This group supports end user move and change activity and provides tier 2 and 3 support. The Telecommunication Services team acquires, installs, maintains, and repairs telecommunications equipment and manages commercial telephony circuits. It supports technologies that include VoIP, circuit-switched telephony, voice mail, contact center services (including call routing scripts), audio conference bridges, commercial telephony services, SONET, and WDM.

Radio & Communications Infrastructure. This team delivers radio services for public safety and other government departments. It provides extremely reliable infrastructure and support for end user mobile and portable radio equipment. The group installs and maintains communications equipment inside 911 dispatch centers and City vehicles, with primary support to SPD and SFD. The team also supports regional planning,

maintenance, interoperability testing, and projects (including PSERN and Washington OneNet) in partnership with other local, state, and federal agencies. This team also designs, acquires, installs, maintains, repairs, and manages in-building structured cabling systems and outside plant fiber optic and copper cable infrastructure for the City and approximately 20 external public agency partners. Technologies include trunked and conventional land mobile radio, microwave radio and other wireless communications systems (including point-to-multipoint and mesh networks,) distributed antenna systems, routing/MPLS, DS3/T1/DACS, outside plant cable infrastructure (including fiber and copper,) and structured cabling infrastructure.

End User Support

This team is responsible for providing a single point of contact for IT technical support, trouble ticket and service request resolution and referral services to other IT workgroups, and for communication for all changes, patches, upgrades and standards changes. The team is also responsible for providing technical support for the City's desktop computers, peripherals, electronic devices and mobile devices. Units within this group include:

Service Desk. The Service Desk team provides a single point of contact for Seattle IT services, promptly resolving incidents and service requests when first contacted whenever possible, escalating issues accurately and efficiently, and keeping users and partners aware of service status and changes.

Device Support. This team provides direct customer support for end user computing to all departments within the City and tier 2 escalation support and management of centralized end user computing applications and hardware. requests.

Device Engineering. This team engineers and deploys software packages for end user applications, device drivers, patches, security updates and custom packages as required. This team evaluates and recommends hardware and software for end user standards. In addition, this team provides tier 3 escalation support and management of centralized end user computing applications and hardware.

Asset Management. This team is responsible tracking and inventory controls for city wide IT assets including desktops, laptops, printers, servers, switches, and miscellaneous Information Technology infrastructure. In addition to inventory control, the team will be forecasting replacement cycles for equipment based on City standards to promote a stable computing environment.

IT Operations Support

The IT Operations Support team is responsible for management of Information Technology facilities (including data centers and communications equipment rooms), and installation and cabling equipment within those facilities. This team provides the enterprise Network Operations Center (NOC) that monitors alerts, performs initial incident analysis, dispatches tier 2 and 3 technical support, and provides initial incident communication for network

infrastructure and computing systems managed by Engineering and Operations. Units within this group include:

Installation Management. This team installs networking and computing equipment in data centers, communications rooms and wiring closets; installs and maintains network cabling within data centers and equipment rooms according to City standards; and supports repair and end user move and change activity (including telephone move projects).

IT Operations Center. This team manages facilities which support City computing and communications services. This includes managing access to facilities, coordinating vendors, maintaining records (including data center inventory management), and, where applicable, monitoring facility systems (including CRUs, fire alarms, water detection sensors, UPS systems, and power consumption). This team also staffs the NOC that monitors alerts from network infrastructure and computing systems, performs initial problem analysis, dispatches appropriate tier 2 and 3 technical support team(s), and provides initial incident communication.

Application Services

This division designs, develops, integrates, implements, and supports application solutions in accordance with city wide architecture and governance. Its teams are organized to support business functions or service groups**.** The integration of application services will be completed gradually in 2017, with details of the organization and integration process still under development.

Applications
These teams will provide development and support for applications that include customer relationship management, billing, finance, human resources, work and asset management and records management.

Shared Platforms
These teams will provide development and support for applications that include engineering, spatial analysis, business intelligence, analytics, SharePoint Online and document management.

Cross Platform Services
These teams will provide support to application teams, including quality assurance, change control, database administration, integration services, and access management activities.

Remote Access Policy

City of Seattle

CJIS Remote Access Policy

June 1st, 2018

Overview

The CJI Remote Access Policy defines the necessary controls for remote access to Criminal Justice Information Services (CJIS) in scope systems.

Purpose

This policy ensures proper measures are taken when granting remote access to any employee, contractor, or vendor, to Criminal Justice Information (CJI) in-scope systems.

Definition

CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, decimation, storage, and destruction of CJI.

Scope and Applicability

This policy applies to personnel at City of Seattle, including those affiliated with third parties who remotely access City of Seattle systems to include CJI data. The policy applies to all systems owned by and/or administered by City of Seattle, including network to network VPN tunnels.

Policy

This policy applies to City of Seattle employees, City of Seattle Police Department employees, contractors, or vendors who have a need to remotely access the CJI (Criminal Justice Information) in-scope systems for maintenance and operations. All access both remote and within the City of Seattle network or Public network, are required to utilize two factor authentication & VPN tunnel on City of Seattle workstation OR through a jump-box protected by two-factor Advanced Authentication (AA). Contractors, Vendors and City employees accessing in-scope systems from non-city computers are required to utilize the jump-box AA solution.

All non-law enforcement personnel who perform criminal justice functions or have access to Criminal justice data shall acknowledge, via signing of the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. Seattle Information Technology employees are not required to sign the Security Addendum provided there is a CJIS Management Control Agreement (MCA) between Seattle Information Technology and Seattle Police/Fire.

- CJIS Security Awareness Training shall be required upon initial assignment, and biennially thereafter, for all personnel who have access to CJI.
- Verify Identification: a state of residency and national fingerprint-based record checks shall be conducted (prior to) assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.
- All requests for access shall be made as specified by the CSO (CJIS Systems Officer). The CSO, or their designee, is authorized to approve access to CJI. All designees shall be from an authorized criminal justice agency.
- VPN access must be approved by the requesting department prior to activation.
- Users must not:
    - Type remote access passwords while someone is watching. Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. (CJIS Security Policy Section 5.5.5) A session lock is not a substitute for logging out of the information system or from disconnecting a remote session.
    - Be connected to other network connections during remote access sessions into CJI data in-scope (e.g., no split tunnels are allowed).
- Users must maintain current virus protection and a host firewall on remote systems to protect from viruses and other remote attacks.
- Vendors must:
    - Be provided with the minimum access required to perform the necessary duties while the VPN session is active. Other access and privileges will be limited to the specific function performed by each vendor or service provider.
    - Be monitored by a City of Seattle CDE administrator during an assisted remote control session using Skype for Business or other current City of Seattle Enterprise standard for remote control sessions. The CDE administrator must have the ability to end the session at any time and the session must be terminated as soon as their work has finished.

Applicability of other Policies

January 17, 2016 1 The City of Seattle has an existing Remote Access Policy that must be adhered to and can be found here.

Enforcement

Enforcement of this policy will be led by the Chief Technology Officer (CTO). Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment or vendor contract termination. Where illegal activities or loss of City of Seattle assets are known or suspected, the City of Seattle must report activities to the appropriate authorities, City of Seattle is obliged to adhere to breach reporting by statutory limitation and must notify the Terminal Agency Coordinator (TAC) of any potential violations. All potential violations that involve CJI must be report to the Washington State Patrol ACCESS Section.

Implementation

This Policy is implemented by the ITD Security, Risk, and Compliance Director and applies to the City of Seattle access to CJI.

Document Control

Version	Content	Contributors	Approval Date
1.0	Initial Draft	Reviews: Denise Mendoza; Pepper Bojang-Jackson Approvers: CISO Andrew Whitaker CTO	
1.1	Initial Draft	Reviews: Denise Mendoza; Pepper Bojang-Jackson	
1.2	Initial Draft	Reviews: Denise Mendoza Bruce Hills Pepper Bojang-Jackson	
1.3	Review	Andrew Whitaker	6/5/18
1.4	Approved	Tracye Cantrell	6/12/18

City of Seattle

Technical Security Audit

Technical Security Audit

Agency Information: Seattle PD - (WASPD0000)

Submitted By: Pepper Bojang-Jackson - On: March 22, 2017 Compliance Report with Agency Responses

Compliance Report

NCIC compliance standards must be improved and a response submitted to the WSP ACCESS Section.

Item:	1
Section Name:	Personnel Security
Question:	Are you maintaining a record of all your agency and/or county/city IT personnel that must receive a state of residency fingerprint background check within 30 days of employment? *(CJIS Security Policy, Version 5.5, Section 5.12.1.1)* Yes Please provide the SID numbers for all the IT personnel.
Agency Response:	List emailed 05/16/17

Item:	2
Section Name:	Personnel Security
Question:	Have all your agency and/or county/city IT personnel viewed the technical security awareness training (Level 4) in CJIS Online? *(CJIS Security Policy, Version 5.5, Section 5.2)* Yes All technical staff must view the technical security training - level 4 once every two years. Please provide a list of names of who viewed the training. The training is available at the following address: https://www.cjisonline.com/
Agency Response:	Sent email 05/16/17

Item:	3

Section Name: Personnel Security

Question: Does your agency use an IT vendor for any IT needs?

Sub Question(s)

Item: 3.1

Section Name: Personnel Security

Question: Have all IT *vendors* had a Washington State fingerprint background check completed? *(CJIS Security Policy, Version 5.5, Section 5.12.1.1 and 5.12.1.2)*

User Answer: Yes

Compliance Response: All IT vendors must have a Washington State fingerprint background check completed.

Agency Response: List emailed 05/16/17

Sub Question(s)

Item: 3.2

Section Name: Personnel Security

Question: Please send a copy of the security addendum signed by each employee of the vendor company to CJISAudits@wsp.wa.gov

User Answer: I have read and will comply.

Compliance Response: Please provide a copy of the signed security addendum for each employee of the vendor company. I am missing security addendums for the following vendors:

1. 4quarters
2. Advantage Factory
3. Dorsey Consulting
4. Gartner
5. Genetec Corp
6. Sabey
7. Sysorex Consulting
8. TASER
9. TEKsystems
10. Versaterm - only a few

Agency Response:

1. 4quarters - Emailed 05/08/17
2. Advantage Factory - All Advantage Factory accounts are

inactive
3. Dorsey Consulting - DOJ Monitoring Team - Should be CJIS Level 2, not 4 (deactivated all accounts)
4. Emailed 05/22/17
5. Genetec Corp - All accounts are inactive.
6. Adashi - Adashi employees are working in an environment that does not currently have CJIS data. Future plans do include CJIS data so they are in the process of completing the Security Addendums.
7. Sysorex Consulting - All accounts are inactive

8. TASER - Emailed 05/18/17
9. TEKsystems - Contractor is now City IT w/updated information.
10. Versaterm - Emailed 05/08/17

Item: 4
Section Name: System and Communications Protection and Information Integrity
Question: Does your agency email CJI? *(CJIS Security Policy, Version 5.5, Section 5.10.1.2)*

Sub Question(s)

Item: 4.1
Section Name: System and Communications Protection and Information Integrity
Question: Is the email that contains CJI encrypted? *(CJIS Security Policy, Version 5.5 Section 5.10.1.2)*
User Answer: No
Compliance Response: CJI that is emailed is required to be encrypted. Please advise when you will have this in place.
Agency Response: Seattle is utilizing Office 365 for email and email is encrypted

Is the email encrypted in transit? https://products.office.com/en-us/business/office-365-trust-center-security

Outlook client to O365 - SSL/TLS connection is established between Outlook client and O365

O365 to OME server - SSL / TLS connection between EXO Transport servers and OME server. "Office 365 uses Transport Layer Security (TLS) to encrypt the connection, or session, between two servers." https://support.office.com/en-us/article/Email-encryption-in-Office-365- c0d87cbe-6d65-4c03-88ad-5216ea5564e8

Is the email encrypted at rest when it sits on the server? https://support.office.com/en-us/article/Email-encryption-in-Office-365-c0d87cbe-6d65-4c03-88ad-5216ea5564e8

What about encryption for data at rest?

"Data at rest" refers to data that isn't actively in transit. In Office 365, email data at rest is encrypted using BitLocker Drive Encryption.
BitLocker encrypts the hard drives in Office 365 datacenters to provide enhanced protection against unauthorized access. To learn more, see BitLocker Overview.

What level of encryption does OME use? - Microsoft attests that they meet and/or exceed FBI CJIS requirements

The CJIS Security Policy defines 13 areas that private contractors such as cloud service providers must evaluate to determine if their use of cloud services can be consistent with CJIS requirements. These areas correspond closely to NIST 800-53, which is also the basis for the Federal Risk and Authorization Management Program (FedRAMP), a program under which Microsoft has been certified for its Government Cloud offerings

Item: 5

Section Name: Event Logging

Question: Does your agency have an established audit trail capable of monitoring the following:

- Successful and unsuccessful log on attempts
- Successful and unsuccessful password changes
- Successful and unsuccessful attempts to access, create, write, delete or change permissions on a user account, file, directory or other system resources
- Successful and unsuccessful actions by privileged accounts
- Successful and unsuccessful attempts for users to access, modify, or destroy audit log files

(CJIS Security Policy, Version 5.5, Section 5.4.1.1)

User Answer: No

Compliance Response: Please advise when your agency will have an established audit trail capable of monitoring the following:

- Successful and unsuccessful log on attempts
- Successful and unsuccessful password changes
- Successful and unsuccessful attempts to access, create, write, delete or

change permissions on a user account, file, directory or other system resources

- Successful and unsuccessful actions by privilegedaccounts
- Successful and unsuccessful attempts for users to access, modify, or destroy audit log files

Agency Response:

Seattle PD has established an audit trail capable of monitoring the following:

- Successful and unsuccessful log on attempts
- Successful and unsuccessful password changes
- Successful and unsuccessful attempts to access, create, write, delete or change permissions on a user account, file, directory or other system resources
- Successful and unsuccessful actions by privilegedaccounts
- Successful and unsuccessful attempts for users to access, modify, or destroy audit log files

Item: 6

Section Name: Identification and Authentication

Question: Does your agency and/or county/city IT department employee perform remote assistance from a non-secure location? Example employees home or coffee shop etc.

(CJIS Security Policy, Version 5.5, Section 5.6.2.2)

User Answer: Yes

Compliance Response: IT has the ability to remote in the system from a non-secure location. Please advise once Advanced Authentication will be in place or when a remote session will be virtually escorted at all times.

Agency Response:

Full policy emailed to ACCESS on 04/23/18:

This policy applies to employees, contractors, or vendors who have a need to remotely access the CJI (Criminal Justice Information) in-scope systems for maintenance and operations. All access both remote and within the Seattle network (except for the SPD network) is through bastion hosts protected by two-factor Advanced Authentication (AA).

*All non-law enforcement personnel who perform criminal justice functions or have access to Criminal justice data shall acknowledge, via signing of the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS

Security Addendum. Seattle Information Technology employees are not required to sign the Security Addendum provided there is a CJIS Management Control Agreement (MCA) between Seattle Information Technology and Seattle Police/Fire.

*CJIS Security Awareness Training shall be required upon initial assignment, and biennially thereafter, for all personnel who have access to CJI.

Verify Identification: a state of residency and national fingerprint-based record checks shall be conducted (prior to) assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.

*All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All designees shall be from an authorized criminal justice agency.

*VPN access must be approved by the requesting department prior to activation.

*Users must not:

Type remote access passwords while someone is watching. Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. (CJIS Security Policy Section 5.5.5) A session lock is not a substitute for logging out of the information system or from disconnecting a remote session.

Be connected to other network connections during remote access sessions into CJI data in-scope (e.g., no split tunnels are allowed).

*Users must maintain current virus protection and a host firewall on remote systems to protect from viruses and other remote attacks.

*Vendors must:

Be provided with the minimum access required to perform the necessary duties while the VPN session is active. Other access and privileges will be limited to the specific function performed by each vendor or service provider.

Be monitored by a City of Seattle CDE administrator during an assisted remote control session using Skype for Business or other current City of Seattle Enterprise standard for remote control sessions. The CDE administrator must have the ability to end the session at any time and the session must be terminated as soon as their work has finished.

Item: 6.1

Section Name: Identification and Authentication

Question: Describe the type of Advanced Authentication (AA) that is being used while the remote session is in process or advise if the session is being virtually escorted at all times. Virtually escorting is permitted when the following conditions are met:

- The session shall be monitored at all times by an authorized escort.
- The escort shall be familiar with the system/area in which the work is being performed.
- The escort shall have the ability to end the session at any time.
- The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.
- The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.

(CJIS Security Policy, Version 5.5, Section 5.5.6)

User Answer: Certificate on the workstation. RSA is being implemented for network equipment.

Rarely workstations are remotely accessed. If they are, an SPD computer would be used to do the support work.

Compliance Response: Please advise when AA will be in place for IT staff that conducts remote assistance on applications or networks that access CJI or when all personnel will be virtually escorted or a policy prohibiting remote access from an unsecure location is established.

Agency Response: See #6

City of Seattle

Item: 7

Section Name: Cloud Computing

Question: Does the agency utilize a cloud provider to host or store CJI related systems, applications or data? *(CJIS Security Policy, Version 5.5, Section 5.10.1.5)*

Sub Question(s)

Item: 7.1

Section Name: Cloud Computing

Question: Is the CJI encrypted prior to entering the cloud?

User Answer: No

Compliance Response: Please advise when the CJI that goes to the cloud will be encrypted.

Agency Response: Seattle is utilizing Office 365 and CJI is encrypted

Report Summary: The Federal Bureau of Investigation (FBI) assigned the Washington State Patrol (WSP) as the Criminal Justice Information Services (CJIS) Systems Agency (CSA) for the state of Washington. The CSA is responsible for establishing and administering an information technology security program throughout the CSA user community, to include the local levels. All standards set forth in the audit questionnaire originate

from the CJIS Security Policy which provides Criminal Justice Agencies (CJA) with a minimum set of security requirements for access to FBI CJIS Division systems and information to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

CJIS Security Policy

[Add here]

Appendix J: CTO Notification of Surveillance Technology

Thank you for your department's efforts to comply with the new Surveillance Ordinance, including a review of your existing technologies to determine which may be subject to the Ordinance. I recognize this was a significant investment of time by your staff; their efforts are helping to build Council and public trust in how the City collects and uses data.

As required by the Ordinance (SMC 14.18.020.D), this is formal notice that the technologies listed below will require review and approval by City Council to remain in use. This list was determined through a process outlined in the Ordinance and was submitted at the end of last year for review to the Mayor's Office and City Council.

The first technology on the list below must be submitted for review by March 31, 2018, with one additional technology submitted for review at the end of each month after that. The City's Privacy Team has been tasked with assisting you and your staff with the completion of this process and has already begun working with your designated department team members to provide direction about the Surveillance Impact Report completion process.

Please let me know if you have any questions.

Thank you,

Michael Mattmiller

Chief Technology Officer

Technology	Description	Proposed Review Order
Automated License Plate Recognition (ALPR)	ALPRs are computer-controlled, high-speed camera systems mounted on parking enforcement or police vehicles that automatically capture an image of license plates that come into view and converts the image of the license plate into alphanumeric data that can be used to locate vehicles reported stolen or otherwise sought for public safety purposes and to enforce parking restrictions.	1
Booking Photo Comparison Software (BPCS)	BCPS is used in situations where a picture of a suspected criminal, such as a burglar or convenience store robber, is taken by a camera. The still screenshot is entered into BPCS, which runs an algorithm to compare it to King County Jail booking photos to identify the person in the picture to further investigate his or her involvement in the crime. Use of BPCS is governed by SPD Manual §12.045.	2
Forward Looking Infrared Real-time video (FLIR)	Two King County Sheriff's Office helicopters with Forward Looking Infrared (FLIR) send a real-time microwave video downlink of ongoing events to commanders and other decision-makers on the ground, facilitating specialized radio tracking equipment to locate bank robbery suspects and provides a platform for aerial photography and digital video of large outdoor locations (e.g., crime scenes and disaster damage, etc.).	3

Technology	Description	Proposed Review Order
Undercover/ Technologies	The following groups of technologies are used to conduct sensitive investigations and should be reviewed together. • **Audio recording devices**: A hidden microphone to audio record individuals without their knowledge. The microphone is either not visible to the subject being recorded or is disguised as another object. Used with search warrant or signed Authorization to Intercept (RCW 9A.73.200). • **Camera systems**: A hidden camera used to record people without their knowledge. The camera is either not visible to the subject being filmed or is disguised as another object. Used with consent, a search warrant (when the area captured by the camera is not in plain view of the public), or with specific and articulable facts that a person has or is about to be engaged in a criminal activity and the camera captures only areas in plain view of the public. • **Tracking devices**: A hidden tracking device carried by a moving vehicle or person that uses the Global Positioning System to determine and track the precise location. U.S. Supreme Court v. Jones mandated that these must have consent or a search warrant to be used.	4
Computer-Aided Dispatch (CAD)	CAD is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field.	5

Technology	Description	Proposed Review Order
CopLogic	System allowing individuals to submit police reports on-line for certain low-level crimes in non-emergency situations where there are no known suspects or information about the crime that can be followed up on. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.	6
Hostage Negotiation Throw Phone	A set of recording and tracking technologies contained in a phone that is used in hostage negotiation situations to facilitate communications.	7
Remotely Operated Vehicles (ROVs)	These are SPD non-recording ROVs/robots used by Arson/Bomb Unit to safely approach suspected explosives, by Harbor Unit to detect drowning victims, vehicles, or other submerged items, and by SWAT in tactical situations to assess dangerous situations from a safe, remote location.	8
911 Logging Recorder	System providing networked access to the logged telephony and radio voice recordings of the 911 center.	9
Computer, cellphone and mobile device extraction tools	Forensics tool used with consent of phone/device owner or pursuant to a warrant to acquire, decode, and analyze data from smartphones, tablets, portable GPS device, desktop and laptop computers.	10
Video Recording Systems	These systems are to record events that take place in a Blood Alcohol Concentration (BAC) Room, holding cells, interview, lineup, and polygraph rooms recording systems.	11
Washington State Patrol (WSP) Aircraft	Provides statewide aerial enforcement, rapid response, airborne assessments of incidents, and transportation services in support of the Patrol's public safety mission. WSP Aviation currently manages seven aircraft equipped with FLIR cameras. SPD requests support as needed from WSP aircraft.	12

Technology	Description	Proposed Review Order
Washington State Patrol (WSP) Drones	WSP has begun using drones for surveying traffic collision sites to expedite incident investigation and facilitate a return to normal traffic flow. SPD may then request assistance documenting crash sites from WSP.	13
Callyo	This software may be installed on an officer's cell phone to allow them to record the audio from phone communications between law enforcement and suspects. Callyo may be used with consent or search warrant.	14
I2 iBase	The I2 iBase crime analysis tool allows for configuring, capturing, controlling, analyzing and displaying complex information and relationships in link and entity data. iBase is both a database application, as well as a modeling and analysis tool. It uses data pulled from SPD's existing systems for modeling and analysis.	15
Parking Enforcement Systems	Several applications are linked together to comprise the enforcement system and used with ALPR for issuing parking citations. This is in support of enforcing the Scofflaw Ordinance SMC 11.35.	16
Situational Awareness Cameras Without Recording	Non-recording cameras that allow officers to observe around corners or other areas during tactical operations where officers need to see the situation before entering a building, floor or room. These may be rolled, tossed, lowered or throw into an area, attached to a hand-held pole and extended around a corner or into an area. Smaller cameras may be rolled under a doorway. The cameras contain wireless transmitters that convey images to officers.	17
Crash Data Retrieval	Tool that allows a Collision Reconstructionist investigating vehicle crashes the opportunity to image data stored in the vehicle's airbag control module. This is done for a vehicle that has been in a crash and is used with consent or search warrant.	18

Technology	Description	Proposed Review Order
Maltego	An interactive data mining tool that renders graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the internet.	19

Please let me know if you have any questions.

Thank you,

Michael

City of Seattle

2019 Surveillance Impact Report

CopLogic

Seattle Police Department

City of Seattle

Table of Contents

Submitting Department Memo 3
Surveillance Impact Report ("SIR") overview 5
Privacy Impact Assessment 6
Financial Information 26
Expertise and References 28
Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet 29
Privacy and Civil Liberties Assessment 46
CTO Response 52
Appendix A: Glossary 57
Appendix B: Meeting Notice(s) 59
Appendix C: Meeting Sign-in Sheet(s) 67
Appendix D: Department of Neighborhood Focus Group Notes 92
Appendix E: All Comments Received from Members of the Public 124
Appendix F: Department Responses to Public Inquiries 132
Appendix G: Letters from Organizations or Commissions 136
Appendix H: Comment Analysis Methodology 160
Appendix I: Supporting Policy Documentation 163
Appendix J: CTO Notification of Surveillance Technology 170

City of Seattle

Submitting Department Memo

Memo

Date: April 29, 2019
To: City Council
From: Deputy Chief GarthGreen, Seattle Police Department
Subject: Cover Memo - CopLogic

Description

CopLogic is a crime reporting software tool that allows members of the public to submit police reports online through a web-based interface. CopLogic is a Software as a Service (SaaS) owned and maintained by LexisNexis. SPD utilizes this technology in two ways: 1) An online public interface allows individuals to report a low-level crime in which no known or describable suspect is available, and for which individuals may need proof of police reporting (i.e., for insurance purposes), without waiting for an officer to dispatch and take a report; 2) An online password-protected interface allows retailers to enter information about retail theft on their property in which a suspect is known and suspect information is available.

Purpose

CopLogic allows for the user, either an individual or a retail store, to report crimes at their own convenience. CopLogic is available 24 hours per day, seven days per week. When users decide that they do not need a police officer to respond to the scene, they may still reap the benefits of reporting an incident, for instance, obtaining a case number for insurance purposes or requesting criminal charges for a theft in their business. CopLogic also eliminates the need for individuals to call 9-1-1 to report a crime and have a report taken. In 2017, 14,356 crimes were reported via CopLogic, freeing resources in the 9-1-1 Center, ensuring that 9-1-1 call takers and SPD officers are available for more serious incidents.

Benefits to the Public

CopLogic benefits both the community and the Seattle Police Department by freeing resources in the 9-1-1 center, eliminating the need for patrol officers to respond in person to take some crime reports, and providing community members with a secure, convenient, and timely way to interact with police. Community members also receive a no-cost copy of their police report when they complete their report with the CopLogic system. CopLogic saves over 20,000 patrol officer hours annually, freeing patrol resources for more serious incidents and saving the Department over $1,000,000 each year.

Privacy and Civil Liberties Considerations

During the public comment period, SPD heard concerns about privacy from community members. They raised concerns around the perceived ability for the public to make complaints about specific people or communities through the system, the lack of access to online reporting for marginalized communities,

what kinds of crimes can be reported using the system, how long records are retained, how secure the collected information is, and who has access to the information – particularly what access the vendor, LexisNexis, has to the information collected by the CopLogic system.

By not allowing the community to report crimes with known or describable suspects via the CopLogic system, SPD has mitigated the concerns that the system allows for collection of information and malicious reporting directed at specific individuals or communities. The agreement between SPD and LexisNexis limits the use and storage of all information collected by or on behalf of the City to only purposes used for providing the service in the CopLogic contract and consultant agreement. They are prohibited from using City data or personal information collected by the system to engage or enable another party to engage in marketing or targeted advertising. Additionally, no access or information shall be provided to any employee or agent of any federal immigration agency without prior review and consent of the City. Additionally, per the agreement between SPD and LexisNexis, reports that are generated in the CopLogic system are imported into SPD's records management system and then auto-deleted from the LexisNexis servers after 120 days. Reports that are rejected by the SPD officers who review the reports are deleted immediately and notification is sent to the community member.

SPD acknowledges that there are barriers to online reporting for some community members. The CopLogic system is, like much of the City of Seattle web presence, not translated into other languages. The system requires the reporter to have access to the internet on either a computer or smart phone and have an email address, both of which may not be available to all members of the community, particularly among traditionally marginalized communities and homeless individuals. Kiosk computers have been installed at SPD precincts which allow community members access to CopLogic online reporting, and the system is available from other public-access computers like those available at libraries. The CopLogic online crime reporting system does not replace other methods of contacting SPD for services and reporting crimes. Community members who need services in languages other than English, do not have access to the internet or an email address, or are uncomfortable making a report online are still able to contact SPD via the telephone or by making a report at an SPD Precinct.

Summary

CopLogic is an opt-in online crime reporting system that benefits the community, SPD, the 9-1-1 Center, and the City of Seattle. CopLogic saves over 20,000 patrol officer hours annually, freeing patrol resources for more serious incidents and saving the Department and the City over $1,000,000 each year. Online reporting allows community members to report certain crimes in a secure, convenient, and frees resources in the 9-1-1 Center, ensuring that 9-1-1 call takers are available for more serious incidents. Only authorized SPD personnel can access the information provided by the individuals through the online reporting tool and all activity in the system is logged and auditable. The vendor, LexisNexis, cannot access the information for any reason other than providing SPD with the online reporting services and is not permitted to share the information with any third party.

City of Seattle

Surveillance Impact Report ("SIR") overview

About the Surveillance Ordinance

The Seattle City Council passed Ordinance 125376, also referred to as the "Surveillance Ordinance," on September 1, 2017. SMC 14.18.020.b.1 charges the City's executive with developing a process to identify surveillance technologies subject to the ordinance. Seattle IT, on behalf of the executive, developed and implemented a process through which a privacy and surveillance review is completed prior to the acquisition of new technologies. This requirement, and the criteria used in the review process, are documented in Seattle it policy pr-02, the "surveillance policy".

How this Document is Completed

This document is completed by the requesting department staff, support and coordinated by the Seattle information technology department ("Seattle it"). As Seattle it and department staff complete the document, they should keep the following in mind.

1. Responses to questions should be in the text or check boxes only; all other information (questions, descriptions, etc.) Should **not** be edited by the department staff completing this document.
2. All content in this report will be available externally to the public. With this in mind, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.

Surveillance Ordinance Review Process

The following is a high-level outline of the complete SIR review process.

Upcoming for Review	Initial Draft	Open Comment Period	Final Draft	Working Group	Council Review
The technology is upcoming for review, but the department has not begun drafting the surveillance impact report (SIR).	Work on the initial draft of the SIR is currently underway.	The initial draft of the SIR and supporting materials have been released for public review and comment. During this time, one or more public meetings will take place to solicit feedback.	During this stage the SIR, including collection of all public comments related to the specific technology, is being compiled and finalized.	The surveillance advisory working group will review each SIR's final draft and complete a civil liberties and privacy assessment, which will then be included with the SIR and submitted to Council.	City Council will decide on the use of the surveillance technology, by full Council vote.

City of Seattle

Privacy Impact Assessment

Purpose

A Privacy Impact Assessment ("PIA") is a method for collecting and documenting detailed information collected in order to conduct an in-depth privacy review of a program or project. A PIA asks questions about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. It also requests information about policies, training and documentation that govern use of the technology. The PIA responses are used to determine privacy risks associated with a project and mitigations that may reduce some or all of those risks. In the interests of transparency about data collection and management, the City of Seattle has committed to publishing all PIAs on an outward facing website for public access.

When is a Privacy Impact Assessment Required?

A PIA may be required in two circumstances.

1. When a project, technology, or other review has been flagged as having a high privacy risk.
2. When a technology is required to complete the surveillance impact report process. This is one deliverable that comprises the report.

1.0 Abstract

1.1 Please provide a brief description (one paragraph) of the purpose and proposed use of the project/technology.

CopLogic is crime reporting tool that allows individuals to submit police reports online. SPD utilizes this technology for two purposes: (1) community members may report specific low-level, non-emergency crimes that have occurred within the Seattle city limits, in which there are no known suspects or additional information that would allow for investigation of the crime; and (2) retail businesses that participate in SPD's Retail Theft Program may report low-level thefts that occur in their businesses when they have identified a suspect. CopLogic provides efficient customer service to community members who may need proof of police reporting (i.e., for insurance purposes) without needing to call 9-1-1 then waiting for an officer to respond and take a report. CopLogic frees resources in the 9-1-1 Center, ensuring that 9-1-1 call takers are available for more serious incidents and frees patrol officer resources by eliminating the need for a police officer to be dispatched for the sole purpose of taking a police report.

1.2 Explain the reason the project/technology is being created or updated and why the PIA is required.

CopLogic is an opt-in system; it is used only when an individual chooses to utilize it. However, individuals may enter personally-identifying information about third parties without providing notice to those individuals, and there is no immediate, systemic method to verify the accuracy of information that individuals provide about those third parties.

2.0 Project / Technology Overview

Provide an overview of the project or technology. The overview gives the context and background necessary to understand the purpose, mission and justification for the project / technology proposed.

2.1 Describe the benefits of the project/technology.

CopLogic has two tracks:

1) An online public interface allows individuals to report a crime in which no known suspect is available, and for which individuals may need proof of police reporting (i.e., for insurance purposes), without waiting for an officer to dispatch and take a report.
2) An online password-protected interface allows retailers to enter information about retail theft on their property in which a suspect known and suspect information is available.

CopLogic allows for the user, either an individual or a retail store, to report crimes at their own convenience. CopLogic is available 24 hours per day, seven days per week. When users decide that they do not need a police officer to respond to the scene, they may still reap the benefits of reporting an incident, for instance, obtaining a case number for insurance purposes or requesting criminal charges for a theft in their business. CopLogic also eliminates the need for individuals to call 9-1-1 to report a crime and have a report taken. Last year, 14,356 crimes were reported via CopLogic which is 14,356 fewer 9-1-1 calls taken by the 9-1-1 Center. This technology frees resources in the 9-1-1 Center, ensuring that 9-1-1 call takers are available for more serious incidents.

City of Seattle

2.2 Provide any data or research demonstrating anticipated benefits.

Research Studies:

- Loss Prevention Technology Case Study "*Using Technology to Enhance the Relationship between Loss Prevention and Local Law Enforcement"*
- Travis Taniguchi and Christopher Salvatore, "Citizen Perceptions of Online Crime Reporting Systems," *The Police Chief* 82 (June 2015): 48–52. http://www.policechiefmagazine.org/citizen-perceptions-of-online-crime-reporting-systems/?ref=3e3a108ad4f36c878bb398b470385dcc

Research shows that allowing individuals to report certain non-urgent crimes and for trained retail loss prevention employees to streamline the shoplifting reporting process provided through online tools such as CopLogic delivers benefits to both the department by eliminating the need for patrol officers to respond in person to take such reports, and providing community members with a secure, convenient, and timely way to interact with police.

SPD has collected data about CopLogic's effectiveness since 2012. The use of CopLogic has increased each year, and it saves numerous police hours by eliminating the need for a patrol officer to respond. The data shows:

	Reports	Hours Saved	Money Saved
2012	7,652	11,478	$573,900.00
2013	9,527	14,290	$714,525.00
2014	12,575	18,862	$943,125.00
2015	12,365	18,547	$927,375.00
2016	13,379	20,068	$1,003,425.00
2017	14,356	21,534	$1,076,700.00
2018*	13,571	20,356	$1,017,825.00

*(2018 Data is calculated through the end of October.)

2.3 Describe the technology involved.

CopLogic is a Software as a Service (SaaS) owned and maintained by LexisNexis. It is used in two ways:

1) Public Interface: Individuals wishing to file a report visit Seattle Police Department's Online Reporting page (https://www.seattle.gov/police/need-help/online-reporting) and follow the prompts to enter information about low-level, non-emergency crimes for which no known suspects exist. CopLogic then generates a report and the reporter receives a temporary unique identification number. An SPD employee, the reviewer, verifies that the report is sufficient and complete. If further information or clarification is needed, the reviewer generates a generic email to the reporter, informing them that the report is missing information that must be included before the file is officially submitted, and providing a link to follow for updates. Once a reviewer determines that the report is complete, the information is electronically transferred into SPD's records management system and receives a general offense (GO) number. This GO number is then provided to the reporter for their records and for insurance purposes.
2) Retail Theft Interface: Retailers who participate in the Seattle Police Department's Retail Theft Program and wish to report a theft first contact the Seattle Police Department's non-emergency number to receive a case number. Then, they access the Retail Theft online page with unique password-protected login information and fill out the Retail Theft online report, which includes information about the retailer, the theft, and the suspect. In most circumstances, retailer security has detained the suspect and included copies of identification with the report that they then submit online.

After a report is made into the Public Interface or the Retail Theft Interface, police officers assigned to the Internet and Telephone Reporting Unit (I-TRU) log in to the CopLogic web portal, utilizing individual user log-in IDs, to access the submitted reports. Once the report is screened by an officer in the I-TRU unit, SPD utilizes an integration server to transfer reports generated in the CopLogic tool into SPD's Records Management System.

2.4 Describe how the project or use of technology relates to the department's mission.

SPD's mission is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional, and dependable police services. CopLogic allows for the user, either an individual or a retail store, to report crimes at their own convenience. CopLogic is available 24 hours per day, seven days per week. When users decide that they do not need a police officer to respond to the scene, they may still benefit from reporting an incident, for instance, by quickly obtaining a case number for insurance purposes or requesting criminal charges for a theft in their business. CopLogic also eliminates the need for individuals to call 9-1-1 to report a crime and have a report taken. Last year, 14,356 crimes were reported via CopLogic which is 14,356 fewer 9-1-1 calls taken by the 9-1-1 Center. This technology frees resources in the 9-1-1 Center, ensuring that 9-1-1 call takers, and then patrol officers, are available for more serious incidents.

2.5 Who will be involved with the deployment and use of the project / technology?

SPD reviewers within the I-TRU unit have access to the reports for the purposes of verifying accuracy and initiating the process of transferring the approved reports into the records management system with a case number (as is assigned to all SPD reports).

Additionally, Seattle IT provides client services and operational support for IT technologies and applications. In supporting SPD systems, operational and application services deploy and service SPD technology systems. Details about the IT department are found in the appendix of this SIR.

3.0 Use Governance

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities contracting with the City are bound by restrictions specified in the surveillance ordinance and privacy principles and must provide written procedures for how the entity will comply with any restrictions identified.

3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

CopLogic is used by the public, including retailers, and, thus, its use is triggered whenever an individual instigates the submission of an online report. The SPD reviewer checks the submission for completion and does one of the following:

1) Sends a generic email to the submitter asking for additional information; or
2) Pushes the report to SPD's records management system, providing the report a General Offense ("GO") number, which is then sent back to the submitter.

3.2 List the legal standards or conditions, if any, that must be met before the project / technology is used.

Individuals may use CopLogic to report a crime online when:

1) The crime is within one of these categories of crime:
    a. Property crimes including property destruction, graffiti, car break ins, theft of auto accessories, theft, shoplifting; or
    b. Drug activity, harassing phone calls, credit card fraud, wage theft, identity theft, or lost property
2) The situation is non-emergent
3) The crime occurred within Seattle city limits (exception for identity theft); and
4) No known suspects or information about the crime would allow for additional investigation.

Retailers may use CopLogic to report a retail theft on their property when:

1) The retailer participates in SPD's Retail Theft Program and has obtained a unique login identifier and password;
2) They have detained the suspect;
3) The suspect does not have any outstanding warrants; and
4) They verify the identification of the suspect and upload copies of the suspect's identification, if available.

3.3 Describe the policies and training required of all personnel operating the project / technology, and who has access to ensure compliance with use and management policies.

Only authorized SPD users can access the system, technology, or the data. Access to the application is limited to SPD personnel via password-protected login credentials.

Once data is input by individuals and retail users of CopLogic on the public-facing website, it is accessed and used on SPD's password-protected network.

All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.

SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

ITD client services interaction with SPD systems is governed according to the terms of the 2018 Management Control Agreement (MCA) between ITD and SPD, which states that:

"Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements." This MCA document may be found in Appendix I.

4.0 Data Collection and Use

4.1 Provide details about what information is being collected from sources other than an individual, including other IT systems, systems of record, commercial data aggregators, publicly available data and/or other City departments.

No information is collected from a source other than the individual instigating the submission of a report.

4.2 What measures are in place to minimize inadvertent or improper collection of data?

Before anyone is permitted to file a report online, they are prompted to answer a series of questions to determine if online reporting is appropriate for the event they wish to report. In addition, the Seattle Police Department provides guidelines to individuals reporting an event about what information they will need to submit to file a report online. Finally, an authorized SPD employee reviews each submission before accepting the report to ensure that appropriate and adequate information has been provided.

Retail security collects only information that is necessary to document and investigate the crime as required on the Retail Theft Reporting form. No other information is requested.

4.3 How and when will the project / technology be deployed or used? By whom? Who will determine when the project / technology is deployed and used?

CopLogic is an online portal that is available for individuals to utilize at any time. It was implemented in the fall of 2011.

Retailers have access to a Retail Theft portal with unique password-protected login information.

CopLogic is a Software as a Service. It utilizes server integration so reports can be transferred to SPD's Records Management System.

4.4 How often will the technology be in operation?

The online portal is continuously in operation, so individuals can instigate and submit reports at any time.

4.5 What is the permanence of the installation? Is it installed permanently, or temporarily?

CopLogic is a permanent installation.

4.6 Is a physical object collecting data or images visible to the public? What are the markings to indicate that it is in use? What signage is used to determine department ownership and contact information?

CopLogic is an online portal, not a physical object. As such, the portal is visible to the public when they visit the online page (https://www.seattle.gov/police/need-help/online-reporting), but is not otherwise visible. The online page contains City of Seattle and SPD branding and contact information. There is also specific text on the web page letting the public know what kind of crimes they may report using this technology.

4.7 How will data that is collected be accessed and by whom?

Only authorized SPD users can access the system, technology, or the data. Access to the application is limited to SPD personnel via password-protected login credentials.

Collected data is securely viewed on SPD's password-protected network with access limited to authorized detectives and identified supervisory personnel within the I-TRU unit. Once a reported incident has been reviewed by SPD personnel, it is electronically transferred into the SPD records management system.

All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.

Incidental data access may occur through delivery of technology client services. All ITD employees are required to comply with appropriate regulatory requirements regarding security and background review. Information on the ITD roles that may be associated with client services for City Departments can be found in Appendix I.

ITD client services interaction with SPD systems is governed by the terms of the 2018 Management Control Agreement (MCA) between ITD and SPD. The MCA document may be found in Appendix I.

4.8 If operated or used by another entity on behalf of the City, provide details about access, and applicable protocols.

CopLogic is owned and maintained by Lexis Nexis. There are no data sharing agreements between SPD and any other entities for CopLogic data. Further, the contract between the City and LexisNexis provides that LexisNexis may only "use, transmit, distribute, modify, reproduce, display, and store the City Data solely for the purposes of (i) providing the Services as contemplated in [its contract with the City]; and (ii) enforcing its rights under [the contract]." A link to the LexisNexis privacy policy can be found here: https://risk.lexisnexis.com/privacy-policy

4.9 What are acceptable reasons for access to the equipment and/or data collected?

SPD reviewers must access the reports to check for accuracy and approve reports so that the report can be transferred into SPD's records management system with an appropriately assigned case number. Once the information is entered into the records management system, the information can be accessed by authorized SPD personnel at any time, as it relates to a specific investigation, just as is the case with any information stored within the records management system.

Incidental data access may occur through delivery of technology client services. All ITD employees are required to comply with appropriate regulatory requirements regarding security and background review. Information on the ITD roles associated with client services for City Departments can be found in Appendix I.

ITD client services interaction with SPD systems is governed according to the terms of the 2018 Management Control Agreement between ITD and SPD, which states that:

"Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBIs Criminal Justice Information Services, (CJIS) Security Policy."

The MCA document may be found in Appendix I.

4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

CopLogic data is stored remotely and managed by the technology provider, Lexis Nexis. Lexis Nexis is Privacy Shield Certified and adheres to the RELX Group Privacy Shield Principles. Per Lexis Nexis: "We use a variety of administrative, physical and technical security measures to help safeguard your personal information." Additionally, SPD's contract with Lexis Nexis includes a clause for audit, in which the "Consultant shall permit the City and any other governmental agency funding the Work, to inspect and audit all pertinent books and records."

SPD personnel can only access CopLogic data when authorized and provided a username and password for the system. CopLogic creates an audit log that records all activity in the system with usernames and timestamps.

ITD client services interaction with SPD systems is governed according to the terms of the 2018 Management Control Agreement between ITD and SPD, which states that:

"Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBIs Criminal Justice Information Services, (CJIS) Security Policy."

The MCA document may be found in Appendix I.

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

CopLogic is a web-hosted solution provided by Lexis Nexis and all information entered into the system is stored on the LexisNexis platform. Per Lexis Nexis: "We use a variety of administrative, physical and technical security measures to help safeguard your personal information." Additionally, Lexis Nexis is Privacy Shield Certified and adheres to the RELX Group Privacy Shield Principles.

5.2 How will the owner allow for departmental and other entities, to audit for compliance with legal deletion requirements?

SPD's Audit, Policy and Research Section (APRS) can conduct an audit of the any system at any time. The Office of Inspector General and the federal monitor can also access all data and can audit for compliance at any time.

Additionally, SPD's contract with Lexis Nexis includes a clause for audit, in which the "Consultant shall permit the City and any other governmental agency funding the Work, to inspect and audit all pertinent books and records."

Seattle Information Technology

City of Seattle Information Technology Department

With

Lexis Nexis Risk Solutions

CONSULTANT AGREEMENT

Title: Project Management for Lexis Nexis

AGREEMENT NUMBER: C3-0201-18

This Agreement is made and entered into by and between the City of Seattle ("the City"), a Washington municipal corporation, through its Department of Information Technology as represented by the Chief Technology Officer; and Lexis Nexis Risk Solutions ("Consultant"), a corporation of the State of Pennsylvania, and authorized to do business in the State of Washington.

The purpose of this contract is to provide the City of Seattle with Project Management Services for Lexis Nexis Desk Officer Reporting System Interface Implementation for Mark43 Cobalt RMS. This project is valued less than $52,000.00. As a result, the Department selected this Consultant through Direct Select.

In consideration of the terms, conditions, covenants and performance of the Scope of Work contained herein, the City and Consultant mutually agree as follows:

1. TERM OF AGREEMENT.
The term of this Agreement begins when fully executed by all parties and ends on October 31, 2018 unless amended by written agreement or terminated earlier under termination provisions.

2. TIME OF BEGINNING AND COMPLETION.
The Consultant shall begin the work outlined in Quote 20180427 - "Scope of Work" ("Work") upon receipt of written notice to proceed from the City. The City will acknowledge in writing when the Work is complete. Time limits established under this Agreement shall not be extended because of delays for which the Consultant is responsible, but may be extended by the City, in writing, for the City's convenience or conditions beyond the Consultant's control.

3. SCOPE OF WORK.
The Scope of Work for this Agreement and the time schedule for completion of such Work are described in Attachment A, which is attached to and made a part of this Agreement.

The Work is subject to City review and approval. The Consultant shall confer with the City periodically and prepare and present information and materials (e.g. detailed outline of completed Work) requested by the City to determine the adequacy of the Work or Consultant's progress.

4. EXPANSION FOR NEW WORK.
This Agreement scope may be expanded for new work. Any expansion for New Work (work not specified within the original Scope of Work Section of this Agreement, and/or not specified in the original RFP as intended work for the Agreement) must comply with all the following limitations and requirements: (a) the

1| Page
Project Management for Lexis Nexis
Revised March 2018
Agreement No. C3-0201-18

5.3 What measures will be used to destroy improperly collected data?

SPD policy contains multiple provisions to avoid improperly collecting data. SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a GO Report. SPD Policy 7.090 specifically governs the collection and submission of photographic evidence. Evidence is submitted to the Evidence Unit and associated with a specific GO Number and investigation. And, SPD Policy 7.110 governs the collection and submission of audio recorded statements. It requires that officers state their name, the Department name, the General Offense number, date and time of recording, the name of the interviewee, and all persons present at the beginning of the recording.

Additionally, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

5.4 Which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

Unit supervisors are responsible for ensuring compliance with data retention requirements within SPD. Audit, Policy & Research Section personnel can also conduct audits of all data collection software and systems. Additionally, any appropriate auditor, including the Office of Inspector General and the federal monitor can audit for compliance at any time.

6.0 Data Sharing and Accuracy

6.1 Which entity or entities inside and external to the City will be data sharing partners?

SPD has no data sharing partners for CopLogic. No person, outside of SPD, has direct access to the application or the data and all requests for information from CopLogic are processed based on existing SPD policies, legal guidelines, and as required by law.

As Seattle IT supports the CopLogic system on behalf of SPD, a Management Control Agreement exists between SPD and Seattle IT. The agreement outlines the specifications for compliance, and enforcement related to supporting the CopLogic system through inter-departmental partnership. The MCA can be found in the appendices of this SIR.

Discrete pieces of information obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law.

Data may be shared with outside entities in connection with criminal prosecutions:

- Seattle City Attorney's Office
- King County Prosecuting Attorney's Office
- King County Department of Public Defense
- Private Defense Attorneys
- Seattle Municipal Court
- King County Superior Court
- Similar entities where prosecution is in Federal or other State jurisdictions

Data may be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

Discrete pieces of information collected by CopLogic may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by SPD Policy 12.050 and 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayoral Directive, dated February 6, 2018.

SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the system.

SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the system.

6.2 Why is data sharing necessary?

Data sharing is not an automatic component of CopLogic reporting. Instead, discrete pieces of information gleaned from the reports are shared only within the context of the situations outlined in 6.1.

6.3 Are there any restrictions on non-City data use?

Yes ☒ No ☐

6.3.1 If you answered yes, provide a copy of the department's procedures and policies for ensuring compliance with these restrictions.

Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20, regulating criminal justice information systems. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260 (auditing and dissemination of criminal history record information systems), and RCW Chapter 10.97 (Washington State Criminal Records Privacy Act).

Once disclosed in response to PRA request, there are no restrictions on non-City data use; however, applicable exemptions will be applied prior to disclosure to any requestor who is not authorized to receive exempt content.

6.4 How does the project/technology review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?

Research agreements must meet the standards reflected in SPD Policy 12.055. Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

6.5 Explain how the project/technology checks the accuracy of the information collected. If accuracy is not checked, please explain why.

The CopLogic system does not automatically check for accuracy. Instead, a reviewer from the I-TRU unit ensures that all fields are completed appropriately by those submitting the report before assigning a General Offense number and approving the report. If necessary information has not been included, the reviewer will contact the reporting party to obtain additional information before the data is electronically transferred into SPD's record management system.

6.6 Describe any procedures that allow individuals to access their information and correct inaccurate or erroneous information.

Individuals may request records pursuant to the PRA, and individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

7.0 Legal Obligations, Risks and Compliance

7.1 What specific legal authorities and/or agreements permit and define the collection of information by the project/technology?

SPD's use of CopLogic is governed by legal requirements and policies as outlined in 3.1, 3.2, 3.3, 4.2, 4.6, and 5.3 of this SIR.

7.2 Describe what privacy training is provided to users either generally or specifically relevant to the project/technology.

SPD Policy 12.050 mandates that all employees receive Security Awareness Training (Level 2), and all employees also receive City Privacy Training. All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), many of which contain specific privacy requirements. Any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

7.3 Given the specific data elements collected, describe the privacy risks identified and for each risk, explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy risks may arise when information is collected about citizens, unrelated to a specific incident. These concerns are mitigated by the requirement that all SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.

CopLogic is to be utilized under specific circumstances, as outlined in 3.2 above. Each report is reviewed to ensure both the accuracy of the report, as well as that it meets the requirements of online reporting (again, as outlined in 3.2 above).

Additionally, SMC 14.12 and SPD Policy 6.060 direct all SPD personnel that "any documentation of information concerning a person's sexual preferences or practices, or their political or religious activities must be for a relevant reason and serve a legitimate law enforcement purpose." Additionally, officers must take care "when photographing demonstrations or other lawful political activities. If demonstrators are not acting unlawfully, police can't photograph them."

Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

Finally, see 5.3 for a detailed discussion about procedures related to noncompliance.

7.4 Is there any aspect of the project/technology that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?

The privacy risks outlined in 7.3 above are mitigated by legal requirements and auditing processes that allow for any auditor, including the Office of Inspector General and the federal monitor, to inspect use and deployment of CopLogic.

The largest privacy risk is the un-authorized release of reported information deemed private or offensive in the RCW. To mitigate this risk, the technology falls under the current SPD policies around dissemination of Department data and information reflected in 6.1.

8.0 Monitoring and Enforcement

8.1 Describe how the project/technology maintains a record of any disclosures outside of the department.

Per SPD Policy 12.080, the Crime Records Unit is responsible to receive and record all requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies." Any subpoenas and requests for public disclosure are logged by SPD's Legal Unit. Any action taken, and data released subsequently in response to subpoenas is then tracked through a log maintained by the Legal Unit. Public disclosure requests are tracked through the City's GovQA Public Records Response System, and responses to Public Disclosure Requests, including responsive records provided to a requestor, are retained by SPD for two years after the request is completed.

8.2 What auditing measures are in place to safeguard the information, and policies that pertain to them, as well as who has access to the audit data? Explain whether the project/technology conducts self-audits, third party audits or reviews.

SPD's Audit, Policy and Research Section is authorized to conduct audits of all investigative data collection software and systems. In addition, the Office of Inspector General and the federal monitor can conduct audits of the software, and its use, at any time. Audit data is available to the public via Public Records Request.

Financial Information

Purpose

This section provides a description of the fiscal impact of the surveillance technology, as required by the surveillance ordinance.

1.0 Fiscal Impact

Provide a description of the fiscal impact of the project/technology by answering the questions below.

1.1 Current or potential sources of funding: initial acquisition costs.

Current ☒ potential ☐

Date of initial acquisition	Date of go live	Direct initial acquisition cost	Professional services for acquisition	Other acquisition costs	Initial acquisition funding source
2010	2010	$33,000	N/A	N/A	SPD Budget

Notes:

N/A

1.2 Current or potential sources of funding: on-going operating costs, including maintenance, licensing, personnel, legal/compliance use auditing, data retention and security costs.

Current ☒ potential ☐

Annual maintenance and licensing	Legal/compliance, audit, data retention and other security costs	Department overhead	IT overhead	Annual funding source
$10,365	N/A	N/A	N/A	SPD Budget

Notes:

2018 Cost (after-tax) per the Contracts Renewal Log

1.3 Cost savings potential through use of the technology

SPD has collected data about CopLogic's effectiveness since 2012. The use of CopLogic has increased each year, and it saves numerous police hours. The data shows:

	Reports	Hours Saved	Money Saved
2012	7,652	11,478	$573,900.00
2013	9,527	14,290	$714,525.00
2014	12,575	18,862	$943,125.00
2015	12,365	18,547	$927,375.00
2016	13,379	20,068	$1,003,425.00
2017	14,356	21,534	$1,076,700.00
2018*	13,571	20,356	$1,017,825.00

*(2018 Data is calculated through the end of October.)

1.4 Current or potential sources of funding including subsidies or free products offered by vendors or governmental entities

This question is not applicable.

Expertise and References

Purpose

The following information is provided to ensure that Council has a group of experts to reference while reviewing the completed surveillance impact report ("SIR"). Any individuals or agencies referenced must be made aware ahead of publication that their information has been included. All materials must be available for Council to access or review, without requiring additional purchase or contract.

1.0 Other Government References

Please list any other government bodies that have implemented this technology and can speak to the implementation of this technology.

Agency, municipality, etc.	Primary contact	Description of current use
King County Sheriff's Office	King County Sheriff's Office Communications Center Phone: (206) 296-3311 Fax: (206) 205-7956	King County uses CopLogic similarly to SPD, allowing the public to report specific non-emergency crimes to the Sheriff's Office.

2.0 Academics, Consultants, and Other Experts

Please list any experts in the technology under consideration, or in the technical completion of the service or function the technology is responsible for.

Agency, municipality, etc.	Primary contact	Description of current use
N/A	N/A	N/A

3.0 White Papers or Other Documents

Please list any authoritative publication, report or guide that is relevant to the use of this technology or this type of technology.

Title	Publication	Link
Using Technology to Enhance the Relationship between Loss Prevention and Local Law Enforcement	Loss Prevention Magazine. (Sept-Oct. 2015)	LPPORTAL.COM
Citizen Perceptions of Online Crime Reporting Systems	*The Police Chief* 82 (June 2015): 48–52.	http://www.policechiefmagazine.org/citizen-perceptions-of-online-crime-reporting-systems/?ref=3e3a108ad4f36c878bb398b470385dcc

Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet

Purpose

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit ("RET") in order to:

- Provide a framework for the mindful completion of the SIR in a way that is sensitive to the historic exclusion of vulnerable and historically underrepresented communities. Particularly, to inform the public engagement efforts departments will complete as part of the surveillance impact report.
- Highlight and mitigate any impacts on racial equity from the adoption and the use of the technology.
- Highlight and mitigate any disparate impacts on individuals or vulnerable communities.
- Fulfill the public engagement requirements of the surveillance impact report.

Adaptation of the RET for Surveillance Impact Reports

The RET was adapted for the specific use by the Seattle Information Technology Departments' ("Seattle IT") Privacy Team, the Office of Civil Rights ("OCR"), and Change Team members from Seattle IT, Seattle City Light, Seattle Fire Department, Seattle Police Department, and Seattle Department of Transportation.

Racial Equity Toolkit Overview

The vision of the Seattle Race and Social Justice Initiative ("RSJI") is to eliminate racial inequity in the community. To do this requires ending individual racism, institutional racism and structural racism. The RET lays out a process and a set of questions to guide the development, implementation and evaluation of policies, initiatives, programs, and budget issues to address the impacts on racial equity.

1.0 Set Outcomes

1.1. Seattle City Council has defined the following inclusion criteria in the surveillance ordinance, and they serve as important touchstones for the risks departments are being asked to resolve and/or mitigate. Which of the following inclusion criteria apply to this technology?

☐ The technology disparately impacts disadvantaged groups.
☐ There is a high likelihood that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service.
☒ The technology collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection.
☐ The technology raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice.

1.2 What are the potential impacts on civil liberties through the implementation of this technology? How is the department mitigating these risks?

The potential impacts of this system on civil liberties are minimal. The risk with this technology is that this information could be disseminated for use in ways that could negatively impact peoples' civil liberties. CopLogic is an opt-in system; it is used only when an individual chooses to utilize it. However, individuals may enter personally-identifying information about third parties without providing notice to those individuals, and there is no immediate, systemic method to verify the accuracy of information that individuals provide about those third parties.

Data entered into CopLogic is reviewed by trained SPD personnel. All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.

Additionally, SPD has established policies regarding the dissemination of data in connection with criminal prosecutions, Washington Public Records Act (Chapter 42.56 RCW), and other data sharing.

1.3 What are the risks for racial or ethnicity-based bias through each use or deployment of this technology? How is the department mitigating these risks?

Include a description of any issues that may arise such as algorithmic bias or the possibility for ethnic bias to emerge in people and/or system decision-making.

Because the information received through the CopLogic portal comes from community members there is a risk that racial or ethnicity-based biased information may be entered. All the information entered is screened by authorized and trained SPD personnel. SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

City of Seattle

1.4 Where in the City is the technology used or deployed?

☒ all Seattle neighborhoods

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County.

If possible, please include any maps or visualizations of historical deployments / use.

N/A

1.4.1 What are the racial demographics of those living in this area or impacted by these issues?

The demographics for the City of Seattle: White - 69.5%; Black or African American - 7.9%; Amer. Indian & Alaska Native - 0.8%; Asian - 13.8%; Native Hawaiian & Other Pac. Islander - 0.4; Other race - 2.4%; Two or more races - 5.1%; Hispanic or Latino ethnicity (of any race): 6.6%; Persons of color: 33.7%.

1.4.2 How does the Department to ensure diverse neighborhoods, communities, or individuals are not specifically targeted through the use or deployment of this technology?

This technology is web-based and available for use by anyone within the city of Seattle with access to the internet, including mobile devices.

1.5 How do decisions around data sharing have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

The Aspen Institute on Community Change defines *structural racism* as "…public policies, institutional practices, cultural representations and other norms [which] work in various, often reinforcing ways to perpetuate racial group inequity."[1] Data sharing has the potential to be a contributing factor to structural racism and thus creating a disparate impact on historically targeted communities. In an effort to mitigate this possibility, SPD has established policies regarding the dissemination of data in connection with criminal prosecutions, Washington Public Records Act (Chapter 42.56 RCW), and other authorized researchers.

Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

No person outside of SPD has direct access to the CopLogic data. Data obtained by the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law. See section 6.0 for more details about data sharing.

1.6 How do decisions around data storage and retention have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

Like decisions around data sharing, data storage and retention have similar potential for disparate impact on historically targeted communities. Because the use of this technology is an opt-in decision by its community users, the risks of improper or biased usage are limited. All information, once reviewed by authorized SPD employees, is electronically transferred into SPD's records management system. The SPD employees tasked with this review are bound by SPD policies pertaining to electronic communications, computer and data usage, and bias-based policing.

1.7 What are potential unintended consequences (both negative and positive potential impact)? What proactive steps can you can / have you taken to ensure these consequences do not occur.

The potential unintended consequences include individuals using the CopLogic system incorrectly in attempt to contact SPD (for example: when an emergency response is appropriate), and the dissemination of information through negligence or misconduct (intentional and unintentional). These are mitigated by documentation and function within the public website portal, review of entered information by SPD personnel, and the application of existing SPD policy.

[1] Aspen Institue Roundtable on Community Change. 2008. "Dismantling Structural Racism: A Racial Equity Theory of Change." Washington D.C.: The Aspen Institute.

City of Seattle

2.0 Public Outreach

2.1 Organizations who received a personal invitation to participate.

Please include a list of all organizations specifically invited to provide feedback on this technology.

1. ACLU of Washington	2. Ethiopian Community Center	3. Planned Parenthood Votes Northwest and Hawaii
4. ACRS (Asian Counselling and Referral Service)	5. Faith Action Network	6. PROVAIL
7. API Chaya	8. Filipino Advisory Council (SPD)	9. Real Change
10. API Coalition of King County	11. Friends of Little Saigon	12. SCIPDA
13. API Coalition of Pierce County	14. Full Life Care	15. Seattle Japanese American Citizens League (JACL)
16. CAIR	17. Garinagu HounGua	18. Seattle Neighborhood Group
19. CARE	20. Helping Link	21. Senior Center of West Seattle
22. Central International District Business Improvement District	23. Horn of Africa	24. Seniors in Action
25. Church Council of Greater Seattle	26. International ImCDA	27. Somali Family Safety Task Force
28. City of Seattle Community Police Commission (CPC)	29. John T. Williams Organizing Committee	30. South East Effective Development
31. City of Seattle Community Technology Advisory Board	32. Kin On Community Health Care	33. South Park Information and Resource Center SPIARC
34. City of Seattle Human Rights Commission	35. Korean Advisory Council (SPD)	36. STEMPaths Innovation Network
37. Coalition for Refugees from Burma	38. Latina/o Bar Association of Washington	39. University of Washington Women's Center
40. Community Passageways	41. Latino Civic Alliance	42. United Indians of All Tribes Foundation
43. Council of American Islamic Relations - Washington	44. LELO (Legacy of Equality, Leadership, and Organizing)	45. Urban League
46. East African Advisory Council (SPD)	47. Literacy Source	48. Wallingford Boys & Girls Club
49. East African Community Services	50. Millionair Club Charity	51. Washington Association of Criminal Defense Lawyers
52. Education for All	53. Native American Advisory Council (SPD)	54. Washington Hall
55. El Centro de la Raza	56. Northwest Immigrant Rights Project	57. West African Community Council
58. Entre Hermanos	59. OneAmerica	60. YouthCare
61. US Transportation expertise	62. Local 27	63. Local 2898
64. (SPD) Demographic Advisory Council	65. South Seattle Crime Prevention Coalition (SSCPC)	66. CWAC
67. NAAC		

2.2 Additional Outreach Efforts

Department	Outreach Area	Description
ITD	Social Media Outreach Plan: Twitter	Directed Tweets and Posts related to Open Public Comment Period for Group 2 Technologies, as well as the BKL event.
SPD, SFD, OPCD, OCR, SPL, SDOT, SPR, SDCI, SCL, OLS, Seattle City Council	Social Media Outreach Plan: Twitter	Tweets and Retweets regarding Group 2 comment period and/or BKL event.
ITD	Press Release	Press release sent to several Seattle media outlets.
ITD	Ethnic Media Press Release	Press Release sent to specific ethnic media publications.
ITD	Social Media Outreach Plan: Facebook Event Post	Seattle IT paid for boosted Facebook posts for their BKL event.
ITD	CTAB	Presented and utilized the Community Technology Advisory Board (CTAB) network and listserv for engaging with interested members of the public
ITD	Blog	Wrote and published a Tech Talk blog post for Group 2 technologies, noting the open public comment period, BKL event, and links to the online survey/comment form.
ITD	Technology Videos	Seattle IT worked with the Seattle Channel to produce several short informational/high level introductory videos on group 2 technologies, which were posted on seattle.gov/privacy. And used at a number of Department of Neighborhoods-led focus groups.

2.3 Additional Department Meetings

Department	Date	Meeting Name	Number in Attendance	Description of Engagement
SPD	2/6/2019	South Seattle Crime Prevention Council	8	Deputy Chief GarthGreen presented the three SPD Group 2 surveillance technologies. One-page summaries and event flyer were distributed. DC GarthGreen and Policy Advisor fielded questions about the technologies. Attendees were directed to the public BKL event and seattle.gov/privacy to provide comment. No physical comment sheets were collected at the event.
SPD	2/7/2019	Fabulous Forum	40	Officer Ritter presented this meeting to approximately 40 members of the public. The public meeting flyer was distributed, paired with a brief introduction to the information around SPD's technologies currently open for public comment through 3-5. The Fabulous Forums are designed to provide valuable educational information to the public regarding a variety of topics ranging from the SPD's cultural history, to how the SPD works at enhancing the relationships between Seattle's police and population it serves, employment opportunities, hate crimes education, self defense and much more.
SPD	3/14/2019	East African Advisory Council	7	A brief presentation on SPD's group 2 surveillance technologies was given. One-page overviews of the technologies were handed out as resources in both English and translated into Somali. Attendees were directed to seattle.gov/privacy to provide comments on the technologies.
SPD	2/19/2019	NA		East African Community Senior Lunch
SPD	2/28/2019	East Precinct Advisory Council at Seattle University	17	A high level overview of the Surveillance Ordinance was provided. A brief introduction to SPD's group 2 technologies (CopLogic, CAD, 911 Logging Recorder) was also provided. One page overviews of each technology were distributed and attendees were directed to seattle.gov/privacy to provide public comment on the technology.

2.3 Scheduled public meeting(s).

Meeting notes, sign-in sheets, all comments received, and questions from the public will be included in Appendix B, C, D, E, F, G, H and I. Comment analysis will be summarized in section 3.0 Public Comment Analysis.

Location	Bertha Knight Landes Room, 1st Floor City Hall 600 4th Avenue, Seattle, WA 98104
Time	February 27, 2018; 6 p.m. – 8 p.m.
Capacity	100+
Link to URL Invite	BKL Event Invitation

City of Seattle

2.4 Scheduled Focus Group Meeting(s)

Meeting 1

Community Engaged	Council on American-Islamic Relations - Washington (CAIR-WA)
Date	Thursday, February 21, 2019

Meeting 2

Community Engaged	Entre Hermanos
Date	Thursday, February 28, 2019

Meeting 3

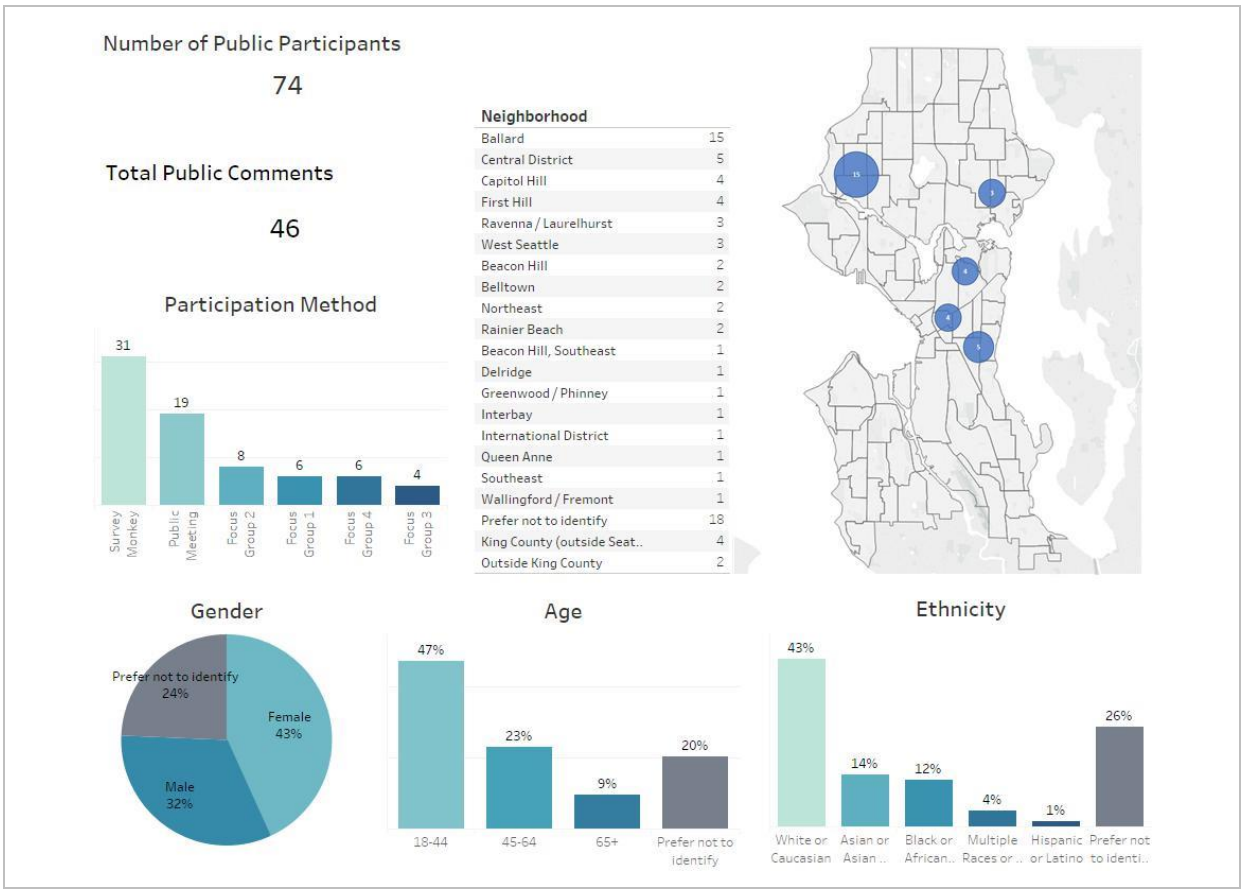
Community Engaged	Byrd Barr Place
Date	Thursday, February 28, 2019

Meeting 4

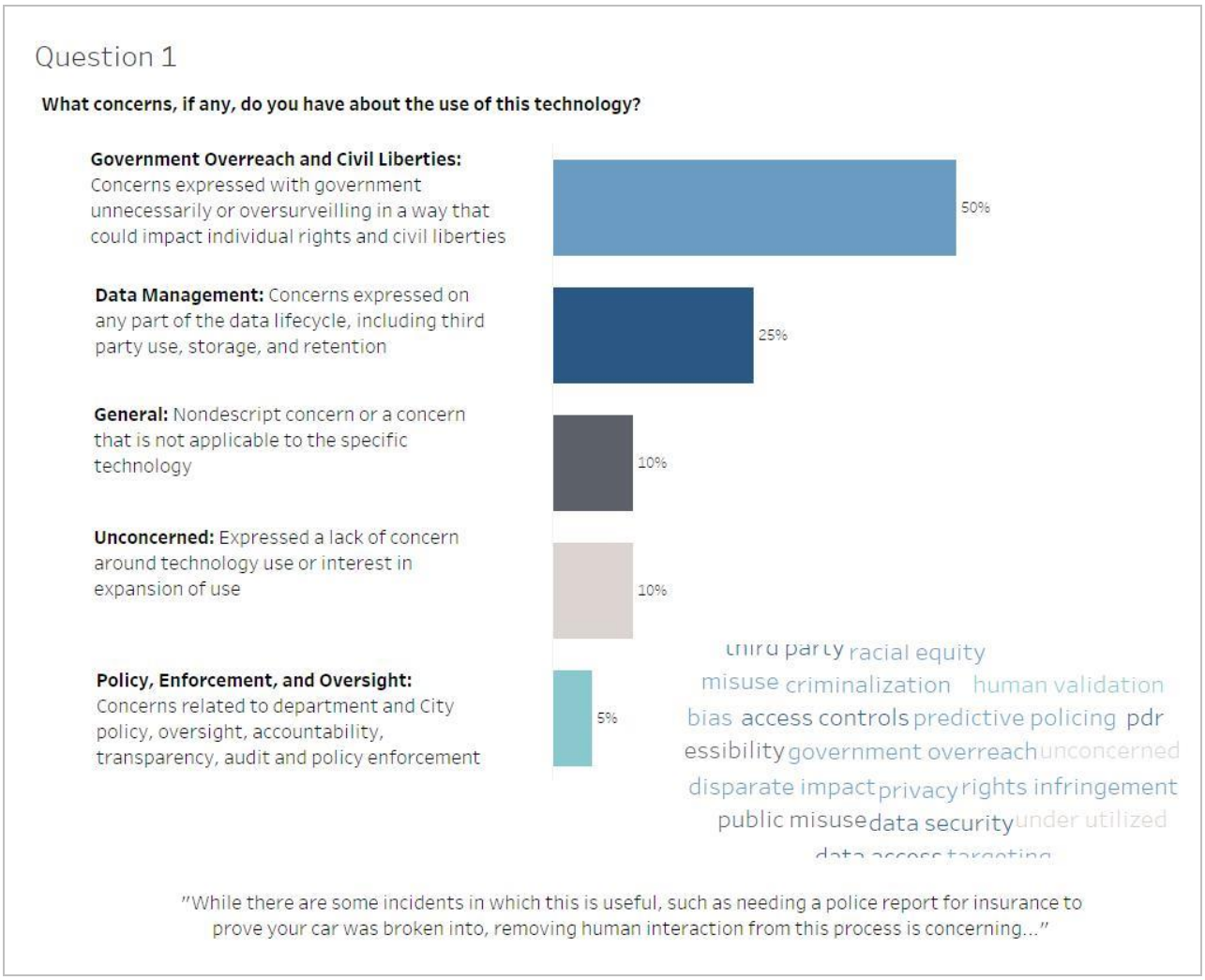
Community Engaged	Friends of Little Saigon
Date	Wednesday, February 27, 2019

3.0 Public Comment Analysis

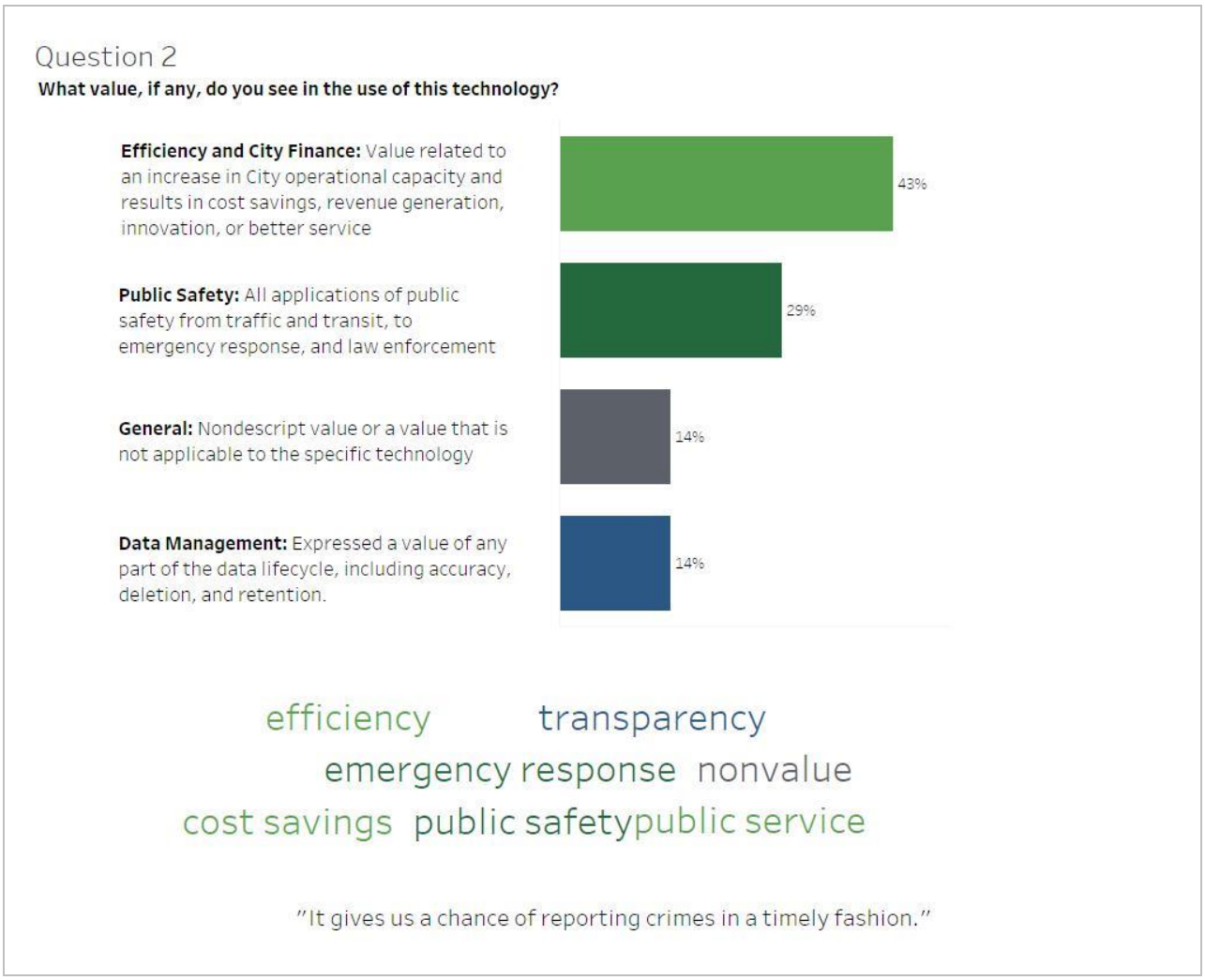
3.1 Summary of Response Volume and Demographic Information



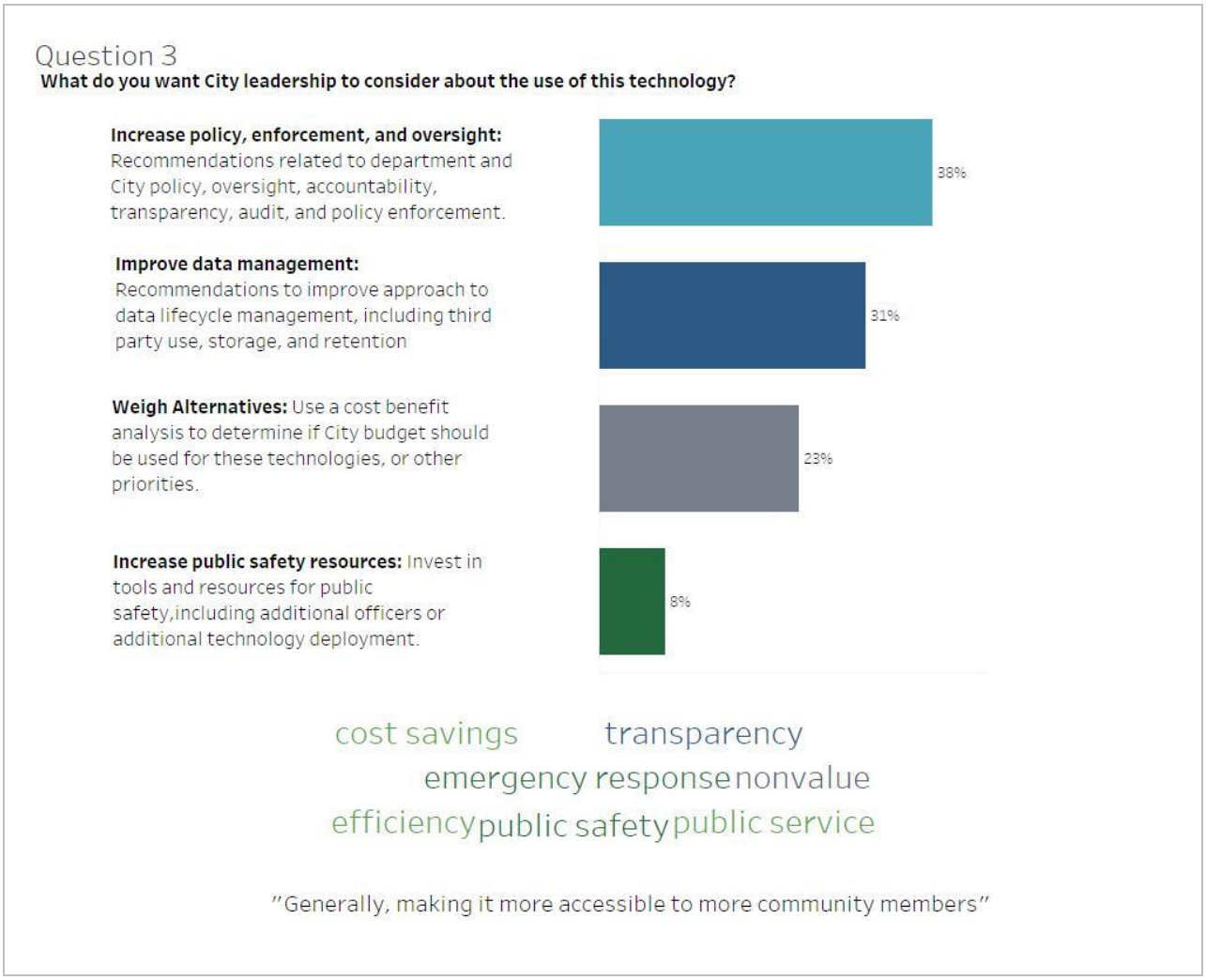
3.2 Question One: What concerns, if any, do you have about the use of this technology?



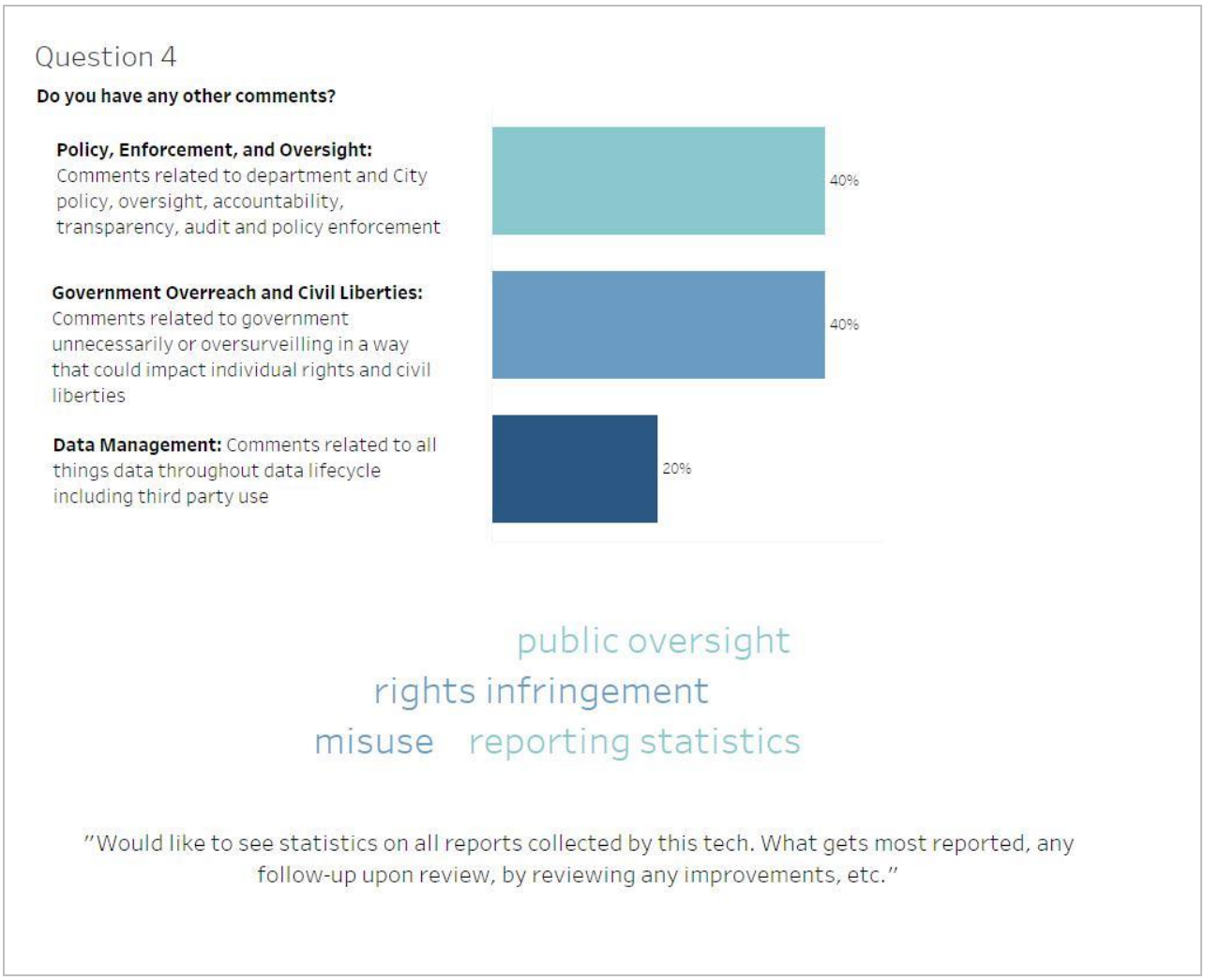
3.3 Question Two: What value, if any, do you see in the use of this technology?



3.4 Question Three: What do you want City leadership to consider about the use of this technology?



3.5 Question Four: Do you have any other comments?



4.0 Equity Annual Reporting

4.1 What metrics for this technology be reported to the CTO for the annual equity assessments?

The Seattle Police Department is currently working to finalize these metrics.

City of Seattle

Privacy and Civil Liberties Assessment

Purpose

This section shall be completed after public engagement has concluded and the department has completed the racial equity toolkit section above. The privacy and civil liberties assessment is completed by the community surveillance working group ("working group"), per the surveillance ordinance which states that the working group shall:

"Provide to the executive and the City Council a privacy and civil liberties impact assessment for each SIR that must be included with any departmental request for surveillance technology acquisition or in-use approval. The impact assessment shall include a description of the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities. The CTO shall share with the working group a copy of the SIR that shall also be posted during the period of public engagement. At the conclusion of the public engagement period, the CTO shall share the final proposed SIR with the working group at least six weeks prior to submittal of the SIR to Council for approval. The working group shall provide its impact assessment in writing to the executive and the City Council for inclusion in the SIR within six weeks of receiving the final proposed SIR. If the working group does not provide the impact assessment before such time, the working group must ask for a two-week extension of time to City Council in writing. If the working group fails to submit an impact statement within eight weeks of receiving the SIR, the department and City Council may proceed with ordinance approval without the impact statement."

Working Group Privacy and Civil Liberties Assessment

The Working Group's Privacy and Civil Liberties Impact Assessment for this technology is below, and is also included in the Ordinance submission package, available as an attachment.

From: Seattle Community Surveillance Working Group (CSWG) To: Seattle Chief Technology Officer

Date: July 7, 2019

Re: Privacy and Civil Liberties Impact Assessment for CopLogic

Executive Summary

On June 4, 2019, the CSWG received the Surveillance Impact Report (SIR) for CopLogic, a surveillance technology included in Group 2 of the Seattle Surveillance Ordinance technology review process. This document is CSWG's Privacy and Civil Liberties Impact Assessment for this technology as set forth in SMC 14.18.080(B)(1), which we provide for inclusion in the final SIR submitted to the City Council.

This document first provides our recommendations to the Council, then provides background information, key concerns, and outstanding questions on CopLogic technology.

Our assessment of CopLogic focuses on three key issues rendering protections around this technology inadequate:

1. There are no specific policies regarding retention of data collected by CopLogic or LexisNexis, and now such data will be integrated into SPD's future Records Management System, Mark43.
2. The retail track of CopLogic raises significant civil liberties concerns, including the potential for retailers to obtain and enter identifying information into CopLogic on the basis of mere suspicion of criminality, without conviction or due process.
3. LexisNexis is not clearly prohibited from retaining CopLogic data or sharing it with third parties.

Recommendations

The Council should adopt clear and enforceable rules that ensure, at a minimum, the following:

1. CopLogic data may be used only for purposes of allowing community members to file police reports or investigating and, as appropriate, prosecuting crimes.
2. The contract between the City of Seattle and LexisNexis must include the following minimum provisions:
   a. LexisNexis may not use CopLogic data for any purpose other than providing the CopLogic tool to the City of Seattle and interfacing it with Mark43.
   b. LexisNexis must immediately delete all CopLogic data after that data has been transferred to SPD's records management system (RMS). LexisNexis must delete all CopLogic data within 30 days of its creation regardless of whether such a transfer has taken place.
   c. LexisNexis must not share CopLogic data with any third party.
   d. LexisNexis and any third party that has access to CopLogic data must be held to the same purpose and use restrictions as SPD.

3. The retail track of CopLogic must be discontinued. Retailers should still be allowed to access and use CopLogic to provide information as any other member of the public would.

Background

CopLogic (otherwise known as the LexisNexis Desk Officer Reporting System)[1] is a crime reporting software tool owned and maintained by LexisNexis, and used by the Seattle Police Department (SPD) to allow members of the public to submit police reports online through a web- based interface. CopLogic targets two types of users:

1. Individuals who wish to report a crime in which no known suspect is available, and for which they may need proof of police reporting (e.g., for insurance purposes). These individuals can report crimes via an online public interface without waiting for an officer to dispatch and take a report.
2. Retail businesses that participate in SPD's Retail Theft Program, which can report low-level thefts occurring in their businesses when they suspect an individual of shoplifting, via an online password-protected interface.

This technology is used by SPD to reduce the need for a police officer to be dispatched for the sole purpose of taking a police report, freeing up resources in SPD's 9-1-1 Center. Data collected by the CopLogic system is transferred to SPD's records management system, but may also be retained in the CopLogic system itself.

While SPD states that it does not allow members of the public (the first type of user) to report crimes with known or describable suspects via CopLogic, retailers participating in SPD's Retail Theft Program (the second type of user) can still do so.

Key Concerns

1. **There are no specific policies regarding retention of data collected by CopLogic or LexisNexis, and how such data will be integrated into SPD's RMS, Mark43.** While the contract between the City of Seattle and LexisNexis for CopLogic itself has not been provided, neither the contract between the City of Seattle and LexisNexis for interfacing that tool with Mark43 nor LexisNexis's Privacy Policy appear to contain restrictions on how long CopLogic/LexisNexis retains collected data. While a memo from SPD Deputy Chief Garth Green[2] (dated April 29, 2019) states that once reports generated in the CopLogic system are imported into SPD's records management system, they are "auto-deleted from the LexisNexis servers after 120 days," there is no specific, enforceable policy or contractual provision provided that supports this deletion. Confusingly, the "Data Retention" section on page 154 of

[1] https://risk.lexisnexis.com/products/desk-officer-reporting-system

[2] Submitting Department Memo, Surveillance Impact Report, CopLogic, SPD, page 3-4.

the SIR introduces the terms "exported report," "approved report," "pending report," and "rejected report" and suggests different associated retention periods, with no further context defining these different types of reports or clear policies enshrining the different retention periods.[3] Finally, there is a lack of clarity on how the CopLogic data will be integrated with and analyzed within Mark43, when it is implemented, and to which third parties it might be made available.

2. **The retail track of CopLogic raises significant civil liberties concerns, including the potential for retailers to obtain and enter identifying information into CopLogic on the basis of mere suspicion of criminality, without conviction or due process.** This raises civil liberties concerns around due process, because individuals merely suspected of committing a crime or infraction will be automatically entered into a law enforcement database, with no application of any legal standard, by a private entity, with no due process or even notice. By blurring the line between private entities and law enforcement, the retail track of CopLogic also raises concerns of mission creep and misuse. It is unclear what training retailers are required to have before acquiring a CopLogic login. And because consumer racial profiling by retailers is a widespread and well-documented practice, it is likely that people of color will be disproportionately apprehended and entered via the retail track of CopLogic.[4,5]
3. **LexisNexis is not clearly prohibited from retaining CopLogic data or sharing it with third parties.** It is not clear what data CopLogic retains, if any, after SPD has imported it into its RMS—no contract for the CopLogic tool itself has been provided in the SIR. The provided contract between City of Seattle and LexisNexis for interfacing CopLogic with Mark43 actually allows sharing of the CopLogic data with third parties for purposes of fulfilling the contract, but it's not clear why LexisNexis would need to do that—so such sharing should be prohibited.[6]

[3] Appendix I: Supporting Policy Documentation, Surveillance Impact Report, CopLogic, page 154.
[4] https://www.aclu.org/blog/racial-justice/race-and-criminal-justice/shopping-while-black-harms-go-deeper-you-think
[5] Pittman, C. 2017. "Shopping while Black": Black consumers' management of racial stigma and racial profiling in retail settings.
Journal of Consumer Culture. https://doi.org/10.1177/1469540517717777
[6] Contract between City of Seattle Information Technology Department with LexisNexis (Agreement number C3-0201-18). Clause 27: "Data Use". Available at:
http://www.seattle.gov/Documents/Departments/Tech/Lexis_Nexis_Consutlant_Agreement.pdf

Outstanding Questions

The following information should be included in an update to the CopLogic SIR:

1. Is there a written contract for the provision of the CopLogic tool to the City of Seattle? If so, that should be included in the SIR, and if not, there should be one.
2. Are there written and enforceable data retention policies restricting LexisNexis's retention of CopLogic data?
3. Are there written and enforceable policies restricting LexisNexis from sharing CopLogic data with third parties?
4. What training do retailers receive, if any, prior to participating in the retailer track of CopLogic?
5. Is there any way to verify or correct inaccurate information entered into the CopLogic system?
6. How will CopLogic data be integrated with Mark43?

The answers to these questions can further inform the content of any binding policy the Council chooses to include in an ordinance on this technology, as recommended above.

City of Seattle

CTO Response

Memo

Date: 11/17/2020

To: Seattle City Council, Transportation and Utilities Committee

From: Saad Bashir

Subject: CTO Response to the Surveillance Working Group CopLogic SIR Review

---

To the Council Transportation and Utilities Committee Members,

I look forward to working together with Council and City departments to ensure continued transparency about the use of surveillance technologies and finding a mutually agreeable means to use technology to improve City services while protecting the privacy and civil rights of the residents we serve. Specific concerns in the Working Group comments about CopLogic are addressed in the attached document.

As provided in the Surveillance Ordinance, SMC 14.18.080, this memo outlines the Chief Technology Officer's (CTO's) response to the Surveillance Working Group assessment on the Surveillance Impact Report for Seattle Police Department's CopLogic.

Background

The Information Technology Department (ITD) is dedicated to the Privacy Principles and Surveillance Ordinance objectives to provide oversight and transparency about the use and acquisition of specialized technologies with potential privacy and civil liberties impacts. All City departments have a shared mission to protect lives and property while balancing technology use and data collection with negative impacts to individuals. This requires ensuring the appropriate use of privacy invasive technologies through technology limitations, policy, training and departmental oversight.

The CTO's role in the SIR process has been to ensure that all City departments are compliant with the Surveillance Ordinance requirements. As part of the review work for surveillance technologies, ITD's Privacy Office has facilitated the creation of the Surveillance Impact Report documentation, including collecting comments and suggestions from the Working Group and members of the public about these technologies. IT and City departments have also worked collaboratively with the Working Group to answer additional questions that came up during their review process.

Technology Purpose

CopLogic is crime reporting tool that allows individuals to submit police reports online. SPD utilizes this technology for two purposes: (1) community members may report specific low-level, non-emergency crimes that have occurred within the Seattle city limits, in which there are no known suspects or additional information that would allow for investigation of the crime; and (2) retail businesses that participate in SPD's Retail Theft Program may report low-level thefts that occur in their businesses when they have identified a suspect. CopLogic provides efficient customer service to community members who may need proof of police reporting (i.e., for insurance purposes) without needing to call 9-1-1 then waiting for an officer to respond and take a report. CopLogic frees resources in the 9-1-1 Center,

ensuring that 9-1-1 call takers are available for more serious incidents and frees patrol officer resources by eliminating the need for a police officer to be dispatched for the sole purpose of taking a police report. Last year, 14,356 crimes were reported via CopLogic which is 14,356 fewer 9-1-1 calls taken by the 9-1-1 Center.

Working Group Concerns

In their review, the Working Group has raised concerns about these devices being used in a privacy impacting way, including data retention and sharing, and civil liberties concerns raised by retailer use, and integrations with other SPD systems. Their specific concerns are:

1. Lack of specific policies regarding retention of data collected by CopLogic
2. Significant civil liberties concerns regarding the retail track of CopLogic
3. Lack of prohibition about LexisNexis retaining CopLogic data or sharing it with third parties.

We believe that policy, training and technology limitations enacted by Seattle Police Department provide adequate mitigation for the potential privacy and civil liberties concerns raised by the Working Group about the use of this important operational technology. Details about this are provided below:

Response to Specific Concerns: CopLogic

Concern: Lack of specific policies regarding retention of data collected by CopLogic.

CTO Assessment: We believe that there is sufficient policy, technical controls and security measures in place to manage the data collected, retained, and deleted through this system. SPD has adequately addressed the policies and practices in place regarding data retention for the information collected through CopLogic. Data collected through the CopLogic system is reviewed and validated by detectives and assigned personnel in the course of criminal investigations. Police policy, the federal monitor, and Office of Inspector General are included in the list of auditing entities that provide oversight to ensure compliance. In addition to the access controls and compliance assurance measures, SPD follows the state legal requirements for retaining data. The retention of data collected by SPD is governed by Washington State law and may be found here
https://www.sos.wa.gov/_assets/archives/recordsmanagement/law-enforcement-records-retention-schedule-v.7.2-(january-2017).pdf

SIR Response:
Section 4.7: How will data that is collected be accessed and by whom?
Collected data is securely viewed on SPD's password-protected network with access limited to authorized detectives and identified supervisory personnel within the I-TRU unit. Once a reported incident has been reviewed by SPD personnel, it is electronically transferred into the SPD records management system.

Section 5.4: Which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?
Unit supervisors are responsible for ensuring compliance with data retention requirements within SPD. Audit, Policy & Research Section personnel can also conduct audits of all data collection software and systems. Additionally, any appropriate auditor, including the Office of Inspector General and the federal monitor can audit for compliance at any time.

Concern: Significant civil liberties concerns regarding the retail track of CopLogic

CTO Assessment: CopLogic provides a means for retail owners, who participate in SPD's Retail Theft Program, to report a variety of criminal activities through an online reporting portal. The SIR outlines how this information is validated through the investigative process, so that information provided through the system is reviewed and validated by trained SPD investigative personnel. This important step mitigates the potential for bias or civil liberties infringement through raw information provided by residents into CopLogic.

SIR Response:
Section 4.9: What are acceptable reasons for access to the equipment and/or data collected?
SPD reviewers must access the reports to check for accuracy and approve reports so that the report can be transferred into SPD's records management system with an appropriately assigned case number. Once the information is entered into the records management system, the information can be accessed by authorized SPD personnel at any time, as it relates to a specific investigation, just as is the case with any information stored within the records management system.

Section 3.1: Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

CopLogic is used by the public, including retailers, and, thus, its use is triggered whenever an individual instigates the submission of an online report. The SPD reviewer checks the submission for completion and does one of the following:

3) Sends a generic email to the submitter asking for additional information; or
4) Pushes the report to SPD's records management system, providing the report a General Offense ("GO") number, which is then sent back to the submitter.

Section 3.2: Individuals may use CopLogic to report a crime online when:

5) The crime is within one of these categories of crime:
    a. Property crimes including property destruction, graffiti, car break ins, theft of auto accessories, theft, shoplifting; or
    b. Drug activity, harassing phone calls, credit card fraud, wage theft, identity theft, or lost property
6) The situation is non-emergent
7) The crime occurred within Seattle city limits (exception for identity theft); and
8) No known suspects or information about the crime would allow for additional investigation.

Retailers may use CopLogic to report a retail theft on their property when:

5) The retailer participates in SPD's Retail Theft Program and has obtained a unique login identifier and password;
6) They have detained the suspect;
7) The suspect does not have any outstanding warrants; and
8) They verify the identification of the suspect and upload copies of the suspect's identification, if available.

Concern: LexisNexis is not clearly prohibited from retaining CopLogic data or sharing it with third parties.

CTO Assessment: The information provided through CopLogic is reviewed through the criminal investigative process. Data use policies and limitations to data access is detailed in the SIR responses below. There are no data sharing partners for this information and all information is used and accessed by SPD personnel for investigative purposes. Discrete pieces of information may be shared through the criminal prosecution process with appropriate entities, and through the Washington Public Records Act as outlined in the SIR responses excerpted below:

SIR Response:
Section 3.3: Describe the policies and training required of all personnel operating the project / technology, and who has access to ensure compliance with use and management policies.

- Only authorized SPD users can access the system, technology, or the data. Access to the application is limited to SPD personnel via password-protected login credentials.
- Once data is input by individuals and retail users of CopLogic on the public-facing website, it is accessed and used on SPD's password-protected network.

Section 6.1: Which entity or entities inside and external to the City will be data sharing partners?

- SPD has no data sharing partners for CopLogic. No person, outside of SPD, has direct access to the application or the data and all requests for information from CopLogic are processed based on existing SPD policies, legal guidelines, and as required by law.
- As Seattle IT supports the CopLogic system on behalf of SPD, a Management Control Agreement exists between SPD and Seattle IT. The agreement outlines the specifications for compliance, and enforcement related to supporting the CopLogic system through inter-departmental partnership. The MCA can be found in the appendices of this SIR.
- Discrete pieces of information obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law.
- Data may be shared with outside entities in connection with criminal prosecutions:
    - Seattle City Attorney's Office
    - King County Prosecuting Attorney's Office
    - King County Department of Public Defense
    - Private Defense Attorneys
    - Seattle Municipal Court
    - King County Superior Court
    - Similar entities where prosecution is in Federal or other State jurisdictions

- Data may be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.
- Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."
- Discrete pieces of information collected by CopLogic may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies

investigating criminal activity as governed by SPD Policy 12.050 and 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayoral Directive, dated February 6, 2018.

- SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the system.
- SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the system.

Appendix A: Glossary

Accountable: (taken from the racial equity toolkit.) Responsive to the needs and concerns of those most impacted by the issues you are working on, particularly to communities of color and those historically underrepresented in the civic process.

Community outcomes: (taken from the racial equity toolkit.) The specific result you are seeking to achieve that advances racial equity.

Contracting equity: (taken from the racial equity toolkit.) Efforts to achieve equitable racial outcomes in the way the City spends resources, including goods and services, consultants and contracting.

DON: "department of neighborhoods."

Immigrant and refugee access to services: (taken from the racial equity toolkit.) Government services and resources are easily available and understandable to all Seattle residents, including non-native English speakers. Full and active participation of immigrant and refugee communities exists in Seattle's civic, economic and cultural life.

Inclusive outreach and public engagement: (taken from the racial equity toolkit.) Processes inclusive of people of diverse races, cultures, gender identities, sexual orientations and socio-economic status. Access to information, resources and civic processes so community members can effectively engage in the design and delivery of public services.

Individual racism: (taken from the racial equity toolkit.) Pre-judgment, bias, stereotypes about an individual or group based on race. The impacts of racism on individuals including white people internalizing privilege, and people of color internalizing oppression.

Institutional racism: (taken from the racial equity toolkit.) Organizational programs, policies or procedures that work to the benefit of white people and to the detriment of people of color, usually unintentionally or inadvertently.

OCR: "Office of Civil Rights."

Opportunity areas: (taken from the racial equity toolkit.) One of seven issue areas the City of Seattle is working on in partnership with the community to eliminate racial disparities and create racial equity. They include: education, health, community development, criminal justice, jobs, housing, and the environment.

Racial equity: (taken from the racial equity toolkit.) When social, economic and political opportunities are not predicted based upon a person's race.

Racial inequity: (taken from the racial equity toolkit.) When a person's race can predict their social, economic, and political opportunities and outcomes.

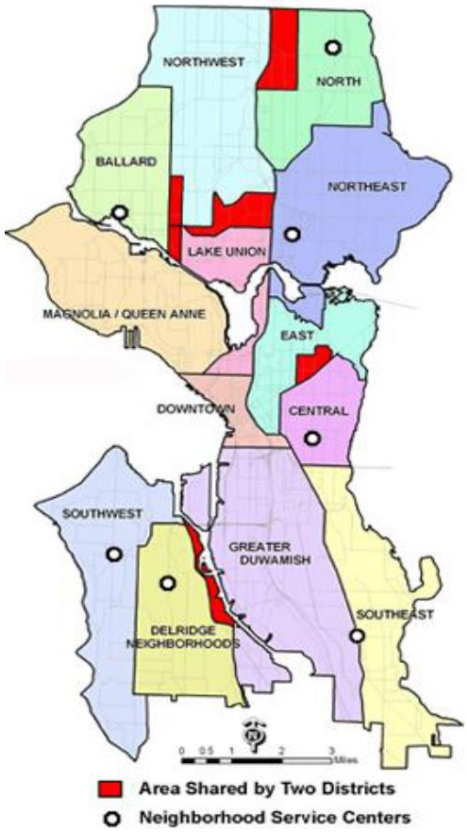
RET: "racial equity toolkit"

Seattle neighborhoods: (taken from the racial equity toolkit neighborhood.) Boundaries defined for the purpose of understanding geographic areas in Seattle.

Stakeholders: (taken from the racial equity toolkit.) Those impacted by proposed policy, program, or budget issue who have potential concerns or issue expertise. Examples might include: specific racial/ethnic groups, other institutions like Seattle housing authority, schools, community-based organizations, change teams, City employees, unions, etc.

Structural racism: (taken from the racial equity toolkit.) The interplay of policies, practices and programs of multiple institutions which leads to adverse outcomes and conditions for communities of color compared to white communities that occurs within the context of racialized historical and cultural conditions.

Surveillance ordinance: Seattle City Council passed ordinance 125376, also referred to as the "surveillance ordinance."



SIR: "surveillance impact report", a document which captures the fulfillment of the Council-defined surveillance technology review process, as required by ordinance 125376.

Workforce equity: (taken from the racial equity toolkit.) Ensure the City's workforce diversity reflects the diversity of Seattle.

City of Seattle

Appendix B: Meeting Notice(s)

City Surveillance Technology Fair

February 27, 2018

6:00 p.m. – 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Join us for a public meeting to comment on a few of the City's surveillance technologies:

Seattle City Light
- Binoculars
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation
- Acyclica

Seattle Fire Department
- Computer Aided Dispatch

Seattle Police Department
- 911 Call Logging Recorder
- Computer Aided Dispatch
- CopLogic

Can't join us in person?

Visit www.seattle.gov/privacy to leave an online comment or send your comment to **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** The Open Comment period is from **February 5 - March 5, 2019.**

Please let us know at Surveillance@seattle.gov if you need any accommodations. For more information, visit Seattle.gov/privacy.

Surveys, sign-in sheets and photos taken at this event are considered a public record and may be subject to public disclosure. For more information see the Public Records Act RCW Chapter 42.56 or visit Seattle.gov/privacy. All comments submitted will be included in the Surveillance Impact Report.

City of Seattle

Giám Sát Thành Phố
Hội Chợ Công Nghệ

ngày 27 tháng 2 năm 2019
6 :00 giờ chiều – 8:00 giờ chiều
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Hãy tham gia cuộc họp công cộng cùng chúng tôi để nhận xét về một số công nghệ giám sát của Thành phố:

Seattle City Light
- Ống nhòm quan sát
- Sensorlink Ampstik
- Đồng hồ đo máy biến áp của Sensorlink

Seattle Department of Transportation (Sở Giao Thông Vận Tải Seattle)
- Acyclica

Seattle Fire Department (Sở Phòng Cháy Chữa Cháy Seattle)
- Hệ Thống Thông Tin Điều Vận Có Máy Tính Trợ Giúp

Seattle Police Department (Sở Cảnh Sát Seattle)
- Hệ Thống Ghi Âm Cuộc Gọi 911
- Hệ Thống Thông Tin Điều Vận Có Máy Tính Trợ Giúp
- CopLogic

Quý vị không thể tới tham dự trực tiếp cùng chúng tôi?

Hãy truy cập www.seattle.gov/privacy và để lại nhận xét trực tuyến hoặc gửi ý kiến của quý vị tới **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** Giai đoạn Góp Ý Mở từ **Ngày 5 tháng 2 - Ngày 5 tháng 3 năm 2019.**

Vui lòng thông báo cho chúng tôi tại Surveillance@seattle.gov nếu quý vị cần bất kỳ điều chỉnh nào. Để có thêm thông tin, hãy truy cập Seattle.gov/privacy.

Các khảo sát, danh sách đăng ký và ảnh chụp tại sự kiện này được coi là thông tin công cộng và có thể được tiết lộ công khai. Để biết thêm thông tin, hãy tham khảo Public Records Act (Đạo Luật Hồ Sơ Công Cộng) RCW Chương 42.56 hoặc truy cập Seattle.gov/privacy. Tất cả các ý kiến đóng góp mà quý vị gửi đến sẽ được đưa vào Báo Cáo Tác Động Giám Sát.

City of Seattle

Eksibisyon ng Teknolohiya Sa Pagmamatyag sa Lungsod

Pebrero 27, 2019

6:00 p.m. - 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Samahan kami para sa isang pampublikong pagpupulong upang magbigay ng komento sa ilan sa mga teknolohiya sa pagmamanman ng Lungsod:

Seattle City Light
- Mga Binocular
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation (Departamento ng Transportasyon ng Seattle)
- Acyclica

Seattle Fire Department (Departamento para sa Sunog ng Seattle)
- Pagdispatsa sa Tulong ng Computer

Seattle Police Department (Departamento ng Pulisya ng Seattle)
- Rekorder ng Pagtawag sa 911
- Pagdispatsa sa Tulong ng Computer
- CopLogic

Hindi kami masasamahan nang personal?

Bumisita sa www.seattle.gov/privacy upang mag-iwan ng online na komento o ipadala ang iyong komento sa **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** Ang panahon ng Bukas na Pagkomento ay sa **Pebrero 5 - Marso 5, 2019.**

Mangyaring ipaalam sa amin sa Surveillance@seattle.gov kung kailangan mo ng anumang tulong. Para sa higit pang impormasyon, bumisita sa Seattle.gov/privacy.

Itinuturing na pampublikong rekord ang mga survey, papel sa pag-sign-in at mga larawan na makukuha sa pangyayaring ito at maaaring mapasailalim sa paghahayag sa publiko. Para sa higit pang impormasyon, tingnan ang Public Records Act (Batas sa Mga Pampublikong Rekord) RCW Kabanata 42.56 o bumisita sa Seattle.gov/privacy. Isasama ang lahat ng isinumiteng komento sa Surveillance Impact Report (Ulat sa Epekto ng Pagmamanman).

City of Seattle

Feria de tecnología de vigilancia ciudadana

27 febrero de 2019

De 6:00 p. m. a 8:00 p. m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Acompáñenos en la reunión pública para dar su opinión sobre algunas de las tecnologías de vigilancia de la ciudad:

Seattle City Light
- Binoculars
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation (Departamento de Transporte de Seattle)
- Acyclica

Seattle Fire Department (Departamento de Bomberos de Seattle)
- Computer Aided Dispatch

Seattle Police Department (Departamento de Policía de Seattle)
- 911 Call Logging Recorder
- Computer Aided Dispatch
- CopLogic

¿No puede asistir en persona?

Visite www.seattle.gov/privacy para dejar un comentario en línea o enviar sus comentarios a **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** El período de comentarios abiertos es desde el **5 de febrero al 5 de marzo de 2019.**

Avísenos en Surveillance@seattle.gov si necesita adaptaciones especiales. Para obtener más información, visite seattle.gov/privacy.

Las encuestas, las planillas de asistencia y las fotos que se tomen en este evento se consideran de dominio público y pueden estar sujetas a la difusión pública. Para obtener más información, consulte la Public Records Act (Ley de Registros Públicos), RCW capítulo 42.56, o visite Seattle.gov/privacy. Todos los comentarios enviados se incluirán en el Informe del efecto de la vigilancia.

City of Seattle

Kormeerida Bandhigga Tiknoolajiyada ee Magaalada

Feebaraayo 27, 2019
6:00 p.m. - 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Nagulasoo biir bandhigga dadweynaha si fikir looga dhiibto dhawr kamid ah aaladaha tiknoolajiyada ee City surveillance:

Seattle City Light
- Binoculars
- Sensorlink Ampstik
- Sensorlink Cabiraha mitirka Gudbiyaha

Seattle Department of Transportation
(Waaxda Gaadiidka ee Seattle)
- Acyclica

Seattle Fire Department
(Waaxda Dab damiska ee Seattle)
- Adeeg Qaybinta Kumbuyuutarka loo adeegsado

Seattle Police Department
(Waaxda Booliiska ee Seattle)
- Qalabka Duuba Wicitaanada 911
- Computer Aided Dispatch
- CopLogic

Nooguma imaan kartid miyaa si toos ah?

Booqo barta www.seattle.gov/privacy si aad fikirkaaga oonleen ahaan uga dhiibato **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.**
Mudada Fikrad Dhiibashadu furantahay waxay kabilaabanaysaa **Feebaraayo 5 - Maarso 5, 2019.**

Fadlan noogusoo gudbi ciwaankaan Surveillance@seattle.gov hadaad ubaahantahay hooy laguusii qabto. Wixii macluumaad dheeri ah, booqo Seattle.gov/privacy.

Xog aruurinada, waraaqaha lasaxixaayo iyo sawirada lagu qaado munaasabadaan waxaa loo aqoonsanayaa diiwaan bulsho waxaana suuragal ah in bulshada lagu dhex faafiyo. Wixii macluumaad dheeri ah kafiiri Public Records Act (Sharciga Diiwaanada Bulshada) RCW Cutubkiisa 42.56 ama booqo Seattle.gov/privacy. Dhammaan fikradaha ladhiibto waxaa lagusoo darayaa Warbixinta ugu danbaysa ee Saamaynta Qalabka Muraaqabada.

City of Seattle

城市监控技术博览会

2019 年 2 月 27 日
下午 6:00 至下午 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 9810

加入我们的公众会议，留下您对纽约市监控技术的意见：

Seattle City Light
- 望远镜
- Sensorlink Ampstik
- Sensorlink 变压器表

Seattle Department of Transportation（西雅图交通局）
- Acyclica

Seattle Fire Department（西雅图消防局）
- 计算机辅助调度

Seattle Police Department（西雅图警察局）
- 911 通话记录录音器
- 计算机辅助调度
- CopLogic

无法亲自前来？

访问 www.seattle.gov/privacy 发表在线评论或将您的意见发送至 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124。开放评论期：2019 年 2 月 5 日至 3 月 5 日。

如果您需要任何住宿服务，请通过 Surveillance@seattle.gov 联系我们。要获得更多信息，请访问 Seattle.gov/privacy。

此次活动中的调查、签到表和照片被视为公共记录，可能会被公开披露。有关更多信息，请参阅 Public Records Act（信息公开法）RCW 第 42.56 章或访问 Seattle.gov/privacy。提交的所有意见都将包含在监控影响报告内。

City of Seattle

도시 감시 기술 박람회

2019 년 2 월 27 일
오후 6:00 – 오후 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

공개모임에 참여하시고, 도시 감시 기술과 관련한 의견을 공유해 주십시오.

Seattle City Light
- 쌍안경
- Sensorlink Ampstik
- Sensorlink 변압기 미터

Seattle Department of Transportation(시애틀 교통국)
- Acyclica

Seattle Fire Department(시애틀 소방국)
- 컴퓨터 지원 출동 지시

Seattle Police Department(시애틀 경찰국)
- 911 전화 기록 녹음기
- 컴퓨터 지원 출동 지시
- CopLogic

현장 참여가 어려우신가요?

www.seattle.gov/privacy 를 방문하셔서 온라인 의견을 남기시거나 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124 로 의견을 송부해 주시기 바랍니다. 공개 의견 수렴 기간은 2019 년 2 월 5 일 – 3 월 5 일입니다.

편의사항이 필요하신 경우 Surveillance@seattle.gov 로 문의해 주시기 바랍니다.
자세한 정보는 Seattle.gov/privacy 를 참조해 주십시오.

본 행사에서 수집된 설문 조사, 참가 신청서 및 사진은 공개 기록으로 간주되며 일반에 공개될 수 있습니다. 자세한 사항은 Public Records Act(공공기록물법) RCW 챕터 42.56 을 참조하시거나, Seattle.gov/privacy 를 방문하시기 바랍니다. 제출된 모든 의견은 감시 영향 보고서에 수록됩니다.

City of Seattle

城市監視技術展覽會

2019 年 2 月 27 日
下午 6:00 至下午 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

加入我們的公眾會議，留下您對紐約市監視技術的意見：

Seattle City Light
- 望遠鏡
- Sensorlink Ampstik
- Sensorlink 變壓器表

Seattle Department of Transportation（西雅圖交通局）
- Acyclica

Seattle Fire Department（西雅圖消防局）
- 電腦輔助發送

Seattle Police Department（西雅圖警察局）
- 911 通話紀錄錄音機
- 電腦輔助發送
- CopLogic

無法親自前來？

造訪 www.seattle.gov/privacy 發表線上評論或將您的意見傳送至 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124。開放評論期：2019 年 2 月 5 日至 3 月 5 日。

如果您需要任何便利服務，請透過 Surveillance@seattle.gov 聯絡我們。要獲得更多資訊，請造訪 Seattle.gov/privacy。

此次活動中的調查、簽入表和照片被視為公共紀錄，可能會被公開披露。有關更多資訊，請查閱 Public Records Act（資訊公開法）RCW 第 42.56 章或造訪 Seattle.gov/privacy。提交的所有意見都將包含在監視影響報告內。

City of Seattle

Appendix C: Meeting Sign-in Sheet(s)

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☒ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☒ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

☐ Include Middle Eastern

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☒ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☒ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☑ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County
- ☐ Prefer not to identify

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☑ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☑ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☒ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☒ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☑ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☒ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☒ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☑ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☑ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☑ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

2

Queen Anne

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☑ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☑ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☑ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☒ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☒ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☒ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood
- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☑ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity
- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☑ White
- ☐ Prefer not to Identify

Age
- ☐ Under 18
- ☑ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender
- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood
- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity
- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age
- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender
- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

X

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☒ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☒ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☒ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☒ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☒ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☒ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☒ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☑ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☑ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

leighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
☒ First Hill
] Georgetown
] Greenwood / Phinney
☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake
☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
☒ Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☒ 18-44
☐ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☒ Female
☐ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☑ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
] Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☐ 45-64
☑ 65+
☐ Prefer not to identify

Gender

☐ Female
☑ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

☑ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
] Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☑ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☑ Female
☐ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney
SE KING COUNTY

☐ International District
☐ Interbay
☐ North
☐ Northeast
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake

☑ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
✓ Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☑ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☐ Female
☑ Male
☐ Transgender
☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☒ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☒ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☒ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☒ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☒ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☒ 65+
- ☐ Prefer not to identify

Gender

- ☒ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☑ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☑ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☑ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☑ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Neighborhood

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☑ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☑ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

City of Seattle

Appendix D: Department of Neighborhood Focus Group Notes

Friends of Little Saigon (FOLS)

Please select which technology you wish to comment on:

☐SCL: Binoculars	☐SCL: Sensorlink Transformer Meter (TMS)	☐SFD: Computer-Aided Dispatch	☐SPD:9-11 Call Recorder
☐SCL: Sensorlink Ampstik	☐SDOT: Acyclica	☐SPD: Computer-Aided Dispatch	☒SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

- Will they keep the data safe on coplogic?
- Can it be hacked?
- What if you report your neighbour and your neighbour hacks the system and find out?
- What is the money amount limit for coplogic / Why is there a limit for coplogic?: (a community member says that she believes that the limit $500 or under, but it's hard to have a limit because a lot of packages cost more than $500 such as electronics get stolen and you won't be able to report it online)
- The departement is having all these technologies being used but not letting the public aware of it
- Coplogic is not clear and is confusing to use (what you can report and what you can't report)
- If coplogic is known by the community would they use it ? (Community members agreed that no one would use coplogic because it's not in Vietnamese. Not even people who speak english fluently even use it.
- Many community members don't trust the system)

What value, if any, do you see in the use of this technology?

- Coplogic has been going on for a few years it's not very effective. The only effective thing is that coplogic is doing saving police hours and time.

What do you want City leadership to consider about the use of this technology?

- Most of the time, our community don't report things because they don't trust the system, they often tell someone that they trust a friend. Is there an option that someone and report a crime for someone else?

Other comments:

- The government should be more transparent with the technology system with the public.
- The translation is much far removed from the actual Vietnamese language.

- The translation is very hard to understand, the language is out of context (The flyer is poorly translate)
- Is there resources to support these technologies? Is there translations so that it is accessible for everyone? Will this accommodate everyone?
- Police should have a software that connects them to translation and interpretation right away instead of having to call a translator
- How will other people know of the technology if they can't come to focus group meetings? Such as flyers? Social media? Etc.
- Besides face to face meetings, are there plans to execute this information of the technology and surveillance to the community?
- Will the City of Seattle go to community events, temple, the church to reach out to the community and explain the technologies?
- These technologies are taking a part of our taxes, so everyone should know. It should be for everyone to know, not only catered to one group or population.

Are there any questions you have, or areas you would like more clarification?

- How effective are the tools/technology?
- How many people know of these technologies? Provide statistics
- What are the statistics of the coplogic?
- What is the data and statistics for coplogic and what are people reporting?
- What is the most common crime that they are reporting?
- And how effective is coplogic based on the statistics and data?

City of Seattle

Friends of Little Saigon (FOLS)

Please select which technology you wish to comment on:

☐SCL: Binoculars	☐SCL: Sensorlink Transformer Meter (TMS)	☐SFD: Computer-Aided Dispatch	☒SPD:9-11 Call Recorder
☐SCL: Sensorlink Ampstik	☐SDOT: Acyclica	☒SPD: Computer-Aided Dispatch	☐SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

- CAD did not work from experience. A community member said that they reported that they needed assistance at 10:00pm and no one showed up, then had to call 911 at 12:00am and someone finally showed up at 4:30am
- Why create more options and technologies if the police department and government can not support it? It's a waste of time and money (taxes). Should have enough personals before they implement technology.
- Government should have enough personals to support translation if they choose to translate.

What do you want City leadership to consider about the use of this technology?

- The city should focus on having the community review the technologies that are yet to be implemented.
- The Vietnamese community is not getting the information we need to report crimes

Other comments:

- Engagement is very important. Engaging the community and engaging different demographics.
- Friday night, Saturdays, and Sunday afternoon work the best for the Vietnamese community.
- If the city wants to involve the vietnamese community and engage the Vietnamese community, it is important to accommodate with our community It is important to proofread the translation, have 3 people proofread. Someone
  pre 1975, post 1975 and current Vietnamese language. The government clearly does not proofread the translation.

Council on American Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington
Thursday, Feb. 21, 2019
Technology Discussed: CopLogic

1. Do you have concerns about this specific technology or how it's used?
    - Having used the system myself the one thing I noted was the type of report you can file, they ask questions like if you knew the suspect, and if you're saying no I don't know who did it. and you check a box that says I understand that no one is going to investigate this
        - What is the point of having a system in place than If no one is going to investigate it
        - It is for common things like my car is broken into and stuff was taken out of my car, you can file it if you need a report for insurance. But if you were to call that and report to the police, they wouldn't come for days
    - So for example if I can be a straight up Islamophobe and I can see a Muslim woman and make a bunch of false reports online, and how long would it take for someone to say I see you making all these reports. Because people can make so many different reports, how do you deal with that
        - There are very limited types of reports that it will accept. So if someone wanted to report graffiti and they were reporting more hate crime related graffiti an officer will review the report
        - So I think the review process would be really important
    - Another barrier is that it's an online system so we need to think about wifi access and there is this assumption that everyone has access to internet and computers. And what I'm hearing is that people can just file a report at a click of their finger. And if these people can do that on their computer what stops them from being able to file all these cases about certain groups and individuals.
    - Additional there have been cases in the past where people are abusing reporting system. This one doesn't allow you to report against known suspect but I could see that happening in the future so I wanted that to be mentioned. The other thing under protection is says all activity can be stored and the data Is monitored by lexis nexus… and this company does a lot of research on crime mapping which brings up some of the concerns on like CVE
        - But what you are saying is that lexis nexus does other mapping that it can use this information for
        - Yes, because I want to clarify what is the technological ambition of SPD because I don't think this would work well in the communities that SPD is supposed to served. And I would want a contract review of what lexis nexus does. Will the info stay on the data and server of lexis nexus, what happens to it
    - Another thing is has SPD given Lexis nexus to use this in any of the research data they do, because they put out a lot of information regarding mapping, and crime control. And what information are they allowed to take
    - We have seen recently people doing interesting things when reporting crimes. I think its important to realize that when reporting crime people have a different perception when reporting crime. People will see you in a certain neighborhood and might think they stole that car, or are doing something bad here. So when we give people the ability to

report online we need to be concerned with accessibility about people being able to report freely… and we saw for a year that if an African American person came to use a swimming pool someone can call and say they don't live here. I think SPD is trying alleviate some of those calls they are getting, but I don't think this is the solution to the problem
    - What is the logic behind this overall, because is seems like it presents more cons than pros, and what is analytics database you use to look at these reports. Because when I am using government data base I can see where I need more surveillance etc. so we are getting all these open wholes in the system. Is this a right wing Donald trump agenda to watch neighbors of color and surveillance
    - I think im more concerned with where does this information end up and how is it used
    - What is the usefulness of the information that is not followed up on. And how does it help the people it's actually serving? So for example someone works for an anti-Muslim white supremacy group and they have people in different areas report issues about different Muslim groups in Seattle how do you prove the validity of these information and make sure they aren't just causing harm
2. What value do you think this brings to our city?
    - I think technology saves time, money, makes filing a report easy, I had to do that once it takes a lot of time.
    - I appreciate that it is easier so something like a hit or run or a car breaking in, that's fine.
3. What worries you about how this is used?
    - The only issues I can think of right now is it seems like it would be very easy to make a fraudulent report or a report that is for a small thing that you can make into a big thing, like the things you see go viral on the internet. So now it seems like the barrier to making a police report is smaller
    - I agree I think the bar is lowered and different people are perceived differently. And we have seen how SPD criminalizes different communities for behaviors that don't need to be criminalizing
    - A lot of different kinds of reports have to do with peoples perceived notion, so my concern comes from how do we make sure that this kind of technology isn't used to map our where Muslims live/are, and there types of religious belief. Or isn't being used to monitor them. How do we ensure that this isn't used to map our communities
    - The only comment I have that in the forms I have filled out is it won't allow you to fill out the form if you are naming a specific individual, you can name a group, but a not a person. The following criteria is there no known suspects, it happens in Seattle, so things like thefts. So you can report, graffiti, identity theft, credit card fraud, simple shop lift. So when I click report it says if you have a suspect it says please call. And when I press report it allows me to report anonymously, so I could report against a community with no follow up
        - Well that doesn't stop them from targeting al-Noor masjid, or Safeway in new holly, or new holly gathering hall, and it can target the people in that community. And people don't feel comfortable with increase police presences, so it targets area if not targeting people
    - When I was buying the house in Dallas (participant currently still lives/works/plays in Seattle) one of the first things I did was looking at a crime map and based off of that if someone is making a lot of reports can that be used for crime mapping because than

that can lower the property value. And if the police isn't following up then how is it being used
- Its definitely possible for people to report inaccurate information

4. What recommendations would you give policy makers at the City about this technology?
    a. But my concern is reporting someone that can really target people of color. And that happens much more threatening to people. So the concept of an upset black women is more intimidating than an upset women that is another race and how many times will behavior like that be reported. Or how many times will a black man be reported against because it seems scary. So I think it lowers the bar when you don't have to talk to an individual when you don't have to talk to a police
    b. My questions are, how accessible are cop logic to people who don't read or speak English. How is SPD going to do what they can to make sure that this doesn't negatively impact communities they are already having issues with like the Sea Tac community that already feels threaten and criminalized by communities.

5. Can you imagine another way to solve the problem this technology solves?
    - So the SPD is very data driven these days and the one thing we repeat is report report report, call 911 and report online whatever you thinking is happening because all of that goes into their data base and is used for them to use resources and put police based off of where there is more crime. The report report report mentality assumes there are good relationships between the community and police, so even if someone doesn't do something bad, I don't know that they would feel comfortable reporting, even if online
    - From the community I have come from I am almost certain that they haven't even used online reporting so how do we make sure that we are giving everyone access to use online reporting. And there are certain crimes that are so common in areas that they don't even report it because they think the police should already know about it
    - I think the department should solely rely on the technology only as a way of collecting info they should still use in personal resources to actively participant in local community and make connections you can't rely only on this technology alone to do this

6. Other comments
    a. Also in this day in age we need to consider that immigration is a issue, and this administrative has blended the different agencies so people have a hard time knowing where SPD starts and ICE starts and those lines have been blurred and that is a real concern for many families

Council on Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington

Thursday, Feb. 21, 2019

Technology Discussed: Binoculars/Spotting Scope

1. Do you have concerns about this specific technology or how it's used?
    0. People in our community don't have the access to say or be apart of these conversation. A lot of these people are literate, and might not have the same cultural values. For Muslim women there are a type of consent that you have when you walk outside and are covered in a certain away versus when you are in the privacy of your own home. And people might not have that cultural and religious awareness
    1. I had one quick concerns, as far as the data that is collected using these binoculars, who has access to it
        - Seattle City Light: Information goes into the billing system, which customers can access if they have the automated reader but do not have access to under the current system
    - I know the focus is on binoculars but my mind is on new technologies and when people who are consumers and feel like I am overcharged how do I follow up and get those issues resolved. For systems that are completed based off of technologies how will I know if that data is being altered.
    2.
2. What value do you think this brings to our city?
    0. I would just add this is more my general comments I think its good that Seattle city lights is providing notifications to people when this is happening. Are they wearing something visible that show people they are from Seattle city lights? And is there a way for people to complain?
        - Yes they are wearing vests that are very visible. Yes we have a couple different avenues the easiest is to call the customer service line and to submit a complaint there
3. What worries you about how this is used?
    0. My primary concerns on my end is if someone is looking into my home with binoculars its a privacy concern. Most Muslim women wear hijab and I don't feel comfortable if someone is using binoculars looking from the outside when we are not wearing the hijab. My concern is that it is a huge invasion of privacy
    1. I have a question as the women expressed the feeling of people reading the meters with binoculars, if the meter has abnormal behavior or is in a different place of the house. Have there been situations where someone sees the person looking at someone house with binoculars, and they might not have gotten notified. Or the meter might be on the opposite side of where they are looking. Are they getting background checks? Or are complaints being followed up

- Seattle City Light: Yes all city employees have background checks, and if a complaint gets called in they will go through disciplinary actions
- What are the average times for disciplinary actions. How long is the process for a full investigation
- Seattle City Light: It's a multiple step process in terms of different levels. There are warnings, and if there was undo actions. Timeline really depends, I'm not sure
- Cause I think that people who go through the different nuances of how privacy can be breach that is just the end all be all of how privacy can breach so I think there needs to be policy put in place so that people don't have their privacy breach and they are being monitored by a pedophile

4. What recommendations would you give policy makers at the City about this technology?
    0. When I look at the Seattle city of light they do a lot of estimated guesses and as a consumer they might give you a $500 fee based off of the estimated guesses so I think it is important to have some sort of device that better clearly shows how much you use

5. Can you imagine another way to solve the problem this technology solves?
    0. My other question is if its actually not efficient why do you get the option to opt out (of the new automated system). If there is an old school way of doing it that involves a breach of privacy because these are human beings using the binoculars, so If this other option is better why are people having the ability to opt out.
6. Other comments: (Many comments were discussed over Seattle City Light's upcoming change from binocular use to automated meter readers)
    0. Who opted out was it home owners?
    1. When we go to a place with 12 tenements do all 12 of them have the ability to opt out or in, or just the owners of the building?
    2. Each home owner has a schedule provided to them and it is a 3 day period which they can come in and look at the system
    3. Is there a cost to them to have the new meter.
        - Seattle City Light: There is no cost with getting the new meter, but there is still a cost If we have to send someone out there to read it
        - What I don't understand is why the new practice is not to just use the new system since that is more accurate and it is doesn't require binoculars
        - What is the cost of opting out
        - Seattle City Light: There is a flat rate
    - I was gonna reiterate when we talk about equity and equitable practices. You can opt out (of the automated system) but there is a fee. And it makes me think how much of It is a choose if one of these you have to pay for and the other one

is free. So that sounds a little problematic when looking at choices of equity. I think choices are great, but also people need to be well informed. Like people within the community need to have more clear information to make the best decision for themselves

- Going back to people who make the decision. I want the person who are living in the house to know what decision is being made. So not just the person who owns the house, but the person living in the home. And not everyone it literate and not everyone speaks English. And its really important that you are giving them information they can actually consume. Instead of giving them notices they cant read

Council on Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington
Thursday, Feb. 21, 2019
Technology Discussed: Acyclica

1. Do you have concerns about this specific technology or how it's used?
    - Where does this data go? Does it go to SDOT? Google maps?
    - My other question is, it said whatever is being transferred is encrypted. All encrypted means to me is getting data from one device to another will be transferred without it being intercepted. What I don't know is, how much information are people getting
    - My concern is related to data, yeah we like to use gps. But what is the perimeter, what is the breach of access. Where is the data being used, and what can that turn into. we might be okay if the data is only being used for traffic related updates, but they might use it for more
    - I also would like to see how acyclica actually does what they do. They are using a lot of words that normally don't know. So I want to know how exactly they are hashing and salting. So for them to be clear about how they doing it. like when whatsapp encrypted they didn't give us the exact code but told us how they are doing it
    - Asking for a greater transparency for how they are doing this
    - I think the purpose of it is really important but the biggest concern is collecting all of this information without consent of passersby.
    - So the specific identifier that acyclica uses it mac addresses? You could potentially use that number to track that phone for the lifetime of the phone, for as long as that phone is on and being used. And that is very concerning.
    - Also I want to understand more where is this data going, and I want to know if this data is going to be used for future projects.
    - I want to ask is this something people opt into
    - People don't even know this is being used

2. What value do you think this brings to our city?
    - I like getting places and I like getting traffic information.
3. What worries you about how this is used?
    - What I don't like is you using my phone to get that information. I want whatever is in my cellphone to be protected. And I wanna know what you can access
    - I think based on Seattle and Seatac's higher up wanting to monitor and map out Muslims and where they are, and I don't like people being able to use our phone to track our location or actions they might think is violent. So based off of Seattle's track record and law enforcement agencies I don't like it
    - People who live outside of Seattle are also being impacted by it anytime they drive in Seattle
    - Could someone "opt out" by having wifi disabled on their device? I don't know if this covers cell towers. Because if it covers cell towers the only thing you could is having your phone on airplane mode

4. What recommendations would you give policy makers at the City about this technology?
    - I think the big question is why aren't we using other vendors, like I mentioned google maps, or waze, in fact komo 4 uses ways. Where other options we're looked at, and what were the trade off there's. And I want to see some transparency between the decision-making processes
    - I don't think this data should be shared with other private agencies, or other interagency programs
    - If all you're looking at is traffic flow, why are you not using the sensors in the road to give traffic flow updates.
    -
5. Can you imagine another way to solve the problem this technology solves?
    - I don't know if this already exists but something that makes it that data can't be used from one technology and use it for a different purposes
    - I think speaking from an industry perspective that is really important to have a processes for. Because all of this data is being used regardless of if you live in Seattle, or people live in different countries even who are visiting. That data is being collected. My understanding is that SDOT doesn't get the data directly. So my concern is how long can acyclica keep this data, use this data. Why wasn't a different option used, one in which some sort of consent can be used, so something like waze, google maps where people can opt in can get that information.
    - Road sensors or ways to count cars
    - I think its better to count cars than phones, because there is some expectation that your car will be monitored.
    - Using vehicle level granularity

City of Seattle

Entre Hermanos

Please select which technology you wish to comment on:

☐SCL: Binoculars	☐SCL: Sensorlink Transformer Meter (TMS)	☐SFD: Computer-Aided Dispatch	☐SPD:9-11 Call Recorder
☐SCL: Sensorlink Ampstik	☒SDOT: Acyclica	☐SPD: Computer-Aided Dispatch	☐SPD: CopLogic

1) What concerns, if any, do you have about the use of this technology?

El uso de wifi en Acyclica porque pueden obtener toda la información de los teléfonos.

Si vale la pena la inversión

Enfocando al grupo: La tecnología ya está instalada. que les preocupa de su uso?

El tráfico sigue igual.

Quien usa o almacena la información.

La preocupación es la colección de data.

Colección y almacenamiento de información es la mayor preocupación.

No es la colección de data lo alarmante sino los recursos (dinero utilizado) ya que o la tecnología no están funcionando porque el tráfico sigue igual. No hay cambio con la nueva tecnología, esos gastos no son válidos ya que no hay resultados. Esos gastos pudieran ser utilizados para la comunidad.

También tienen que ver si la tecnología emite radiación o alguna otra cosa dañina; perjudicial a la salud.

El gobierno tiene todos los datos.

No necesitan esta tecnología para tener los datos porque ya existen métodos para eso, incluso aplicaciones o alguna otra cosa.

La otra preocupación del grupo es que no haya un cambio al problema que se quiere resolver. En el caso de Acrylica sería el mejorar el tráfico.

- Tecnologías como esta necesitan recolectar más opiniones de expertos.
- Sería bueno que la información sea compartida con la comunidad. (Transparencia en fines y objetivos de la tecnología y datos guardados, tácticas implementadas.)

2) What do you want City leadership to consider about the use of this technology?

Hay lugares donde no se necesitan. En algunas partes de Magnolia, Queen Anne, Northgate, no se ocupan.

Seguimiento de pregunta: En las comunidades donde viven los latinos que tanto se ocupa Acyclica?

Participante no cree que allí se ocupan.

Hablaron sobre la necesitad de puntos estratégicos y calles con más necesidad de ayuda por causa del tráfico.

What do you think about this technology in particular ?

Bien, la tecnología ayuda con la velocidad o el movimiento de los coches.

La información se guarda y analizan por donde viajas o cuantas veces cruzas este rastreo.

Si es solo para ver el tráfico está bien.

Está bien en algunas partes. Puede que sea algo bueno. Pero puede que esta tecnología pueda compartir información personal que puede ser utilizada de otra forma en especial si hay Hacking (forma negativa, uso de datos).

La tecnología en sí no es tan grande (de tamaño) para ser algo visualmente desagradable. La información captada a través de estos medios puede que ayude a conducir el tráfico de mejor manera pero también puede que tome información personal.

Are there any questions you have, or areas you would like more clarification? ●

La tecnología no es un router, sino colección de data para planeaciones urbanas.

Participante: “quiero creer” “convencerme” que los sensores están allí para ayudar con el tráfico.

No se sabe cuándo las instalaron, los resultados deberían de ser públicos. Si la tecnología es para aliviar el flujo de tráfico entonces por qué no extienden el programa? O por qué no hay mejoramiento del tráfico?

Alternatives to this technology

- Alguna pantalla que indique cuáles vías son alternativas puede reemplazar esto.

- Cambios al límite de velocidad puede que alivie el flujo del tráfico.
- Dejar de construir tanto.
- Rediseño de calles ayudaría flujo de tráfico.
- El rediseñar las vías servirá para las futuras generaciones.

City of Seattle

Please select which technology you wish to comment on:

☒SCL: Binoculars	☒SCL: Sensorlink Transformer Meter (TMS)	☐SFD: Computer-Aided Dispatch	☐SPD:9-11 Call Recorder
☐SCL: Sensorlink Ampstik	☐SDOT: Acyclica	☐SPD: Computer-Aided Dispatch	☐SPD: CopLogic

Entre Hermanos

1) What concerns, if any, do you have about the use of this technology?

Los binoculares son preocupantes si la persona no tiene ética. Es preocupante que una persona vea a través de binoculares a que una tecnología mida el uso de la electricidad

Al grupo le incomoda el uso de binoculares

Sensorlynk específicamente la preocupación sería que le quita el trabajo a una persona.

Si es para detectar robo el grupo cree que hay otras maneras de saber quien roba

que no tan solo será para leer la electricidad sino para obtener otros tipos de información si cámaras fueran usadas

2) What value, if any, do you see in the use of this technology?

Ahorro de energía

Record y datos mas precisos

Oportunidad de trabajo a quien utiliza los binoculares

Estabiliza los precios de la electricidad

3) What do you want City leadership to consider about the use of this technology?

: Usar background check, uso de uniforme por trabajadores, cámara en binoculares.

What do you think about this technology in particular ?

Sensorlink Si

Binoculares son invasivos

Are there any questions you have, or areas you would like more clarification? ●

La confianza en estos medidores serán confiables? Serán efectivos?

El uso de binoculares se puede acompañar de una cámara añadida

Alternatives to this technology

Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad

City of Seattle

Entre Hermanos

Please select which technology you wish to comment on:

☐SCL: Binoculars	☐SCL: Sensorlink Transformer Meter (TMS)	☐SFD: Computer-Aided Dispatch	☐SPD:9-11 Call Recorder
☐SCL: Sensorlink Ampstik	☐SDOT: Acyclica	☐SPD: Computer-Aided Dispatch	☒SPD: CopLogic

1) What concerns, if any, do you have about the use of this technology?

Las fallas electrónicas son preocupantes especialmente en reportes policiacos.

Las preocupaciones es que el reporte no salió, no llegó por cualquier razón.

No todos podrán o saben usar las computadoras.

Fallas de los algoritmos de cada demanda es alarmante.

Que y cuando determina la urgencia de respuesta

Las personas le temen a los policías. Y este medio puede ayudar a que el miedo disminuya.

La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

2) What value, if any, do you see in the use of this technology?

La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

El uso de computadora está bien para las denuncias.

Si personas usan esta tecnología y es analizada en tiempo real por otras personas no hay problema.

Es otro método para denunciar

Está de acuerdo con el uso de computadoras para denunciar solo que no todos son capaz de usar este método/tecnología.

3) What do you want City leadership to consider about the use of this technology?
Que sea multi-idioma, implementar audio, implementar sistemas que ayuden a múltiples personas con diversas capacidades/necesidades

Si es usada de manera adecuada y como han dicho está bien.

El uso de la tecnología es bueno para dar respuesta para todas las cosas y personas

What do you think about this technology in particular ?

Grupo están de acuerdo con su uso.

Puede salvar una vida.

Los riesgos y acciones determinan la urgencia de la intermisión policiaca.

Alguna gente se siente más capaz de presentar una queja a través de este sistema, la tecnología en uso tiene validez.

Bueno para la violencia doméstica.

Are there any questions you have, or areas you would like more clarification?

La computadora decidirá la importancia/urgencia del reporte/emergencia dando a llevar acciones de emergencia.

Gravedad de emergencia es determina por tecnología.

La definición de emergencia es diferente con cada persona.

Cada uno tiene la definición de vigilancia, pero ¿que tal la definición de emergencia?

SITUATIONS TO APPLY ITS USE

Una pelea en la calle, un malestar corporal, cuestiones de vida, abuso doméstico

Si nos basamos en la definición de emergencia sólo en cuanto estemos en peligro inmediato o en tiempos mínimos/ de transcurrencia alarmante/peligrosa el uso de será implementado o limitado solo a instantes inmediatos de peligro.

Para reportar algo que ya sucedió o que son recurrentes.

Basado en el concepto de emergencia, las personas pueden tomar el método adecuado para reportar su caso y a través del medio necesario.

Los reportes no son anónimos.

Los datos son recolectados aun, a pesar de la opción escogida.

Alternatives to this technology

Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad

City of Seattle

Entre Hermanos

City of Seattle
Surveillance

Inicio

Resumen: El departamento de vecindarios quiere saber la opinión de este grupo. Ellos verán videos de un minuto y medio y encontrarán folletos en sus mesas donde encontraran más información sobre lo visto.

Demográficos:

Ocho personas participaron, una de West Seattle, una de First Hill, dos de Ravenna/Laurelhurst y cuatro de King County (outside Seattle).

Cuatro personas se consideraron hispano o latino, una como india americana o nativa de Alaska, y tres no opinaron.

Cinco personas marcaron 18-44 como su rango de edad, dos marcaron 45-64 como el suyo y una no opinó.

Cinco personas marcaron masculino como género, una como transgénero, una como femenino, y otra no opinó.

Otra Información Importante:

- Preguntas serán hechas.
- Habrá una hoja para poder conversar sobre videos de interés
- Se les agradeció por venir.
- El concepto de vigilancia será manejado como la ciudad de Seattle lo maneja.
- Tom: Agradeció a los invitados por venir

Surveillance. In 2017 city council passed an ordinance to see what technology fit the definition of surveillance. The information gathered by these surveillance technologies are as follows: to “observe or analyze the movements, behaviors, or actions of identifiable individuals in a manner” which "is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice.”

Presentador: Preguntó si la conversación en inglés fue entendida.

Grupo: Concordó.

Tom: Do not let information on videos stop you from making comments or raising questions.

Presentador: Dio a entender el concepto de vigilancia como ha sido interpretada por la ciudad de Seattle. Fue analizada de esta manera: “La vigilancia es definida como tecnologías que observan o analizan los movimientos, comportamientos, o acciones de individuales identificables de una manera que razonablemente levanta inquietudes sobre libertades civiles, la libertad de expresión o asociación, igualdad racial o justicia social.”

- Los movimientos de la gente son observados a través de esta tecnología y puede que para algunas personas esto sea incómodo.
- Las cámaras de policía no califican como tecnologías de vigilancia en este tema.
- La presentación mostrada en la pantalla a través de los videos será transmitida en inglés.
- Se pidió que todos se traten con respeto y que opinen y que su nombre sea mencionado e incluso la vecindad donde viven.

El Grupo

Participante vino porque quiere obtener más información y dar su opinión. Es de Seattle.

Participante viene de Shoreline/Seattle para ver cuánto la tecnología entra afecta

Participante vino porque quiere saber qué información es colectada por el gobierno y para qué usan esa información. Puede que la información obtenida a través de la tecnología sea usada para perseguir a personas de color/minorías/personas marginadas.

Participante vino de First Hill, porque quiere ver el punto de vista de la ciudad y ver que opiniones surgirán.

Participante viene de Seatac porque tiene interés en el tema y porque la seguridad es importante y quiere saber a dónde llega la información.

Participante vine en Ravenna/Northgate, quiere ver que tan confiable es la tecnología y para qué es utilizada. Perjudicial o beneficial?

Participante vine en Seatac y vino porque es un tema muy interesante ya que se tiene que saber/mantener informado de lo que hacen los gobernantes.

Participante vino de Burien por la importancia del tema y la privacidad.

Presentador: La tecnología no es nueva. Ya está siendo usada. Y quieren saber el formato para que las futuras tecnologías tengan.

El video de Seattle Department of Transportation de Acyclica fue mostrado

Esta tecnología es un sensor que detecta el wifi. Es un sensor que detecta la tecnología wifi.

Seattle Metering Tool fue mostrada

Nadie del grupo sabe del tema más el presentador no hablará a fondo de esto para no influenciar opiniones.

Video de Fire Department's Computer Aided Dispatch fue mostrado

El 9-1-1 logging recorder video fue mostrado

Aclaración: Información impresa fue entregada explicando cada una de las tecnologías.

Video de Coplogic fue mostrado

El grupo no conocía que se puede reportar a la policía a través de su página/en línea.

El video de Seattle Police Computer Aided Dispatch fue mostrado

Esta tecnología es similar a la de los bomberos.

Se preguntó cuál video era de interés para analizar

Se acordó el análisis de Acyclica, Binoculares/Sensorlink, y Coplogic

Las Preguntas que sea harán serán las siguientes:

¿Qué piensan de este sistema de tecnología en específico y el motivo de usarla?
¿Cuál creen que sea el aporte de esta tecnología a la cuidad?
¿Qué preocupación les causa el uso que se le dará a este sistema?
¿Qué recomendarían a el grupo de políticos de la cuidad responsables de tomar las decisiones de implementar estas tecnologías?
¿Qué otra manera habría de resolver el problema que esta tecnología esta designada a resolver?

La Acyclica

Pregunta: ¿Qué piensan de este sistema de tecnología en específico y el motivo de usarla? (Como se usa y cuál es el uso)

- Bien, la tecnología ayuda con la velocidad o el movimiento de los coches.
- La información se guarda y analizan por donde viajas o cuantas veces cruzas este rastreo.
- Si es solo para ver el tráfico está bien.

- Está bien en algunas partes. Puede que sea algo bueno. Pero puede que esta tecnología pueda compartir información personal que puede ser utilizada de otra forma en especial si hay Hacking (forma negativa, uso de datos).

- La tecnología en sí no es tan grande (de tamaño) para ser algo visualmente desagradable. La información captada a través de estos medios puede que ayude a conducir el tráfico de mejor manera pero también puede que tome información personal.

Pregunta: Qué es lo que aporta esta tecnología a la ciudad?

- Seria algo bueno el aporte por la agilidad del tráfico solo si la tecnología está sincronizada con los semáforos, de otra manera no es útil si no aporta para el mejoramiento del tráfico.

- Participante dice que hay alternativas para esquivar el tráfico.

- Participante opina que la tecnología es interesante ya que usa google maps y está de acuerdo con el mejoramiento del tráfico.

- Si el objetivo es de mejorar el tráfico está de acuerdo. Pero también quiere saber en qué lugar(es) estarán los aparatos, si algunas personas serán beneficiadas más que otras.

Pregunta: Qué preocupaciones tienen con posible uso/uso potencial de esta tecnología?

- Le preocupa el uso de wifi en Acyclica porque pueden obtener toda la información de los teléfonos.

- Si el potencial puede ser aplicada a la inversión.

Enfocando al grupo: La tecnología ya está instalada, que les preocupa de su uso?

- El tráfico sigue igual.

- Quien usa o almacena la información.

- La preocupación es la colección de data.

Más de la mitad de grupo opina que esa (el almacén y colección de información) es la preocupación.

- Participante no está de acuerdo. No es la colección de data lo alarmante sino los recursos (dinero utilizado) ya que o la tecnología no están funcionando porque el tráfico sigue igual. No hay cambio con la nueva tecnología, esos gastos no son válidos ya que no hay resultados. Esos gastos pudieran ser utilizados para la comunidad.

- También tienen que ver si la tecnología emite radiación o alguna otra cosa dañina; perjudicial a la salud.

- El gobierno tiene todos los datos.

- Opinión de otro participante: No necesitan esta tecnología para tener los datos porque ya existen métodos para eso, incluso aplicaciones o alguna otra cosa.

La otra preocupación del grupo es que no haya un cambio al problema que se quiere resolver. En el caso de Acrylica sería el mejorar el tráfico.

- Tecnologías como esta necesitan recolectar más opiniones de expertos.

- Sería bueno que la información sea compartida con la comunidad. (Transparencia en fines y objetivos de la tecnología y datos guardados, tácticas implementadas.)

Pregunta: Le dirían algo a los políticos algo del lugar donde se encuentran estos aparatos?

- Hay lugares donde no se necesitan. En algunas partes de Magnolia, Queen Anne, Northgate, no se ocupan.

Seguimiento de pregunta: En las comunidades donde viven los latinos que tanto se ocupa Acyclica?

- Participante no cree que allí se ocupan.

Hablaron sobre la necesitad de puntos estratégicos y calles con más necesidad de ayuda por causa del tráfico.

Presentrador: Crees que Acylica es como el router de google?

- La tecnología no es un router, sino colección de data para planeaciones urbanas.

- Participante: “quiero creer” “convencerme” que los sensores están allí para ayudar con el tráfico.

- No se sabe cuándo las instalaron, los resultados deberían de ser públicos. Si la tecnología es para aliviar el flujo de tráfico entonces por qué no extienden el programa? O por qué no hay mejoramiento del tráfico?

Otra pregunta: Alguna otra tecnología que pueda ser utilizada en vez de Acyclica?

Alternativas:

- Alguna pantalla que indique cuáles vías son alternativas puede reemplazar esto.
- Cambios al límite de velocidad puede que alivie el flujo del tráfico.
- Dejar de construir tanto.
- Rediseño de calles ayudaría flujo de tráfico.
- El rediseñar las vías servirá para las futuras generaciones.

Tecnologia #2

Sensorlink/Binoculares

Pregunta: Que opina el grupo de la tecnología?

- Los binoculares son preocupantes si la persona no tiene ética. Es preocupante que una persona vea a través de binoculares a que una tecnología mida el uso de la electricidad.

- Un sensor que detecta la electricidad sería mejor.

- Al grupo le incomoda el uso de binoculares.

Pregunta: Qué opinas sobre la tecnología medidora de electricidad (sensorlink) y que sea usada en tu casa?

- No le incomoda o afecta a dos participantes.

- La preocupación sería que le quita el trabajo a una persona.

- Los binoculares son invasivos.

- Para que usar binoculares si es que se puede llegar a el hogar y ver el medidor en persona, pidiendo permiso? Si la tecnología es usa para ver que las personas se roban la electricidad, creen que no saben quiénes roban?

- El grupo cree que si saben.

Pregunta: Cual creen que sea el aporte que esta tecnología?

- El video dice que 3 millones de dólares son ahorrados.

Pregunta: De qué manera beneficia esto a la cuidad/ciudadanos/comunidad?

- El robo de la luz es preocupante.

- Si ya llevan el record y datos y le hacen saber a la comunidad puede que ahorren dinero.

- Uso de binoculares puede dar trabajo a una persona y dinero puede ser ahorrado con esta tecnología.

- La tecnología trae gasto de electricidad para poder ver gastos de luz? Si pretende evitar el robo entonces los gastos de la factura eléctrica deberían de seguir estables.

Pregunta: La confianza en estos medidores serán confiables? Serán efectivos?

- Ayuda a la precisión, a bajar precios.

- Que quiten los binoculares sería una sugerencia, o usar binoculares que graban con video.

- Si ya tienen récord sobre la energía (consumo, gastos, etc.), el robo de energía no es suficiente para establecer este tipo de tecnología ya que puede ser identificado el robo o alguna otra anomalía dependiendo en el nivel alto o bajo o repentino analizado/visto/detectado por métodos convencionales ya establecidos.

- Otra recomendación: Usar background check, uso de uniforme por trabajadores, cámara en binoculares.

- Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad

- .La preocupación es que no tan solo será para leer la electricidad sino para obtener otros tipos de información si cámaras fueran usadas.

Tecnologia #3 Coplogic

- Esta tecnología no solo el ahorro de tiempo, sino el ahorro de tiempo policial ya que ellos trabajarían en otras cosas

- El uso de computadora está bien para las denuncias.

- Si personas usan esta tecnología y es analizada en tiempo real por otras personas no hay problema.

Enfoque: Lo que estamos queriendo dialogar es el uso del internet y las denuncias.

- Es otro método para denunciar

- Está de acuerdo con el uso de computadoras para denunciar solo que no todos son capaz de usar este método/tecnología.

Pregunta: En que ayuda a la comunidad?

- Por qué usar estos métodos?
- Grupo están de acuerdo con su uso.
- Puede salvar una vida.
- Los riesgos y acciones determinan la urgencia de la intermisión policiaca.
- Alguna gente se siente más capaz de acudir a través de este sistema la tecnología en uso tiene validez.
- Bueno para la violencia doméstica.
- Las fallas electrónicas son preocupantes especialmente en reportes policiacos.
- Las preocupaciones es que el reporte no salió, no llegó por cualquier razón.
- No todos podrán o saben usar las computadoras.
- Fallas de los algoritmos o cuando o que promueve urgencia de cada demanda es alarmante.
- Criterio de demandas y que clase de preocupación de parámetros son confiables tienen que ser cuestionados/analizados, y que/quien es digno de prioridad o importancia o de ayuda.

Pregunta: De qué manera este uso beneficiaria a la comunidad?

- Personas pueden ser discriminadas
- Las personas le temen a los policías. Y este medio puede ayudar a que el miedo disminuya.
- La computadora decidirá la importancia/urgencia del reporte/emergencia dando a llevar acciones de emergencia.
- Gravedad de emergencia determina uso de tecnología.

Pregunta: Alguna inquietud sobre el uso de esta tecnología?

- La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

Pregunta: En qué situación usarán esta tecnología?

- Una pelea en la calle, un malestar corporal, cuestiones de vida, abuso doméstico
- Cada uno tiene la definición de vigilancia, pero que tal la definición de emergencia?
- La definición de emergencia es diferente con cada persona.
- Si nos basamos en la definición de emergencia sólo en cuanto estemos en peligro inmediato o en tiempos mínimos/ de transcurrencia alarmante/peligrosa el uso de será implementado o limitado solo a instantes inmediatos de peligro

Pregunta: Para qué sirve el reporte de la computadora?

- Para reportar algo que ya sucedió o que son recurrentes.
- Basado en el concepto de emergencia, las personas pueden tomar el método adecuado para reportar su caso y a través del medio necesario.
- Los reportes no son anónimos.
- Los datos son recolectados aun, a pesar de la opción escogida.

Pregunta: Qué les recomendarían a los políticos?

- Que sea multi-idioma, implementar audio, implementar sistemas que ayuden a múltiples personas con diversas capacidades/necesidades

Pregunta: Algún otro comentario en general sobre la tecnología de vigilancia?

- Si es usada de manera adecuada y como han dicho está bien.

- El uso de la tecnología es bueno para dar respuesta para todas las cosas y personas.

Consejo:

- Den información más información sobre lo que están haciendo. (transparencia/divulgación de información)

- Que haya más transparencia.

Ser transparentes sobre la colección de datos, para que haya discusiones y decisiones Informadas, en todas las tecnologías implementadas/por implementar.

Byrd Barr Place

2/28/2019 Surveillance Technology Focus Group

Thursday, February 28, 2019
1:42 PM

Disclaimer: some of these notes are written in first-person. These should not be considered direct quotes

Videos:

- Acyclica: sensors recognize when a wifi enabled device is in range of it. Attached to street lights
- 911 recorder: records the conversation with the person calling 911, and conversation with the dispatched officers
- CopLogic: Online police report, treated as a regular policy report
- Computer Aided Dispatch
- Seattle City Light: Binoculars for meter readers; sensor to see if someone is stealing electricity

Tom: Read definition of surveillance

Craig: invasion of privacy?

- Electric one: I never even know they had the sensor one.

Community Member: used to be in the tech industry for thirty years. Writing a book about surveillance and technology
Wanda: I like the online police report. If someone is experiencing a crisis or trauma, you can go ahead and report it.

- Surveillance, I understand the concern, but overall I think it's a good thing. There is good and bad in any location, you'll find people who are taking advantage of it, but hopefully there are systems in place.
- Used to work nights, and catching the bus at night is scary. Having the cameras and police out when catching the bus helps, I appreciate that. No one likes to be watched, but if it's gonna keep people safe, that's a good thing.

Mercy: security is a great safety issue
Craig: there are some parts of the neighborhood/city that need to be watched, and some that need to be left alone
Wanda: as long as it's even
Craig: Sometimes it's not even
Both: There are hot spots though

Which of the surveillance technologies do you think could be abused to pinpoint specific communities?

IG: The Computer Aided Dispatch

Talking about the International District:

- Lots of businesses and residential crammed together in a larger space
- Talking about a great community member who died; if they had surveillance technology them, maybe they would have found his killer

"Some neighborhoods need to be watched"

- Gangs; drug use

Tom: getting back to CAD, how do we feel about the information that is stored

- Craig: there are concerns, but who is allowed to see it, how is it stored? That's a concern
    - Is it used for BOLOs? Is it everyone who is in the area, all of the police officers? Or is there some discretion as to which police officers would be given the information?
- Wanda: plenty of people are arrested who "fit a description"
    - Discussion about the racial discrimination: how people who think that "all [insert race here] look alike".
    - Individuals may think like that, but police officers have the capability to ruin someone's life.
- Marjorie: just recently got a smart phone, and it's new to me that someone could know where I'm going and I wouldn't be aware of it
    - Without my consent.
- Mercy: grew up with the idea that big brother is watching you
    - Tracking how many times I go to the library seems like a waste of money
    - People who are not law abiding citizens, they are the ones to be worried
- Craig: What about selling weed, coke, etc. Should they be worried?
    - Mercy: well at least in Seattle, it's ok to sell
- Mercy: big brother is watching. We already know that, it's just more obvious now
- There is a lot of technology that we are not made aware of

Tom: So acyclica, is it worth it? Some people worried it's tracking, is it something that we can live without?

- Should we put up signs that this road is tracked?
    - Viron: Maybe
    - Mercy: let people out there know that you're on camera.
    - Viron: does it work if your device is not turned on?

Tom: what do you want to tell the city council about tech that is collecting personal information?

- Wanda: they should get our individual consent
- Martha: putting it on the ballot doesn't mean that you are getting individual consent, because if you vote no but it still passes, you didn't give your consent
- Deana: there are some places around Capitol Hill that I don't feel safe at at night
    - Talking about fire department responding to a fire in her building: when one building alarm system goes off, it goes directly to the fire department - affects multiple buildings.
        - Response time is very good.
    - I choose to turn off the GPS tracking, because I don't need people to know where I'm at
        - If others are watching where I'm at, that's an invasion of privacy. I should be able to walk out my front door and go wherever I want without anyone knowing.
- Location privacy: you can tell a lot about a person based on where they go, and tracking that can build a pretty extensive profile of who you are
- IG: now that I know they are tracking, I will turn it off.

Mr. Surveillance: Surveillance is always secret, and it's an aggressive act. It's meant to exert power over others.

Do you think any individual could raise enough concern that it would change anything?

- Resounding no
- Maybe with a larger group
    - Maybe with the whole city

SCL binoculars:

- Craig: they should warn their customers and let them know they are coming into their yard/looking through binoculars.
- Wanda: as long as they aren't looking in people's windows.
    - When we're walking down the street, it's a little different. Certain neighborhoods do need more surveillance than others

Regarding being watched in public:

- Eydie: in public, it depends on how long. If it's a short period of time, that's one thing, but if you're tracked the whole time you're out, it's unreasonable.
    - I don't know what the solutions would be.
    - Even when the meter read just walks into your yard, it's unnerving.
    - What’s the purpose of tracking it this way?
- Mercy: (referring to the acyclica) Why are they doing it all the time? Have they not gotten the information yet?
    - They should already know what the traffic flow would be.
    - We lost a lane to the bicyclist
- Craig: facial recognition used on the street is bad.
- Vyron: sometimes you can't walk down the street and shake someone's hand without getting in trouble
- Mr. Surveillance: The technology has gotten ahead of the law, and it means they have to pay less people

Tom: Are we willing to accept more technology to have less police?

- Craig: how about just making it even? Police have an image to people of color; they are afraid of why they are going to be there. We can police ourselves
- Wanda: I disagree. There are some who think there should be less, but there are also a lot of people who worry about walking down the street
    - As a woman and DV survivor, I appreciate the police and appreciate living in a country where I can call a number for help.
    - I have a big problem with the shooting of unarmed black men, but as an individual I still appreciate the police.
    - But I have a problem being tracked, and I have a problem being watched in my home.
- General comment: The number of police being on the corner is a touchy situation

- Knowing the police that are on your corner makes a difference. They can police the community better if there is more of a relationship between the two.
- Craig: it has to be both, even. You can't trade off the technology for the police.
- Mr. Surveillance: The trend is they want to go to more technology and less police.

Tom: If right now we have lots of technology, and we want a balance, then how do we do that?

- Craig: keep it the way it is but clean up the police department. Make sure the people who are working there are good at their jobs, not biased or discriminating

CopLogic: making police reports online

- Craig: I think it's stupid.
  - Would use that technology for stupid crimes
- Mercy: you could report your neighbor for silly things
  - Anonymous reporting of crimes that could target people for things they might not call 911 for
- Wanda: there were some lines of traffic where I saw cars lined up with their windows smashed in; nothing taken, but glass all over the place.
  - Police response when called: maybe you should get a cheaper type of car
  - Would he have said that to us if we were a different skin color, or lived in a different neighborhood?
- IG: I think it's a bad thing: someone could make up a story and the officer didn't have to check it.
- Marjorie: I think the online reporting could be abused

City of Seattle

Appendix E: All Comments Received from Members of the Public

ID: 10617696279

Submitted Through: Survey Monkey

Date: 3/25/2019 1:32:51 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

Higher Concerns: 1) Software-as-a-Service (SaaS) solution instead of locally (Seattle IT/SPD) hosting CopLogic. Since this is hosted/managed by LexisNexis, LexisNexis has control of the data (either for legal usage of the data as outlined in the contract with them or for possible exposure if they were to have a security breach). 2) Data retention period for data entered into CopLogic isn't specified in the SIR or the IT/LexisNexis contract. It is unclear what happens to a report on the CopLogic side after it is submitted to the SPD RMS by an officer. Is it automatically deleted from CopLogic then? More broadly, regardless on whether a report is submitted to the SPD RMS, how long is that data retained in CopLogic? 3) No special data handling/security/privacy requirements for "personal information" are placed on LexisNexis. The Seattle IT/LexisNexis contract defines "personal information" (and with a reasonably good definition from the privacy side) but the contract does NOT go on to state any special requirements for "personal information". Per the contract, LexisNexis can handle "personal information" in the same manner as it handles "city data". 4) Citizens with lower technical skills, citizens without Internet access, and/or citizens with confusing/expensive Internet plans may be unable or dissuaded from submitting reports to SPD. People who are most likely to fall into those categories are likely already disadvantaged in other areas of life as well (older citizens, minorities, low-income, disabled, etc.). Lesser Concerns: 1) No 2-step-verification/2-factor-authentication (2SV/2FA) for officer login to CopLogic, but, per SPD, the officer-login side of CopLogic is not Internet-facing (you have to be on SPD's network to access it) so the risk is reduced. 2) Per the response at the SIR tech fair, CopLogic's access back to the SPD RMS is one-way, write-only. However, it is unclear how credentials are scoped and if that means CopLogic's RMS creds could be used to write to any arbitrary records in the SPD RMS or if it can only impact CopLogic-generated records in the RMS. That being said, even if the creds have overly scoped permissions, this would be a security issue, not a privacy issue (since the creds supposedly don't have read access). 3) Email addresses is a required field when submitting a report via CopLogic, whereas it would be optional for an in-person report. However, at least the Seattle IT/LexisNexis contract prohibits the use of the data entered via CopLogic from being used for targeted advertising. 4) Accidental release of personal information of citizens via PRA requests. However, per the SPD rep at the SIR tech fair, SPD redacts names, addresses, phone numbers, building access codes, etc. as a matter of practice when responding to PRA requests, so the likelihood of release seems low here. 5) From the draft SIR 6.3.1, "Once disclosed in response to PRA request, there are no restrictions on non-City data use; however, applicable exemptions will be applied prior to disclosure to any requestor who is not authorized to receive exempt content." This sentence was unclear to me, specifically, for example, if

SPD released the records for a non-citizen to that non-citizen, would that then mean SPD could freely share those same records with ICE? But the SPD rep at the tech fair, said that SPD would only ever release records they are authorized to do so (their behavior doesn't change post-PRA-release), the sentence in the SIR was simply explaining that SPD isn't responsible for what happens with the data that is released (the receiver of that data could further share that data in ways that SPD would not).

What value, if any, do you see in the use of this technology?

It is likely significantly more convenient to most citizens. It likely also reduces the number of officers needed.

What do you want City leadership to consider about the use of this technology?

1) LexisNexis Desk Officer Reporting System (DORS) aka CopLogic apparently supports a locally hosted option ("You may also choose to host the application internally; it's completely up to you!" taken from: https://secure.coplogic.com/products/dors-overview.shtml). Assuming that the locally hosted option is entirely self-contained (that is, it's not just the web form that is locally hosted, but also the backend data storage for CopLogic), then it would be better to for the City of Seattle (SPD/IT) to locally host it instead, since there would be no exposure of citizen's information to a third-party just to report simple crimes. This would improve citizen's privacy and reduce the risk if there was a LexisNexis security breach. 2) Data retention is another issue. Neither the draft SIR nor the IT/LexisNexis contract specify the data retention policy for data on the CopLogic side (not the SPD RMS). What happens to a CopLogic report after an officer submits it to the SPD RMS? How long does LexisNexis store the reports? What's the lifecycle for reports that are found inadequate/invalid by the officer? Does the officer delete them? Do reports in CopLogic "expire" and therefore get auto-deleted after some length of time? What length of time? 3) The Seattle IT/LexisNexis contract should be altered to actually place specific data handling/security/privacy requirements on LexisNexis for "personal information" entered in via CopLogic. 4) When SPD people or systems direct citizens to use online reporting, it should be made clear that they aren't required to do so (if they are unable or unwilling to report online they should still be able to report directly). This is to ensure disadvantaged populations still have a mechanism for reporting minor crimes.

Do you have any other comments?

It is unclear to the public what vendor SPD uses for their RMS; and what (if any) additional data processing and/or data analysis capabilities are available on top of that. The SPD RMS should go through similar scrutiny by the public and the council.

Are there any questions you have, or areas you would like clarification?

It would be helpful if once initial public release of the draft SIRs happened, that within each SIR there was a version history noting what has changed over time (so first release to the public = version 1; say a draft SIR has a contract(s) added, then the version history table says versions 2 noting the date & changes that were the added contracts in whichever Appendix).

City of Seattle

ID: 10617457428

Submitted Through: Survey Monkey

Date: 3/25/2019 11:57:26 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

No concerns except that we need this because we're desperately short of police officers.

What value, if any, do you see in the use of this technology?

It gives us a chance of reporting crimes in a timely fashion.

What do you want City leadership to consider about the use of this technology?

It saves a lot of money.

Do you have any other comments?

Are there any questions you have, or areas you would like clarification?

Are they planning to increase the dollar value of what you can report using this? It seems low.

ID: 11

Submitted Through: Focus Group

Date: 2/28/2019

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

The different types of communities that do not have access (whether linguistic/ rapport with police department) to the technology. Not equal playing field. The anonymous remote reporting may lead to an increase in religious profiling/targeting of criminalized identities for harmless behavior. SPD's relationship with the IDF is just one example of a poor rapport of the department with more marginalizaed communities (militarization of the police).

What value, if any, do you see in the use of this technology?

What do you want City leadership to consider about the use of this technology?

Do you have any other comments?

Are there any questions you have, or areas you would like clarification?

ID: 8

Submitted Through: Focus Group

Date: 2/28/2019

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

targeting of people of color - who have been seen/depicted as more intimidating -- requires individual perceptions of others (ex: harassment)

What value, if any, do you see in the use of this technology?

saving time, person power, and money especially with things such as car break ins, hit and run

What do you want City leadership to consider about the use of this technology?

The validity of reports that are coming through. How do we ensure reports are not hurting communities of color. Crime-mapping which can happen with this technology

Do you have any other comments?

this can target locations that have been frequented by communities of color (masjid, gathering spaces, grocery stores, community centers)

Are there any questions you have, or areas you would like clarification?

what happens with data, how long is it kept in their systems

ID: 6

Submitted Through: Focus Group

Date: 2/27/2019

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

Not available in other languages -- not accessible form is a little confusing and long

What value, if any, do you see in the use of this technology?

saves time on the department side. Makes it easier to report on individual/community member's time

What do you want City leadership to consider about the use of this technology?

generally, making it more accessible to more community members

Do you have any other comments?

Would like to see statistics on all reports collected by this tech. What gets most reported, any follow-up upon review, by reviewing any improvements, etc.

Are there any questions you have, or areas you would like clarification?

ID: 5

Submitted Through: Focus Group

Date: 2/27/2019

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

My Concern: will data be safe kept.

What value, if any, do you see in the use of this technology?

convenience and effective and accountable

What do you want City leadership to consider about the use of this technology?

allow enough trial times - testing times- before applying

Do you have any other comments?

Are there any questions you have, or areas you would like clarification?

Again, how to keep data safe

ID: 2

Submitted Through: Focus Group

Date: 2/28/2019

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

People misusing/abusing the resource; can the number of reports become so excessive to the point where they can't all properly be tended to?

What value, if any, do you see in the use of this technology?

Great for accessibility for folks who can't report in person or over the phone. May be easier to convey information as opposed to talking with cops (who I've had multiple negative experiences with reporting crimes)

What do you want City leadership to consider about the use of this technology?

See number 1.

Do you have any other comments?

Are there any questions you have, or areas you would like clarification?

ID: 10549555511

Submitted Through: Survey Monkey

Date: 2/22/2019 3:28:12 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

While there are some incidents in which this is useful, such as needing a police report for insurance to prove your car was broken into, removing human interaction from this process is concerning in its potential to embolden people to report "suspicious activity" without review, as online reports are only available for incidents in which no police follow up is needed or possible. I see the potential for city residents to act upon biases and equate race, religion, or other aspects of identity with crime or suspicious activity, and for these reports to go without verification or investigation. Consequently, I have concerns for increased police presence in neighborhoods deemed to be high-crime or suspicious, creating a vicious circle of continued mistrust between the police and community members.

What value, if any, do you see in the use of this technology?

Only for incidents with absolutely no consequence for other people, like reporting a car break in for insurance purposes.

What do you want City leadership to consider about the use of this technology?

I would like City Council to consider the potential consequences of this reporting tool and focus more resources toward improving community trust

Do you have any other comments?

Are there any questions you have, or areas you would like clarification?

ID: 10533827008

Submitted Through: Survey Monkey

Date: 2/15/2019 3:11:01 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

This will be used to disproportionately report the homeless and people of color for existing in a place where someone feels uncomfortable

What value, if any, do you see in the use of this technology?

None whatsoever

What do you want City leadership to consider about the use of this technology?

Quit while you're ahead and put that money towards community welfare projects, affordable housing, and helping the homeless and addicted

Do you have any other comments?

Tax Amazon

Are there any questions you have, or areas you would like clarification?

Appendix F: Department Responses to Public Inquiries

Community Comment Responses:

FG	2/28/2019	SPD: CopLogic	What happens with data? How long is it kept in their systems?

Reports that are generated in the CopLogic system are auto-deleted from the LexisNexis servers after 120 days per the CopLogic system configuration. Reports that are rejected by SPD employees after their review are deleted immediately.

FG	2/27/2019	SPD: CopLogic	How do we keep the data safe?

The portal SPD staff use to view, approve, and import reports from CopLogic into SPD's records management system requires "Triple Lock" authentication. "Triple Lock" means that each staff member has a unique username and password, IP restricted logins (they must be authenticated on the SPD network) and use a private URL to log into the system. Only certain CJIS certified employees who have roles associated with the CopLogic online reporting process are given this access. Additionally, the LexisNexis CopLogic system is CJIS Complaint and per the contract with LexisNexis, the City requires the vendor to have the system tested for security vulnerabilities articulated in the industry standard OWASP Top-10.

FG	2/28/2019	SPD: CopLogic	How do we ensure reports are not hurting communities of color?

Because the use of this technology is an opt-in decision by its community users and crimes with known or describable suspects are not reportable through CopLogic, the risks of improper or biased usage are limited. This system does not allow for reports of crimes with known or describable suspects. All information, once reviewed by authorized SPD employees, is electronically transferred into SPD's records management system. The SPD employees tasked with this review are bound by SPD policies pertaining to electronic communications, computer and data usage, and bias-based policing. Additionally, all reports that can be made through the online reporting system can also be made utilizing other methods including by telephone.

FG	2/28/2019	SPD: CopLogic	Can the number of reports become so excessive to the point where they can't all be properly tended to?

All requests for service, no matter what the method for making that request, are responded to by SPD. The online reporting tool, CopLogic, allows for certain non-emergency requests with no known or describable suspect to be reviewed by SPD officers in an efficient manner that frees up patrol officers allowing them to respond faster to requests in a timely fashion.

FG	2/21/2019	SPD: CopLogic	What is the usefulness of the information that is not followed up on? And how does it help the people it is actually serving?

All reports made through the CopLogic online reporting system are reviewed by SPD officers. Often a report is made even when there is little that an SPD officer can act on, for example when a property theft happens and there is no known or describable suspect. An insurance claim may still require that a police report be filed and the CopLogic system allows community members to file this report in a convenient way. Community members wishing to speak with SPD employees to make their report may still initiate their report over the phone or in person at a precinct.

FG	2/21/2019	SPD: CopLogic	How is SPD going to do what they can to make sure that this doesn't negatively impact communities they are already having issues with that already feels threaten and criminalize by communities?

Because the use of this technology is an opt-in decision by its community users and crimes with known or describable suspects are not reportable through CopLogic, the risks of improper or biased usage are limited. This system does not allow for reports of crimes with known or describable suspects. All information, once reviewed by authorized SPD employees, is electronically transferred into SPD's records management system. The SPD employees tasked with this review are bound by SPD policies pertaining bias-based policing. Additionally, all reports that can be made through the online reporting system can also be made utilizing other methods including by telephone.

FOLS FG	2/27/2019	SPD: CopLogic	Will they keep the data safe on coplogic?

The portal SPD staff use to view, approve, and import reports from CopLogic into SPD's records management system requires "Triple Lock" authentication. "Triple Lock" means that each staff member has a unique username and password, IP restricted logins (they must be authenticated on the SPD network) and use a private URL to log into the system. Only certain CJIS certified employees who have roles associated with the CopLogic online reporting process are given this access. Additionally, the LexisNexis CopLogic system is CJIS Complaint and per the contract with LexisNexis, the City requires the vendor to have the system tested for security vulnerabilities articulated in the industry standard OWASP Top-10. The Consultant Agreement limits the vendor's (LexisNexis) use and storage of all information collected by or on behalf of the City to only purposes used for providing the service in the CopLogic contact and Consultant Agreement. They are prohibited from using City data or personal information to engage or enable another party to engage in marketing or targeted advertising. Additionally, no access or information shall be provided to any employee or agent of any federal immigration agency without prior review and consent of the City.

FOLS FG	2/27/2019	SPD: CopLogic	Can the data be hacked?

The portal SPD staff use to view, approve, and import reports from CopLogic into SPD's records management system requires "Triple Lock" authentication. "Triple Lock" means that each staff member has a unique username and password, IP restricted logins (they must be authenticated on the SPD network) and use a private URL to log into the system. Only certain CJIS certified employees who have roles associated with the CopLogic online reporting process are given this access. Additionally, the LexisNexis CopLogic system is CJIS Complaint and per the contract with LexisNexis, the City requires the vendor to have the system tested for security vulnerabilities articulated in the industry standard OWASP Top-10.

FOLS FG	2/27/2019	SPD: CopLogic	what if you report your neighbour and your neighbor hacks the system and find out?

This system does not allow for reports of crimes with known or describable suspects, therefore you would not be able to use the CopLogic online reporting system to report a crime committed by a neighbor. Please contact 9-1-1, the SPD non-emergency number, or your local SPD precinct to file a report involving a known suspect.

FOLS FG	2/27/2019	SPD: CopLogic	What is the money amount limit for coplogic/why is there a limit for coplogic?

Theft of property valued at less than $500 may be reported using CopLogic. The online reporting tool is designed to allow community members to report certain low-level property crimes only. When the value of stolen property exceeds $500 it is more appropriate for an officer to respond in person to take the crime report.

FOLS FG	2/27/2019	SPD: CopLogic	Is there an option that someone and report a crime for someone else?

For community users who are not part of the retail users program, there is not an option to use CopLogic online reporting to report a crime for someone else. If a community member needs to make a report on behalf of another person, they will need to contact SPD either by phone or in person.

FOLS FG	2/27/2019	SPD: CopLogic	Is there resources to support these technologies? Is there translations so that it is accessible for everyone? Will this accommodate everyone?

With the support of Seattle IT, CopLogic benefits both the community and the Seattle Police Department by freeing resources in the 9-1-1 center, eliminating the need for patrol officers to respond in person to take some crime reports. The CopLogic online reporting tool, as with the SPD and City of Seattle websites, are not currently available in translations. Community members who need to request services need to contact SPD by phone or in person for translation services.

FOLS FG	2/27/2019	SPD: CopLogic	How will other people know of the technology if they can't come to focus group meetings? Such as flyers? Social media?

Links to the CopLogic online reporting system are prominently displayed on the Seattle Police website and is promoted on other SPD social media outlets such as Facebook, Twitter, and the Seattle Police Blotter. Additionally, callers to the non-emergency number are informed about online reporting and given the option to make their report online.

City of Seattle

Appendix G: Letters from Organizations or Commissions

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

March 12th, 2019

Seattle City Council
600 4th Ave
Seattle, WA 98104

Re: Surveillance Ordinance Group 2 Public Comment

We would like to first thank City Council for passing one of the strongest surveillance technology policies in the country, and thank Seattle IT for facilitating this public review process.

These public comments were prepared by volunteers from the Community Technology Advisory Board (CTAB) Privacy & Cybersecurity Committee, as part of the surveillance technology review defined in Ordinance 125376. These volunteers range from published authors, to members of the Seattle Privacy Coalition, to industry experts with decades of experience in the information security and privacy sectors.

We reviewed and discussed the Group 2 Surveillance Impact Reports (SIRs) with a specific emphasis on privacy policy, access control, and data retention. Some recurring themes emerged, however, that we believe will benefit the City as a whole, independent of any specific technology:

- **Interdepartmental sharing of privacy best practices**: When we share what we've learned with each other, the overall health of the privacy ecosystem goes up.
- **Regular external security audits**: Coordinated by ITD (Seattle IT), routine third-party security audits are invaluable for both hosted-service vendors and on-premises systems.
- **Mergers and acquisitions**: These large, sometimes billion-dollar ownership changes introduce uncertainty. Any time a vendor, especially one with a hosted service, changes ownership, a thorough review of any privacy policy or contractual changes should be reviewed.
- **Remaining a Welcoming City**: As part of the Welcoming Cities Resolution, no department should comply with a request for information from Immigration and Customs Enforcement (ICE) without a criminal warrant. In addition, the privacy of all citizens should be protected equally and without consideration of their immigration status.

Sincerely,

Privacy & Cybersecurity Committee volunteers
Torgie Madison, Co-Chair
Smriti Chandashekar, Co-Chair
Camille Malonzo
Sean McLellan
Kevin Orme
Chris Prosser
Rabecca Rocha
Adam Shostack
T.J. Telan

Community Technology Advisory Board
Steven Maheshwary, CTAB Chair
Charlotte Lunday, CTAB Co-Vice Chair
Torgie Madison, CTAB Co-Vice Chair
Smriti Chandashekar, CTAB Member
Mark DeLoura, CTAB Member
John Krull, CTAB Member
Karia Wong, CTAB Member

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SFD: Computer-Aided Dispatch (CAD)

Comments

The use of a centralized Computer-Aided Dispatch (CAD) system is essential to protecting the health and safety for all Seattle citizens. The National Fire Protection Association (NFPA) standards outline specific alarm answering, turnout, and arrival times[1] that could only be accomplished in a city of this size with a CAD system.

In addition, with over 96,000 SFD responses per year (2017)[2], only a computerized system could meet the state's response reporting guidelines established in RCW 35A.92.030[3].

CentralSquare provides the dispatch service used by SFD. CentralSquare is a new entity resulting from the merger of Superion, TriTech, Zuercher, and Aptean[4] in September 2018.

Recommendations

- Tritech, the underlying technology supplying SFD with CAD services, has been in use since 2003 [SIR 4.3], making it 16 years old. As with any technology, advancements in security, speed, usefulness, and reliability come swiftly. Due to the age of the technology, we recommend conducting a survey into the plausibility of replacing Tritech as SFD's CAD solution.

- Tritech was merged very recently into CentralSquare in one of the largest-ever government technology mergers to date. Due diligence should be exercised to ensure that this vendor is keeping up to date with industry best practices for security and data protection, and that their privacy policies are still satisfactory after the CentralSquare merger. We recommend ensuring that the original contracts and privacy policies have remained unchanged as a result of this merger.

---

[1] "NFPA Standard 1710." https://services.prod.iaff.org/ContentFile/Get/30541
[2] "2017 annual report - Seattle.gov." https://www.seattle.gov/Documents/Departments/Fire/FINAL%20Annual%20Report_2017.pdf
[3] "RCW 35A.92.030: Policy statement—Service ... - Access WA.gov." https://app.leg.wa.gov/rcw/default.aspx?cite=35A.92.030
[4] "Superion, TriTech, Zuercher, and Aptean's Public Sector Business to " 5 Sep. 2018, https://www.tritech.com/news/superion-tritech-zuercher-and-apteans-public-sector-business-to-form-centr a

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SDOT: Acyclica

Comments

Traffic congestion is an increasingly major issue for our city. Seattle is the fastest-growing major city in the US this decade, at 18.7% growth, or 114,00 new residents[5]. Seattle ranks sixth in the nation for traffic congestion[6]. The need for intelligent traffic shaping and development has never been greater. Acyclica, a service provided by Western Systems and now owned by FLIR[7], is an implementation of surveillance technology specifically designed to address this problem.

We were happy to see the 2015 independent audit of Acyclica's systems [SIR 8.2]. This is an excellent industry best practice, and one that we'll be recommending to other departments throughout this document.

In addition, we are pleased to see the hashing function's salt value rotated every 24-hours [SIR 4.10]. This ensures that even the 10-year retention policy [SIR 5.2] cannot be abused to correlate multiple commute sessions and individually identify a person.

Recommendations

- FLIR Systems' acquisition of Acyclica is a recent development (September 2018). We recommend verifying that the Western Systems terms [SIR 3.1] still apply. If they have been superseded by new terms from FLIR Systems, those should be subject to an audit by SDOT and Seattle IT. Specifically, section 2.5.1 of Western Systems' terms must still apply:

  > 2.5.1. It is the understanding of the City that the data gathered are encrypted to fully eliminate the possibility of identifying individuals or vehicles. In no event shall City or Western Systems and its subcontractors make any use of the data gathered by the devices for any purpose that would identify the individuals or vehicles included in the data.

- FLIR Systems is known primarily as an infrared technology vendor. Special care should be taken if FLIR/Acyclica attempt to couple IR scanning with WiFi/MAC sniffing. Implementation of an IR system would necessitate a new public surveillance review.

---

[5] "114,000 more people: Seattle now decade's fastest-growing big city in ...." 24 May. 2018, https://www.seattletimes.com/seattle-news/data/114000-more-people-seattle-now-this-decades-fastest-growing-big-city-in-all-of-united-states/
[6] "INRIX Global Traffic Scorecard." http://inrix.com/scorecard/
[7] "FLIR Systems Acquires Acyclica | FLIR Systems, Inc.." 11 Sep. 2018, http://investors.flir.com/news-releases/news-release-details/flir-systems-acquires-acyclica

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SCL: Binoculars, Check Meter, SensorLink

Comments

As these three technologies are serving the same team and mission objectives, we will review them here in a combined section.

The mission of the Current Diversion Team (CDT) is to investigate and gather evidence of illegal activity related to the redirection and consumption of electricity without paying for its use. As such, none of these technologies surveil the public at large. They instead target specific locations and equipment, albeit without the associated customer's knowledge.

It appears as though all data collected through the Check Meter Device and SensorLink Amp Fork are done without relying on a third-party service, so the usual scrutiny of a vendor's privacy policies does not apply.

Recommendations

- **Binoculars**: We have no recommendations for the use of binoculars.
- **Check Meter Device & SensorLink Amp Fork**: As noted in the comments above, we have no further recommendations for the use of the Check Meter Device and SensorLink Amp Fork technologies.
- **Racial Equity**: As with any city-wide monitoring practice, it can be easy to more closely scrutinize one neighborhood over another. Current diversion may be equally illegal (and equally prevalent) across the city, but the enforcement of this law may be unevenly applied. This could introduce racial bias by disproportionately burdening specific neighborhoods with a higher level of surveillance.

  As described, DPP 500 P III-416 section 5.2[8] asserts that all customers shall receive uniform consideration [SIR RET 1.7]. To ensure this policy is respected, we encourage City Light to track and routinely review the neighborhoods where CDT performs investigations, with a specific emphasis on racial equity. This information should be made publicly available.

  When asked at the February 27th Surveillance Technology public meeting, SDOT indicated that no tracking is currently being done on where current diversion is enforced.

[8] "SCL DPP 500 P III-416 Current Diversion - Seattle.gov." 11 Jan. 2012, http://www.seattle.gov/light/policies/docs/III-416%20Current%20Diversion.pdf

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: 911 Logging Recorder

Comments

This is a technology that the general public would likely already assume is in place. Some of the more sensational 911 call logs have been, for example, played routinely on the news around the country. Since it would not alarm the public to know that 911 call recording is taking place, our recommendations will focus primarily on data use, retention, and access control.

Call logging services are provided by NICE Ltd., an Israeli company founded in 1986. This vendor has had a troubling history with data breaches. For example, a severe vulnerability discovered in 2014 allowed unauthorized users full access to a NICE customer's databases and audio recordings[9]. Again, in 2017, a NICE-owned server was set up with public permissions, exposing phone numbers, names, and PINs of 6 million Verizon customers[10].

Recommendations

- SIR Appendix K includes a CJIS audit performed in 2017. SIR section 4.10 also mentions that ITD (Seattle IT) periodically performs routine monitoring of the SPD systems.

  However, given the problematic history with the quality of the technology vendor, if any of the NICE servers, networks, or applications were installed by the vendor (or installation was overseen/advised by the vendor), we recommend an external audit of the implementation of the call logging technology.

- SIR sections 3.3 and 4.2 outline the SPD-mandated access control and data retention policies, however it is not apparent if there is a policy that strictly locks down the use of this technology to a well-defined list of allowed cases. We recommend formally documenting the allowed 911 Logging use cases, and creating a new SIR for any new desired applications of this technology.

  With a 90-day retention policy [SIR 4.2], and with SPD receiving 900,000 calls per year[11], there are about 220,000 audio recordings existing at any given time. This is enough for a data mining, machine learning, or voice recognition project.

---

[9] "Backdoor in Call Monitoring, Surveillance Gear — Krebs on Security." 28 May. 2014, https://krebsonsecurity.com/2014/05/backdoor-in-call-monitoring-surveillance-gear/
[10] "Nice Systems exposes 14 million Verizon customers on open AWS ...." 12 Jul. 2017, https://www.techspot.com/news/70106-nice-systems-exposes-14-million-verizon-customers-open.html
[11] "9-1-1 Center - Police | seattle.gov." https://www.seattle.gov/police/about-us/about-policing/9-1-1-center

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: Computer-Aided Dispatch (CAD)

Comments

As mentioned in the section "SFD: Computer-Aided Dispatch (CAD)" and the section "SPD: 911 Logging Recorder", these dispatch technologies are mandatory for functional emergency services of a city this size. No other system would be able to meet the federal- and state-mandated response times and reporting requirements.

SIR section 4.10 mentions that ITD (Seattle IT) performs routine inspections of the Versaterm implementation.

Versaterm, founded in 1977, provides the technology used by SPD's CAD system. SPD purchased this technology in 2004. In September of 2016, there was a legal dispute between Versaterm and the City of Seattle over a Public Records Act (PRA) disclosure of certain training and operating manuals[12]. The court ruled in favor of Versaterm.

Recommendations

- It is not immediately clear what use cases are described in SIR 2.5 describing data access by "other civilian staff whose business needs require access to this data". All partnerships and data flows between SPD and businesses should be explicitly disclosed.

- This system has been in place for 15 years. As with any technology, advancements in security, speed, usefulness, and reliability come swiftly. Due to the age of the technology, and the potential damaged relationship between Seattle and Versaterm due to the aforementioned legal dispute, we recommend conducting a survey into the plausibility of replacing Versaterm as SPD's CAD solution.

- As mentioned in the introduction to this document, Seattle has adopted the Welcoming Cities Resolution[13]. In honoring this resolution, we recommend that SPD never disclose identifying information, from CAD or any system, to Immigrations and Customs Enforcement (ICE) without a criminal warrant.

---

[12] "Versaterm Inc. v. City of Seattle, CASE NO. C16-1217JLR | Casetext." 13 Sep. 2016, https://casetext.com/case/versaterm-inc-v-city-of-seattle-2
[13] "Welcoming Cities Resolution - Council | seattle.gov." http://www.seattle.gov/council/issues/past-issues/welcoming-cities-resolution

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: CopLogic

Comments

Track 1 - Public reporting of no-suspect, no-evidence, non-emergency crimes

CTAB understands that in cases where no evidence or suspect is available, a crime should be reported (for statistical or insurance purposes) but does not require the physical appearance of an SPD officer.

Track 2 - Retail Loss Prevention

This track is more problematic, as it could be used by retailers as a method to unreasonably detain, intimidate, or invade the privacy of a member of the public accused of, but not proven guilty of, shoplifting.

Recommendations

- **Track 2**: If not already done, retailers should be trained and informed that having a CopLogic login does not allow them to act as if they are law enforcement officers. Members of the public suspected of shoplifting need to have an accurate description of their rights in order to make informed decisions before providing identifying information. Retailers are also held to a lower standard than SPD regarding racial bias. It is virtually guaranteed that people of color are disproportionately apprehended and entered into the retail track of CopLogic.

  We recommend discontinuing Track 2 entirely.

- **Track 1 & 2**: If not already done, SPD, in coordination with Seattle IT, should perform or hire a company to perform an audit of the vendor's systems. If this audit has not been performed in the 8 years since purchasing this system, it should absolutely be done before the 10-year mark in 2020.
- **Track 1 & 2**: It is not immediately clear in the SIR or LexisNexis's Privacy Policy what CopLogic does with these records long-term, after SPD has imported them into their on-premises system. A written statement from LexisNexis on how this data is used, mined, or sold to affiliates/partners should be acquired by SPD.
- **Track 1 & 2**: We recommend migrating CopLogic to an on-premises solution. We found the LexisNexis privacy policy to be obfuscated and vague[14]. Such sensitive information should not be protected by trust alone.

[14] "Privacy Policy | LexisNexis." 7 May. 2018, https://www.lexisnexis.com/en-us/terms/privacy-policy.page

City of Seattle

March 20, 2019

RE: ACLU-WA Comments Regarding Group 2 Surveillance Technologies

Dear Seattle IT:

On behalf of the ACLU of Washington, I write to offer our comments on the surveillance technologies included in Group 2 of the Seattle Surveillance Ordinance process. We are submitting these comments by mail and electronically because they do not conform to the specific format of the online comment form provided on the CTO's website, and because the technologies form groups in which some comments apply to multiple technologies.

These comments should be considered preliminary, given that the Surveillance Impact Reports (SIR) for each technology leave a number of significant questions unanswered. Specific unanswered questions for each technology are noted in the comments relating to that technology, and it is our hope that those questions will be answered in the updated SIR provided to the Community Surveillance Working Group and to the City Council prior to their review of that technology. In addition to the SIR, our comments are also based on independent research relating to the technology at hand.

The 8 technologies in Group 2 are covered in the following order.

I. Acyclica (SDOT)

II. CopLogic (SPD)

III. Computer-Aided Dispatch & 911 Logging Recorder Group

1. Computer-Aided Dispatch (SPD)
2. Computer-Aided Dispatch (SFD)
3. 911 Logging Recorder (SPD)

IV. Current Diversion Technology Group

1. Check Meter Device (Seattle City Light)
2. SensorLink Amp Fork (Seattle City Light)
3. Binoculars/Spotting Scope (Seattle City Light)

ACLU
AMERICAN CIVIL LIBERTIES UNION
Washington

901 Fifth Ave, Suite #630
Seattle, WA 98164
(206) 624-2184
aclu-wa.org

Tana Lin
Board President

Michele Storms
Executive Director

Shankar Narayan
Technology & Liberty Project Director

City of Seattle

I. Acyclica - SDOT

Background

Acyclica technology is a powerful location-tracking technology that raises a number of civil liberties concerns because of its ability to uniquely identify individuals and their daily movements. Acyclica (via its hardware vendor, Western Systems), manufactures Intelligent Transportation System (ITS) sensors called RoadTrend that are used by the Seattle Department of Transportation for the stated purpose of traffic management. These RoadTrend sensors collect encrypted media access control (MAC) addresses, which are transmitted by any Wi-Fi enabled device including phones, cameras, laptops, and vehicles. Collection of MAC addresses, even when hashed (a method of de-identifying data irreversibly),[1] can present locational privacy challenges.

Experts analyzing a dataset of 1.5 million individuals found that just knowing four points of approximate spaces and times that individuals were near cell antennas or made a call were enough to uniquely identify 95% of individuals.[2] In the case of Acyclica's operation in Seattle, the dataset is comprised of MAC addresses recorded on at least 301 intersections,[3] which allows Acyclica to generate even more precise location information about individuals. Not only do the RoadTrend sensors pick up the MAC addresses of vehicle drivers and riders, but these sensors can also pick up the MAC addresses of all nearby individuals, including pedestrians, bicyclists, and people in close structures (e.g., apartments, offices, and hospitals). Acyclica technology's location tracking capabilities means that SDOT's use of Acyclica can not only uniquely identify individuals with ease, but can also create a detailed map of their movements. This raises privacy concerns for Seattle residents, who may be tracked without their consent by this technology while going about their daily lives.

These location-tracking concerns are exacerbated by the lack of clarity around whether SDOT has a contract with Acyclica (see below). Without a contract, data ownership and scope of data sharing and repurposing by Acyclica is unclear. For example, without contractual restrictions, Acyclica

[1] Hashing is a one-way function that scrambles plain text to produce a unique message digest. Unlike encryption—which is a two-way function, allowing for decryption—what is hashed cannot be un-hashed. However, hashed location data can still be used to uniquely identify individuals. While it is infeasible to compute an input given only its hash output, pre-computing a table of hashes is possible. These types of tables consisting of pre-computed hashes and their inputs are called rainbow tables. With a rainbow table, if an entity has a hash, then they only need to look up that hash in their table to then know what the original MAC address was.
[2] Montjoye, Y., Hidalgo, C., Verleysen, M., and Blondel, V. 2013. Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports.* 3:1375.
[3] The SIR states that SDOT has 301 Acyclica units installed throughout the City. However, an attached location excel sheet in Section 2.1 lists 389 Acyclica units, but only specifies 300 locations.

would be able to share the raw data (i.e., the non-aggregated, hashed data before it is summarized and sent to SDOT) with any third parties, and these third parties would be able to use the data in any way they see fit, including combining the data with additional data such as license plate reader or facial recognition data. Acyclica could also share the data with law enforcement agencies that may repurpose the data, as has happened with other City data. For example, in 2018, U.S. Immigration and Customs Enforcement (ICE) approached Seattle City Light with an administrative subpoena demanding information on a particular customer location, including phone numbers and information on related accounts.[4] ICE also now has agency-wide access to a nationwide network of license plate readers controlled by Vigilant Solutions,[5] indicating the agency may seek additional location data for immigration enforcement purposes in the future. Data collected via Acyclica should never be used for law enforcement purposes.

The uncertainty around the presence or absence of a contract contributes to two key issues: (1) lack of a clearly defined purpose of use of Acyclica technology; and (2) lack of clear restrictions on the use of Acyclica technology that track that purpose. With no contract, SDOT cannot enforce policies restricting the use of Acyclica technology to the intended purpose.

There are also a number of contradictory statements in the SIR concerning the operation of Acyclica technology,[6] as well as discrepancies between the SIR, the information shared at the technology fair (the first public meeting to discuss the Group 2 technologies),[7] and ACLU-WA's conversation with the President of Acyclica, Daniel Benhammou. All these leave us with concerns over whether SDOT fully understands (and the SIR reflects) the capabilities of the technology. In addition, there remain a number of critical unanswered questions that the final SIR must address (set forth below).

Of additional concern is the recent acquisition of Acyclica by FLIR Systems, an infrared and thermal imaging company funded by the U.S. Department of Defense.[8] As of March 2019, FLIR has discontinued Acyclica RoadTrend sensors.[9] Neither the implications of the FLIR acquisition nor the discontinuation of the RoadTrend sensors are mentioned in the SIR—but if the sensors used will change, the SIR should make clear how that will impact the technology.

a. Specific Concerns

- *Inadequate Policies Defining Purpose of Use.* Policies cited in the SIR are vague,

[4] https://crosscut.com/2018/02/immigration-officials-subpoena-city-light-customer-info
[5] https://www.theverge.com/2018/3/1/17067188/ice-license-plate-data-california-vigilant-solutions-alpr-sanctuary
[6] Explained in further detail in 1. Acyclica – SDOT *Major Concerns* below.
[7] http://www.seattle.gov/tech/initiatives/privacy/events-calendar#/?i=3
[8] https://www.crunchbase.com/acquisition/flir-systems-acquires-acyclica--e6043a1a#section-overview
[9] https://www.flir.com/support/products/roadtrend#Specifications

short, and impose no meaningful restrictions on the purposes for which Acyclica devices may be used.[10] Section 1.1 of the abstract set forth in the SIR states that Acyclica is used by over 50 agencies to "to help to monitor and improve traffic congestion." Section 2.1 is similarly vague, providing what appear to be examples of some types of information the technology produces (e.g., calculated average speeds) in order to facilitate outcomes (correcting traffic signal timing, providing information to travelers about expected delays, and allowing SDOT to meet traffic records and reporting requirements)—but it's not clear this list is exhaustive. Section 2.1 fails to describe the purpose of use, all the types of information Acyclica provides, and all the types of work that Acyclica technology facilitates. All these must be clarified.

- *Lack of Clarity on Whether Acyclica and SDOT have a Written Contract.* The SIR does not state that any contract exists, and in the 2018 conversation ACLU-WA had with Benhammou, he stated that there was no contract between the two parties. However, at the 2019 technology fair, the SDOT representative affirmatively stated that SDOT has a contract with Acyclica. As previously mentioned, the lack of a contract limits SDOT's ability to restrict the scope of data sharing and repurposing. The only contractual document provided appears to be a terms sheet in Section 3.0 detailing SDOT's terms of service with Western Systems (the hardware vendor that manufactures the Acyclica RoadTrend sensors), which states that Western Systems only deals with the maintenance and replacement of the hardware used to gather the data, and not the data itself.

- *Lack of Clarity on Data Ownership.* At the technology fair, the SDOT representative stated that SDOT owns all the data collected (including the raw data), but the SIR only states that the aggregated traffic data is owned by SDOT. In the 2018 conversation, Benhammou stated that Acyclica owns all the raw data. There is an apparent lack of clarity between SDOT and Acyclica concerning ownership of data that must be addressed.

- *Data Retention Periods are Unclear.* Section 5.2 of the SIR states that there is a 10-year internal deletion requirement for the aggregated traffic data owned by SDOT, but pg. 37 of the SIR states that "the data is deleted within 24 hours to prevent tracking devices over time." In the 2018 interview, Benhammou stated that Acyclica retains all non-aggregated data indefinitely. It is unclear whether the different retention periods stated in the SIR are referring to different types of data. The lack of clarity on data retention periods also relates to the lack of clarity on data ownership given that data retention periods may depend on data ownership.

[10] As noted in 1. Acyclica – SDOT *Background* above.

- *Inaccurate Descriptions of Anonymization/Data Security Practices.* The SIR appears to use the terms "encryption" and "hashing" interchangeably in some parts of the SIR, making it difficult to clearly understand Acyclica's practices in this area. For example, Section 7.2 states: "Contractually, Acyclica guarantees that the data gathered is encrypted to fully eliminate the possibility of identifying individuals or vehicles." But by design, encryption allows for decryption with a key, meaning anyone with that key and access to the data can identify individuals. (Also, if there is no contract between SDOT and Acyclica, the use of 'contractually' is misleading). This language is also used in the terms sheet detailing SDOT's contract with Western Systems (in Section 2.5.1 in the embedded contract). The SIR compounds this confusion with additional contradictory statements. For example, the SIR states in multiple sections that the data collected by the RoadTrend sensors are encrypted and hashed on the actual sensor. However, according to a letter from Benhammou provided by SDOT representatives at the technology fair,[11] the data is never hashed on the sensor—the data is only hashed after being transmitted to Acyclica's cloud server. These contradictory descriptions cause concern.

- *No Restrictions on Non-City Data Use.* Section 6.3 of the SIR states that there are no restrictions on non-City data use. However, there are no policies cited making clear the criteria for such use, any inter-agency agreements governing sharing of Acyclica data with non-City parties, or why the data must be shared in the first place.

- *Not All Locations of Acyclica Devices are Specified.* Section 2.1 of the SIR states that there are 301 Acyclica locations in Seattle. However, in the embedded excel sheet detailing the serial numbers and specific intersections in which Acyclica devices are installed, there are 389 serial numbers, but only 300 addresses/locations specified. The total number and the locations of Acyclica devices collecting data in Seattle is unclear. This gives rise to the concern that there are unspecified locations in which Acyclica devices are collecting MAC addresses.

- *No Mention of RoadTrend Sensor Discontinuation.* As noted in the background,[12] Acyclica has been acquired by FLIR, an infrared and thermal imaging company. As of March 2019, FLIR's product webpage states that the Acyclica RoadTrend sensors (those currently used by SDOT) have been discontinued.[13] From the information we have, it is unclear if SDOT will be able to continue using the RoadTrend sensors described in the 2019 SIR. Given that FLIR sensors, such as the TrafiOne, have capabilities that go much farther than those of the

[11] Included in Appendix 1.
[12] As noted in 1. Acyclica – SDOT *Background* above.
[13] https://www.flir.com/support/products/roadtrend#Specifications

RoadTrend sensors (e.g., camera technology and thermal imaging)[14] as well as potentially different technical implementations, their use would give rise to even more serious privacy and misuse concerns. Neither the implications of the FLIR acquisition nor the discontinuation of the RoadTrend sensors are mentioned in the SIR.

- *No Mention of Protecting MAC Addresses of Non-Drivers/Riders (e.g., people in nearby buildings).* The Acyclica sensors will pick up the MAC addresses of all nearby individuals, regardless of whether they are or are not driving or riding in a vehicle. The SIR does not mention any steps taken to reduce the privacy infringements on non-drivers/riders.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- For what specific purpose or purposes will Acyclica be used, and what policies state this?
- Does SDOT have a contract with Acyclica, and if so, why is the contract not included in the SIR?
- Who owns the raw, non-aggregated data collected by Acyclica devices?
- What is the retention period for the different types of collected data (aggregated and non-aggregated)—for both SDOT and Acyclica?
- Provide accurate descriptions of Acyclica's data security practices, including encryption and hashing, consistent with the letter from Daniel Benhammou, including any additional practices that prevent reidentification.
- What third parties will access Acyclica's data, for what purpose, and under what conditions?
- Why are 89 locations not specified in the embedded Acyclica locations sheet in Section 2.1 of the SIR?
- Will SDOT continue to use Acyclica RoadTrend Sensors, and for how long? If SDOT plans to switch to other sensors, which ones, and how do their capabilities differ from the RoadTrend Sensors?
- Did SDOT consider any other alternatives when deciding to acquire Acyclica? Did SDOT consider other, more privacy protective traffic management tools in use (for example, inductive-loop detectors currently used by the Washington State Department of Transportation and the US

[14] https://www.flir.com/support/products/trafione#Resources

Department of Transportation)?[15]

- How does SDOT plan to reduce the privacy infringements on non-drivers/riders?

c. Recommendations for Regulation:

At this stage, pending answers to the questions set forth above, we can make only preliminary recommendations for regulation of Acyclica. We recommend that the Council adopt, via ordinance, clear and enforceable rules that ensure, at a minimum, the following:

- There must be a binding contract between SDOT and Acyclica.
- The contract between SDOT and Acyclica must include the following minimum provisions:
  - A data retention period of 12 hours or less for any data Acyclica collects, within which time Acyclica must aggregate the data, submit it to SDOT, and delete both non-aggregated and aggregated data.
  - SDOT receives only aggregated data.
  - SDOT owns all data, not Acyclica.
  - Acyclica cannot share the data collected with any other entity besides SDOT for any purpose.
- The ordinance must define a specific purpose of use for Acyclica technology, and all use of the tool and its data must be restricted to that purpose. For example: Acyclica may only be used for traffic management purposes, defined as activities concerning calculating average travel times, regulating traffic signals, controlling traffic disruptions, determining the placement of barricades or signals for the duration of road incidents impeding normal traffic flow, providing information to travelers about traffic flow and expected delays, and allowing SDOT to meet traffic records and reporting requirements.
- SDOT must produce an annual report detailing its use of Acyclica, including details how SDOT used the data collected, the amount of data collected, and for how long it was retained and in what form.

II. CopLogic – SPD

[15] https://www.fhwa.dot.gov/publications/research/operations/its/06108/03.cfm

Background

CopLogic (LexisNexis's Desk Officer Reporting System-DORS)[16] is a technology owned by LexisNexis and used by the Seattle Police Department to allow members of the public and retailers to submit online police reports regarding non-emergency crimes. Members of the public and retailers can submit these reports through an online portal they can access via their phone, tablet, or computer. Community members can report non-emergency crimes that have occurred within the Seattle city limits, and retail businesses that participate in SPD's Retail Theft Program may report low-level thefts that occur in their businesses when they have identified a suspect. This technology is used by SPD for the stated purpose of freeing up resources in the 9-1-1 Center, reducing the need for a police officer to be dispatched for the sole purpose of taking a police report.

This technology gives rise to potential civil liberties concerns because it allows for the collection of information about community members, unrelated to a specific incident, and without any systematic method to verify accuracy or correct inaccurate information. In addition, there is lack of clarity surrounding data retention and data sharing by LexisNexis, and around how CopLogic data will be integrated into SPD's Records Management System.

a. Concerns

- *Lack of Clarity on CopLogic/LexisNexis Data Collection and Retention.* There is no information in the SIR or in the contract between SPD and LexisNexis detailing the data retention period by LexisNexis (Section 5.2 of the SIR). This lack of clarity stems in part from an unclear description of what's provided by LexisNexis—it's described as an online portal, but the SIR and the contract provided appears to contemplate in Section 4.8 that LexisNexis will indeed access and store collected data. If true, the nature of that access should be clarified, and data restrictions including clear access limitations and retention periods should accordingly be put in place. Once reports are transferred over to SPD's Records Management System (RMS), the reports should be deleted by CopLogic/LexisNexis.

- *Lack of Clarity on LexisNexis Data Sharing with Other Agencies or Third Parties.* If LexisNexis does access and store data, it should do so only for purposes of fulfilling the contract, and should not share that data with third parties. But the contract between SPD and LexisNexis does not make clear whether LexisNexis is prohibited entirely from sharing data with other entities (it does contain a restriction on "transmit[ting]" the data, but without reference to third parties.

[16] https://risk.lexisnexis.com/products/desk-officer-reporting-system

- *No Way to Correct Inaccurate Information Collected About Community Members.* Community members or retailers may enter personally-identifying information about third parties without providing notice to those individuals, and there is no immediate, systematic method to verify the accuracy of information that individuals provide about third parties. There are also no stated measures in the SIR to destroy improperly collected data.

- *Lack of clarity on how the CopLogic data will be integrated with and analyzed within SPD's RMS.* At the technology fair, SPD stated that completed complaints will go into Mark43[17] when it is implemented. ACLU-WA has previously raised concerns about the Mark43 system, and it should be made clear how CopLogic data will enter that system, including to what third parties it will be made available.[18]

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What data does LexisNexis collect and store via CopLogic? What are LexisNexis's data retention policies for CopLogic data?

- Are there specific policies restricting LexisNexis from sharing CopLogic data with third parties? If so, what are they?

- Is there any way to verify or correct inaccurate information collected about community members?

- How will CopLogic data be integrated with Mark43?

c. Recommendations for Regulation:

Pending answers to the questions set forth above, we can make only preliminary recommendations for regulation of CopLogic. SPD should adopt clear and enforceable policies that ensure, at a minimum, the following:

- After CopLogic data is transferred to SPD's RMS, LexisNexis must delete all CopLogic data.

- LexisNexis is prohibited from using CopLogic data for any purpose other than those set forth in the contract, and from sharing CopLogic data with third parties.

[17] https://www.aclu-wa.org/docs/aclu-letter-king-county-council-regarding-mark-43
[18] A Records Management System (RMS) is the management of records for an organization throughout the records-life cycle. New RMSs (e.g., Mark43) may have capabilities that allow for law enforcement agencies to track and analyze the behavior of specific groups of people, leading to concerns of bias in big data policing, particularly for communities of color.

- Methods are available to the public to correct inaccurate information entered in the CopLogic portal.
- Measures are implemented to delete improperly collected data.

III. Computer-Aided Dispatch & 911 Logging Recorder Group

Overall, concerns around the Computer-Aided Dispatch (CAD) and 911 Logging Recorder technologies focus on use of the technologies and/or collected data them for purposes other than those intended, over-retention of data, and sharing of that data with third parties (such as federal law enforcement agencies). Therefore, for all of these technologies as appropriate, we recommend that the responsible agency should adopt clear and enforceable rules that ensure, at a minimum, the following:

- The purpose of use must be clearly defined, and its operation and data collected must be explicitly restricted to that purpose only.
- Data retention must be limited to the time needed to effectuate the purpose defined.
- Data sharing with third parties, if any, must be limited to those held to the same restrictions.
- Clear policies must govern operation, and all operators should be trained in those policies.

Specific comments follow:

1. Computer-Aided Dispatch – SPD

Background

CAD is a software package (made by Versaterm) utilized by the Seattle Police Department's 9-1-1 Center that consists of a set of servers and software deployed on dedicated terminals in the 9-1-1 center, in SPD computers, and as an application on patrol vehicles' mobile data computers and on some officers' smart phones. The stated purpose of CAD is to assist 9-1-1 Center call takers and dispatchers with receiving requests for police services, collecting information from callers, and providing dispatchers with real-time patrol unit availability. Concerns include lack of clarity surrounding data retention and data sharing with third parties.

a. Concerns:

- *Lack of clarity on data retention within CAD v. RMS.* While the SIR makes clear that at some point, CAD data is transferred to SPD's RMS, it is unclear what data, if any, the CAD system itself retains and for how long. If the CAD system does retain some data (for example, call logs)

independent of the RMS, and that data is accessible to the vendor, appropriate data protections should be put in place. But because the SIR usually references "data collected by CAD," it is unclear where that data resides.

- *Lack of a policy defining purpose of the technology and limiting its use to that purpose*: Unlike SFD's similar system, SPD appears to have no specific policy defining the purpose of use for CAD and limiting its use to that purpose.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- Does the CAD system itself store data? If so, what data and for how long? Who can access that data?

c. Recommendations for Regulation:

Depending on the answer to the question above, appropriate data protections may be needed as described above. In addition, SPD should adopt a policy similar to SFD's, clearly defining purpose and limiting use of the tool to that purpose.

2. Computer-Aided Dispatch – SFD

Background

Computer Aided Dispatch (CAD) is a suite of software packages used by SFD and made by Tritech that provide unit recommendations for 911 emergency calls based on the reported problem and location of a caller. The stated purpose of CAD is to allow SFD to manage emergency and non-emergency call taking and dispatching operations. The technology allows SFD to quickly enable personnel to execute rapid aid deployment.

Generally and positively, SFD clearly defines the purpose of use, restricts CAD operation and data collection to that purpose only, limits sharing with third parties, and specifies policies on operation and training. However, SFD must clarify what data is retained within CAD, data retention policies, and provide information about its data sharing partners.

d. Concerns

- *Lack of clarity on data retention within CAD*. It is unclear what data, if any, the CAD system itself retains and for how long. If the CAD system does retain some data (for example, call logs) and that data is accessible to the vendor, appropriate data protections should be put in place.
- *Lack of clarity on data retention policies*. At the technology fair, we learned that CAD data is retained indefinitely. It is not clear what justifies indefinite retention of this data.

- *Lack of clarity on data sharing partners.* In Section 6.3 of the SIR, SFD states that in rare case where CAD data is shared with partners other than those specifically named in the SIR, a third-party nondisclosure agreement is signed. However, there are no examples or details of who those partners are and the purposes for which CAD data would be shared.

e. Outstanding Questions That Must be Addressed in the Final SIR:

- Does the CAD system itself store data? If so, what data and for how long? Who can access that data?
- Who are SFD's data sharing partners? For what purpose is data shared with them?

f. Recommendations for Regulation:

Depending on the answer to the question regarding if the CAD system itself stores data, appropriate data protections may be needed as described above. SFD should adopt a clear policy requiring deletion of CAD data no longer needed. In addition, depending on how data is shared, SFD should adopt a policy that clearly limits what for what purposes CAD data would be shared, and with what entities.

3. 911 Logging Recorder – SPD

Background

The NICE 911 logging recorder is a technology used by SPD to audio-record all telephone calls to SPD's 9-1-1 communications center and all radio traffic between dispatchers and patrol officers. The stated purpose of the 9-1-1 Logging Recorder is to allow SPD to provide evidence to officers and detectives who investigate crimes and the prosecutors who prosecute offenders. These recordings also provide transparency and accountability for SPD, as they record in real time the interactions between 9-1-1 call takers and callers, and the radio traffic between 9-1-1 dispatchers and police officers. The NICE system also supports the 9-1-1 center's mission of quickly determining the nature of the call and getting the caller the assistance they need as quickly as possible with high quality, consistent and professional services.

Concerns include lack of clarity surrounding data retention schedules and data sharing with third parties.

a. Concerns

- *Lack of clarity on data retention.* Section 4.2 of the SIR states: "Recordings

requested for law enforcement and public disclosure are downloaded and maintained for the retention period related to the incident type." Similar to other technologies noted above, it is unclear whether the 9-1-1 system itself stores these recordings, or if they are stored on SPD's RMS. If the former, it should be made clear how the technology vendor accesses these recordings and for what purpose, if at all.

- *More clarity needed on data sharing with third parties.* There are no details or examples of the "discrete pieces of data" that are shared outside entities and individuals as referenced in Section 6.0 of the SIR.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What is SPD's data retention schedule for data stored in the NICE system, if any?
- What "discrete pieces of data" does SPD share with third parties?

c. Recommendations for Regulation:

SPD should adopt a clear policy requiring deletion of data no longer needed. In addition, depending on how data is shared, SPD should adopt a policy that clearly limits what for what purposes data would be shared, and with what entities.

IV. Current Diversion Technology Group – Seattle City Light

The technologies in this group—the Check Meter device (SensorLink TMS), the SensorLink Amp Fork, and the Binoculars/Spotting Scope raise civil liberties concerns primarily due to lack of explicit, written policies imposing meaningful restrictions on use of the technologies. While the purpose of the current diversion technologies appears clear—to assess whether suspected diversions of current have occurred and/or are continuing to occur—there are no explicit policies in the SIR detailing restrictions on what can and cannot be recorded by these technologies.

Below are short descriptions of the technologies, followed by concerns and recommendations.

Background

1. Check Meter Device (SensorLink TMS)

The SensorLink TMS device measures the amount of City Light-provided electrical energy flowing through the service-drop wire over time, digitally capturing the instantaneous information on the device for later retrieval by the Current Diversion Team via the use of a secure wireless protocol.

The stated purpose of use is to allow Seattle City Light to maintain the integrity of its electricity distribution system, to determine whether suspected current diversions have taken place, and to provide the valuation of the diverted energy to proper authorities for cost recovery.

2. SensorLink Amp Fork

The SensorLink Amp Fork is an electrical device mounted on an extensible pole allowing a circular clamp to be placed around the service-drop wire that provides electrical service to a customer location via its City Light-provided meter. The device then displays instantaneous readings of the amount of electrical energy (measured in amperage, or "amps") that the Current Diversion Team may compare against the readings displayed on the meter, allowing them to determine if current is presently being diverted.

The stated purpose of use of the Amp Fork is to allow Seattle City Light to assess whether suspected diversions of current have occurred and/or are continuing to occur. The Amp Fork allows the Utility to determine the valuation of the energy illegally diverted, which supports City Light's mission of recovering this value for ratepayers via a process called "back-billing."

3. Binoculars/Spotting Scope

The binoculars are standard, commercial-grade, unpowered binoculars. They do not contain any special enhancements requiring power (e.g., night-vision or video-recording capabilities). They are used to read a meter from a distance when the Current Diversion Team is otherwise unable to access physically the meter for the purpose of inspection upon suspected current diversion.

The stated purpose of the binoculars is to allow Seattle City Light to inspect meters and other implicated electrical infrastructure at a distance. If a determination of diversion is sustained, data may be used to respond to lawful requests from the proper law enforcement authorities for evidence for recovering the value of the diverted energy.

a. Concerns Regarding all Three Current Diversion Technologies

- *Absence of explicit, written policies imposing meaningful restrictions on use.* At the technology fair, a Seattle City Light representative stated that these technologies are used only for the purpose of checking current diversions, but could not confirm that Seattle City Light had clear, written policies for what data could and could not be recorded (e.g., an employee using the binoculars to view non-meter related information). The absence of written, specific policies increases the risk of unwarranted surveillance of individuals. There is also no mention in the SIRs of

specific data protection policies in place to safeguard the data (e.g., encryption, hashing, etc.).

- *Seattle City Light's records retention schedule is mentioned in the SIRs, but details about it are omitted.* It is unclear how long Seattle City Light retains data collected, and for what reason.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What enforceable policies, if any, apply to use of these three technologies?
- What is Seattle City Light's data retention schedule?

c. Recommendations for Regulation:

Seattle City Light must create clear, enforceable policies that, at a minimum:

- Define purpose of use for each technology and restrict its use to that purpose.
- Clearly state what clear data protection policies exist to safeguard stored data, if any, and ensure the deletion of data collected by the technology immediately after the relevant current diversion investigation has closed.

Thank you for your consideration, and please don't hesitate to contact me with questions.

Best,

Shankar Narayan
Technology and Liberty Project Director

Jennifer Lee
Technology and Liberty Project Advocate

Appendix 1: Benhammou Letter

City of Seattle

Acyclica

February 6th, 2015

RE: Acyclica data privacy standards

To whom it may concern:

The purpose of this letter is to provide information regarding the data privacy standards maintained by Acyclica. Acyclica is a traffic information company specializing in traffic congestion information management and analysis. Among the various types of data sources which make of Acyclica's traffic data portfolio including GPS probe data, video detection and inductive loops, Acyclica also utilizes our own patent-pending technology for the collection of Bluetooth and Wifi MAC addresses. MAC or Media Access Control addresses are unique 48-bit numbers which are associated with devices with Bluetooth and/or Wifi capable devices.

While MAC addresses themselves are inherently anonymous, Acyclica goes to great lengths to further obfuscate the original source of data through a combination of hashing and encryption to all but guarantee that information derived from the initial data bears no trace of any individual.

Acyclica's technology for collecting MAC addresses for congestion measurement operates by detecting nearby MAC addresses. The MAC addresses are then encrypted using GPG encryption before being transmitted to the cloud for processing. Encrypting the data prior to transmission means that no MAC addresses are ever written where they can be retrieved from the hardware. Once the data is received by our servers, the data is further anonymized using a SHA-256 algorithm which makes the raw MAC address nearly impossible to decipher from the hashed output. Furthermore, any customer seeking to download data for further investigation or integration through our API can only ever view the hashed MAC address.

Acyclica occasionally provides data to partners to help enhance the quality of congestion information. The information which is provided to such partners is received through API calls which only return aggregated information about traffic data over a given period such as the average travel-time over a 5-minute period. Aggregating the data provides a final layer of anonymization by reporting on the collective trend of all vehicles rather than the specific behavior of a single vehicle.

As always questions, comments and concerns are welcome. Please do let me know if we can provide further clarity and transparency on our internal operations with regards to data processing and privacy standards. We take the privacy of the public very seriously and always treat our customers and the data with the utmost respect.

Regards,

Daniel Benhammou
President
Acyclica Inc.

City of Seattle

Appendix H: Comment Analysis Methodology

Overview

The approach to comment analysis includes combination of qualitative and quantitative methods. A basic qualitative text analysis of the comments received, and a subsequent comparative analysis of results, were validated against quantitative results. Each comment was analyzed in the following ways, to observe trends and confirm conclusions:

1. Analyzed collectively, as a whole, with all other comments received
2. Analyzed by technology
3. Analyzed by technology and question

A summary of findings are included in Appendix B: Public Comment Demographics and Analysis. All comments received are included in Appendix E: All Individual Comments Received.

Background on Methodological Framework

A modified Framework Methodology was used for qualitative analysis of the comments received, which "*…approaches [that] identify commonalities and differences in qualitative data, before focusing on relationships between different parts of the data, thereby seeking to draw descriptive and/or explanatory conclusions clustered around themes" (Gale, N.K., et.al, 2013).* Framework Methodology is a coding process which includes both inductive and deductive approaches to qualitative analysis.

The goal is to classify the subject data so that it can be meaningfully compared with other elements of the data and help inform decision-making. Framework Methodology is "not designed to be representative of a wider population, but purposive to capture diversity around a phenomenon" (*Gale, N.K., et.al, 2013).*

Methodology

Step One: Prepare Data

1. Compile data received.
    a. Daily collection and maintenance of 2 primary datasets.
        i. Master dataset: a record of all raw comments received, questions generated at public meetings, and demographic information collected from all methods of submission.
        ii. Comment analysis dataset: the dataset used for comment analysis that contains coded data and the qualitative codebook. The codebook contains the qualitative codes used for analysis and their definitions.
2. Clean the compiled data.
    a. Ensure data is as consistent and complete as possible. Remove special characters for machine readability and analysis.
    b. Comments submitted through SurveyMonkey for "General Surveillance"

remained in the "General Surveillance" category for the analysis, regardless of content of the comment. Comments on surveillance generally, generated at public meetings, were categorized as such.

c. Filter data by technology for inclusion in individual SIRs.

Step Two: Conduct Qualitative Analysis Using Framework Methodology

1. Become familiar with the structure and content of the data. This occurred daily compilation and cleaning of the data in step one.
2. Individually and collaboratively code the comments received, and identify emergent themes.
   I. Begin with deductive coding by developing pre-defined codes derived from the prescribed survey and small group facilitator questions and responses.
   II. Use clean data, as outlined in Data Cleaning section above, to inductively code comments.
      A. Each coder individually reviews the comments and independently codes them.
      B. Coders compare and discuss codes, subcodes, and broad themes that emerge.
      C. Qualitative codes are added as a new field (or series of fields) into the Comments dataset to derive greater insight into themes, and provide increased opportunity for visualizing findings.
   III. Develop the analytical framework.
      A. Coders discuss codes, sub-codes, and broad themes that emerge, until codes are agreed upon by all parties.
      B. Codes are grouped into larger categories or themes.
      C. The codes are be documented and defined in the codebook.
   IV. Apply the framework to code the remainder of the comments received.
   V. Interpret the data by identifying differences and map relationships between codes and themes, using R and Tableau.

Step Three: Conduct Quantitative Analysis

1. Identify frequency of qualitative codes for each technology overall, by questions, or by themes:
   I. Analyze results for single word codes.
   II. Analyze results for word pair codes (for context).
2. Identify the most commonly used words and word pairs (most common and least common) for all comments received.
   I. Compare results with qualitative code frequencies and use to validate codes.
   II. Create network graph to identify relationships and frequencies between

words used in comments submitted. Use this graph to validate analysis and themes.

3. Extract CSVs of single word codes, word pair codes, and word pairs in text of the comments, as well as the corresponding frequencies for generating visualizations in Tableau.

Step Four: Summarization

1. Visualize themes and codes in Tableau. Use call out quotes to provide context and tone.
2. Included summary information and analysis in the appendices of each SIR.

Appendix I: Supporting Policy Documentation

Management Control Agreement

Management Control Agreement Between
Seattle Police Department and
City of Seattle Information Technology Department

The City of Seattle Police Department ("SPD"), also referred to as the Criminal Justice Agency, and the City of seattle Information Technology Department (''ITD") are departments of the municipal corporation of the City of Seattle.

Pursuant to Seattle Municipal Code ("SMC") 3.23, ITD provides information technology systems, services, and support to SPD and is therefore required to support, enable, enforce, and comply with SPD policy requirements, including the FBl's Criminal Justice Information Services ("CJIS") Security Policy.

Pursuant to the CJIS Security Policy, it is agreed that with respect to the administration of computer systems, network infrastructure, devices, and services interfacing directly or indirectly with A Central Computerized Enforcement System ("ACCESS") for the exchange of criminal history/criminal justice information, the Criminal Justice Agency shall have the authority, via managed control, to set and enforce:

Priorities that guarantee the priority, integrity, and availability of service needed by the criminal justice community.

Requirements for the selection, authorization, supervision, and termination of physical and logical access to Criminal Justice Information ("CJI").

Policy governing operation of justice systems, data, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a communications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.

Restriction of unauthorized physical and logical access to or use of systems and equipment accessing CJI.

Compliance with all rules and regulations of the Criminal Justice Agency policies and CJIS Security Policy in the operation of, access to, or control over any CJI systems, data, or infrastructure.

The responsibility for management control of the criminal justice function remains solely with the Criminal Justice Agency. ITD will not enter into any agreements or allow any

access to, possession of, or control over any SPD CJI systems, data, or infrastructure without explicit authorization from at least one SPD Authorized Party. SPD Authorized Parties must be SPD employees and include:
Chief of Police
Chief Operating Officer

This agreement covers the overall supervision of all Criminal Justice Agency systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, administration, and maintenance of any Criminal Justice Agency system to include NCIC Programs that may be subsequently designed and/or implemented within the Criminal Justice Agency.

Additional agreements, such as a Memorandum of Agreements, Service Level Agreements, and/or Continuity Plans, may be established and maintained to further delineate, define, and assign roles, responsibilities, and requirements of and agreements between SPD and ITD, and other City of Seattle Departments and/or agencies.

Tracye Cantrell

Tracye Cantrell
Interim Chief Technology Officer
Seattle Information Technology Department

Date Feb 2, 2018

Carmen Best

Carmen Best
Interim Chief of Police |
Seattle Police Department

Date 2-7-2018

Reference: CJIS Security Policy, Version 5.5, dated June 1, 2016 (CJISD-ITS-DOC-08140-5 .5)

IT Support Services for City Technology

Engineering and Operations

This division designs, implements, operates, and supports technology solutions and resources in accordance with city wide architecture and governance. Responsibilities for this division include:

- Primary communications networks that provide public safety and constituent access to and from City government; the telephone system, the data network, and Public Safety Radio System. Responsible for sustaining all three systems operating as close to 100% availability as possible 24 hours a day, seven days a week.
- Design, acquisition, installation, maintenance, repair and management of fiber optic cables on behalf of City departments and approximately 20 other local, state and federal agencies.
- Procurement requests, allocation, operation and maintenance of city wide and departmental servers, virtual enterprise computing and SAN storage environments for large scale mission critical applications in a secure, reliable, 24/7 production environment for enterprise computing.
- Allocation, operation and maintenance of enterprise level services like messaging services, web access, file sharing, user management and remote access solutions.
- Collaborate with Enterprise Architecture team to develop standards for information technology equipment and software.
- Service Desk and technical support services for City's computers, peripherals, electronic devices and mobile device management.
- Centralized IT asset management to include research, procurement request, surplus and asset transfer.
- Facility management for a reliable production computing environment to the City departments.
- Support for other enterprise services and tools.

Compute System Technologies

This team manages the operations and maintenance of computing infrastructure, including servers, storage, backup and recovery, and enterprise support systems (e.g., Active Directory, VPN, etc.). The team is also responsible for safeguarding systems and data by performing required security patches, updates, and backups to ensure systems operate at as close to 100% availability as possible 24x7. Units within this group include:

Systems Operations. The team is focused on delivering the computing environment across multiple departments. The team has technical expertise to design, integrate, and operate a secure, reliable computing environment. Key technologies include Windows, Solaris, IBM AIX, and Linux.

Enterprise Services. Enterprise Services (ES) are large scale infrastructure and application services used by the City of Seattle end user community. This includes both SaaS and NGDC hosted infrastructure and application services. The team is responsible for EA vendor management, system administration, upgrades and technical support. Key technologies includes Microsoft Active Directory (AD), Distributed File System (DFS), Exchange Online, Office 365 and SharePoint Online infrastructure.

Infrastructure Tools. The team provides a single focus for the design, planning, deployment and maintenance of standard enterprise infrastructure monitoring and management tools. This includes system performance (Solarwinds, SCOM), configuration management (SCCM, WSUS), and monitoring and system management (Trend Micro, CRM, Vipre).

Virtual and Data Infrastructure. This team engineers and operates reliable, flexible, performant virtualized Windows, UNIX and Linux platforms and their related technologies in direct support of critical business applications. Key technologies include Solaris, Unix, Linux, Windows, and vmWare, and the associated virtualization Nutanix, IBM LPAR, and Solaris hardware.

The team also engineers and operates reliable, flexible, performant storage and data protection solutions to host and protect critical business data of all types, leveraging SAN, NAS, object, and cloud technologies. Key technologies include Dell Compellent, Quantum, Hitachi, NetApp, Cloud storage, Brocade fiber channel switching, and Commvault.

Network And Communications Technologies

This team is responsible for designing, installing, operating, and maintaining data, voice, radio, fiber optic, and structured cabling infrastructure that integrates with other technologies to provide access to resources used by City departments and the public we serve. Units within this group include:

Network Engineering & Operations. The Network Services team engineers, operates and maintains the City's data network, including data center core networks, the internet perimeter, the network backbone, and local area networks that support systems and users across the City. This group designs, acquires, installs, maintains, repairs, and manages an enterprise data network that aligns with City architectures and standards. This group also participates in development of those standards and provides tier 2 and 3 end user support. This team supports technologies that include routing, switching, load balancing, enterprise Wi-Fi, DNS/DHCP/NTP, and network security (including firewalls, VPN appliances, certificate infrastructure, network access control, and web filtering.)

Telecommunication Engineering & Operations. The Telecommunications Services team engineers, operates, and maintains a highly-reliable enterprise telephone and contact center infrastructure. This group supports end user move and change activity and provides tier 2 and 3 support. The Telecommunication Services team acquires, installs, maintains, and repairs telecommunications equipment and manages commercial telephony circuits. It supports technologies that include VoIP, circuit-switched telephony, voice mail, contact center services (including call routing scripts), audio conference bridges, commercial telephony services, SONET, and WDM.

Radio & Communications Infrastructure. This team delivers radio services for public safety and other government departments. It provides extremely reliable infrastructure and support for end user mobile and portable radio equipment. The group installs and maintains communications equipment inside 911 dispatch centers and City vehicles, with primary support to SPD and SFD. The team also supports regional planning, maintenance, interoperability testing, and projects (including PSERN and Washington OneNet) in partnership with other local, state, and federal agencies. This team also designs, acquires, installs, maintains, repairs, and manages in-building structured

cabling systems and outside plant fiber optic and copper cable infrastructure for the City and approximately 20 external public agency partners. Technologies include trunked and conventional land mobile radio, microwave radio and other wireless communications systems (including point-to-multipoint and mesh networks,) distributed antenna systems, routing/MPLS, DS3/T1/DACS, outside plant cable infrastructure (including fiber and copper,) and structured cabling infrastructure.

End User Support

This team is responsible for providing a single point of contact for IT technical support, trouble ticket and service request resolution and referral services to other IT workgroups, and for communication for all changes, patches, upgrades and standards changes. The team is also responsible for providing technical support for the City's desktop computers, peripherals, electronic devices and mobile devices. Units within this group include:

Service Desk. The Service Desk team provides a single point of contact for Seattle IT services, promptly resolving incidents and service requests when first contacted whenever possible, escalating issues accurately and efficiently, and keeping users and partners aware of service status and changes.

Device Support. This team provides direct customer support for end user computing to all departments within the City and tier 2 escalation support and management of centralized end user computing applications and hardware. requests.

Device Engineering. This team engineers and deploys software packages for end user applications, device drivers, patches, security updates and custom packages as required. This team evaluates and recommends hardware and software for end user standards. In addition, this team provides tier 3 escalation support and management of centralized end user computing applications and hardware.

Asset Management. This team is responsible tracking and inventory controls for city wide IT assets including desktops, laptops, printers, servers, switches, and miscellaneous Information Technology infrastructure. In addition to inventory control, the team will be forecasting replacement cycles for equipment based on City standards to promote a stable computing environment.

IT Operations Support

The IT Operations Support team is responsible for management of Information Technology facilities (including data centers and communications equipment rooms), and installation and cabling equipment within those facilities. This team provides the enterprise Network Operations Center (NOC) that monitors alerts, performs initial incident analysis, dispatches tier 2 and 3 technical support, and provides initial incident communication for network infrastructure and computing systems managed by Engineering and Operations. Units within this group include:

Installation Management. This team installs networking and computing equipment in data centers, communications rooms and wiring closets; installs and maintains network cabling within data centers and equipment rooms according to City standards; and

supports repair and end user move and change activity (including telephone move projects).

IT Operations Center. This team manages facilities which support City computing and communications services. This includes managing access to facilities, coordinating vendors, maintaining records (including data center inventory management), and, where applicable, monitoring facility systems (including CRUs, fire alarms, water detection sensors, UPS systems, and power consumption). This team also staffs the NOC that monitors alerts from network infrastructure and computing systems, performs initial problem analysis, dispatches appropriate tier 2 and 3 technical support team(s), and provides initial incident communication.

Application Services

This division designs, develops, integrates, implements, and supports application solutions in accordance with city wide architecture and governance. Its teams are organized to support business functions or service groups**.** The integration of application services will be completed gradually in 2017, with details of the organization and integration process still under development.

Applications

These teams will provide development and support for applications that include customer relationship management, billing, finance, human resources, work and asset management and records management.

Shared Platforms

These teams will provide development and support for applications that include engineering, spatial analysis, business intelligence, analytics, SharePoint Online and document management.

Cross Platform Services

These teams will provide support to application teams, including quality assurance, change control, database administration, integration services, and access management activities.

Data Retention

Exported report will be auto-deleted after this many days	120	(blank or 0 means exported report will not be auto-deleted)
Approved report will be auto-deleted after this many days	120	(blank or 0 means approved report will not be auto-deleted)
Pending report will be auto-rejected after this many days	30	(blank or 0 means pending report will not be auto-rejected)
Rejected report will be auto-deleted after this many days	120	

City of Seattle

Appendix J: CTO Notification of Surveillance Technology

Thank you for your department's efforts to comply with the new Surveillance Ordinance, including a review of your existing technologies to determine which may be subject to the Ordinance. I recognize this was a significant investment of time by your staff; their efforts are helping to build Council and public trust in how the City collects and uses data.

As required by the Ordinance (SMC 14.18.020.D), this is formal notice that the technologies listed below will require review and approval by City Council to remain in use. This list was determined through a process outlined in the Ordinance and was submitted at the end of last year for review to the Mayor's Office and City Council.

The first technology on the list below must be submitted for review by March 31, 2018, with one additional technology submitted for review at the end of each month after that. The City's Privacy Team has been tasked with assisting you and your staff with the completion of this process and has already begun working with your designated department team members to provide direction about the Surveillance Impact Report completion process.

Please let me know if you have any questions.

Thank you,

Michael Mattmiller

Chief Technology Officer

Technology	Description	Proposed Review Order
Automated License Plate Recognition (ALPR)	ALPRs are computer-controlled, high-speed camera systems mounted on parking enforcement or police vehicles that automatically capture an image of license plates that come into view and converts the image of the license plate into alphanumeric data that can be used to locate vehicles reported stolen or otherwise sought for public safety purposes and to enforce parking restrictions.	1
Booking Photo Comparison Software (BPCS)	BCPS is used in situations where a picture of a suspected criminal, such as a burglar or convenience store robber, is taken by a camera. The still screenshot is entered into BPCS, which runs an algorithm to compare it to King County Jail booking photos to identify the person in the picture to further investigate his or her involvement in the crime. Use of BPCS is governed by SPD Manual §12.045.	2
Forward Looking Infrared Real-time video (FLIR)	Two King County Sheriff's Office helicopters with Forward Looking Infrared (FLIR) send a real-time microwave video downlink of ongoing events to commanders and other decision-makers on the ground, facilitating specialized radio tracking equipment to locate bank robbery suspects and provides a platform for aerial photography and digital video of large outdoor locations (e.g., crime scenes and disaster damage, etc.).	3

Technology	Description	Proposed Review Order
Undercover/ Technologies	The following groups of technologies are used to conduct sensitive investigations and should be reviewed together. • **Audio recording devices**: A hidden microphone to audio record individuals without their knowledge. The microphone is either not visible to the subject being recorded or is disguised as another object. Used with search warrant or signed Authorization to Intercept (RCW 9A.73.200). • **Camera systems**: A hidden camera used to record people without their knowledge. The camera is either not visible to the subject being filmed or is disguised as another object. Used with consent, a search warrant (when the area captured by the camera is not in plain view of the public), or with specific and articulable facts that a person has or is about to be engaged in a criminal activity and the camera captures only areas in plain view of the public. • **Tracking devices**: A hidden tracking device carried by a moving vehicle or person that uses the Global Positioning System to determine and track the precise location. U.S. Supreme Court v. Jones mandated that these must have consent or a search warrant to be used.	4
Computer-Aided Dispatch (CAD)	CAD is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field.	5

Technology	Description	Proposed Review Order
CopLogic	System allowing individuals to submit police reports on-line for certain low-level crimes in non-emergency situations where there are no known suspects or information about the crime that can be followed up on. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.	6
Hostage Negotiation Throw Phone	A set of recording and tracking technologies contained in a phone that is used in hostage negotiation situations to facilitate communications.	7
Remotely Operated Vehicles (ROVs)	These are SPD non-recording ROVs/robots used by Arson/Bomb Unit to safely approach suspected explosives, by Harbor Unit to detect drowning victims, vehicles, or other submerged items, and by SWAT in tactical situations to assess dangerous situations from a safe, remote location.	8
911 Logging Recorder	System providing networked access to the logged telephony and radio voice recordings of the 911 center.	9
Computer, cellphone and mobile device extraction tools	Forensics tool used with consent of phone/device owner or pursuant to a warrant to acquire, decode, and analyze data from smartphones, tablets, portable GPS device, desktop and laptop computers.	10
Video Recording Systems	These systems are to record events that take place in a Blood Alcohol Concentration (BAC) Room, holding cells, interview, lineup, and polygraph rooms recording systems.	11
Washington State Patrol (WSP) Aircraft	Provides statewide aerial enforcement, rapid response, airborne assessments of incidents, and transportation services in support of the Patrol's public safety mission. WSP Aviation currently manages seven aircraft equipped with FLIR cameras. SPD requests support as needed from WSP aircraft.	12

Technology	Description	Proposed Review Order
Washington State Patrol (WSP) Drones	WSP has begun using drones for surveying traffic collision sites to expedite incident investigation and facilitate a return to normal traffic flow. SPD may then request assistance documenting crash sites from WSP.	13
Callyo	This software may be installed on an officer's cell phone to allow them to record the audio from phone communications between law enforcement and suspects. Callyo may be used with consent or search warrant.	14
I2 iBase	The I2 iBase crime analysis tool allows for configuring, capturing, controlling, analyzing and displaying complex information and relationships in link and entity data. iBase is both a database application, as well as a modeling and analysis tool. It uses data pulled from SPD's existing systems for modeling and analysis.	15
Parking Enforcement Systems	Several applications are linked together to comprise the enforcement system and used with ALPR for issuing parking citations. This is in support of enforcing the Scofflaw Ordinance SMC 11.35.	16
Situational Awareness Cameras Without Recording	Non-recording cameras that allow officers to observe around corners or other areas during tactical operations where officers need to see the situation before entering a building, floor or room. These may be rolled, tossed, lowered or throw into an area, attached to a hand-held pole and extended around a corner or into an area. Smaller cameras may be rolled under a doorway. The cameras contain wireless transmitters that convey images to officers.	17
Crash Data Retrieval	Tool that allows a Collision Reconstructionist investigating vehicle crashes the opportunity to image data stored in the vehicle's airbag control module. This is done for a vehicle that has been in a crash and is used with consent or search warrant.	18

Technology	Description	Proposed Review Order
Maltego	An interactive data mining tool that renders graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the internet.	19

Please let me know if you have any questions.

Thank you,

Michael

City of Seattle

2020 Surveillance Impact Report Executive Overview

911 Logging Recorder

Seattle Police Department

DRAFT

City of Seattle

Overview

The Operational Policy statements in this document represent the only allowable uses of the equipment and data collected by this technology.

This Executive Overview documents information about the collection, use, sharing, security and access controls for data that is gathered through the Seattle Police Department's 911 Logging Recorder. All information provided here is contained in the body of the full Surveillance Impact Review (SIR) document but is provided in a condensed format for easier access and consideration.

1.0 Technology Description

The NICE 9-1-1 Logging Recorder audio-records all telephone calls to SPD's 9-1-1 communications center and all radio traffic between dispatchers and patrol officers.

2.0 Purpose

Operational Policies:

> **Use of the technology other than the recording of calls to and from 9-1-1, police radio traffic, and retrieval of those recordings for law enforcement or public disclosure purposes is out of policy and subject to SPD disciplinary action.**
>
> **The technology is used in two distinct ways.**
>
> 1. **The system automatically records all calls into the 9-1-1 system, police non-emergency phone line, and police radio traffic.**
> 2. **It is used to retrieve recordings by authorized personnel.**

The NICE 9-1-1 Logging Recorder is automatically used to record all calls into the 9-1-1 system, police non-emergency phone line, and police radio traffic. Police communications analysts also routinely use the NICE 9-1-1 Logging Recorder to capture audio recordings germane to police investigations and forward those recordings to detective units, outside legal entities such as the Seattle City Attorneys' Office, the King County Prosecutors Office, and defense attorneys. Police Communications Supervisors and Analysts routinely listen to audio recordings for Quality Assurance purposes. The 9-1-1 Recordings Office is overseen by the 9-1-1 Administrative Manager.

This technology audio-records 9-1-1 and non-emergency telephone calls and police radio traffic for evidentiary and public disclosure purposes. Audio recordings are routinely used in criminal prosecutions and are routinely used within the 9-1-1 Center for training and quality control purposes.

DRAFT

3.0 Data Collection and Use

Operational Policy:

> **No information is collected from a source other than individual who calls 9-1-1 or from the officers and dispatchers.**

The technology is used to record all telephone calls between the public and the 9-1-1 Center, and police radio traffic. This is triggered when a community member contacts the department by calling 9-1-1 or the departments non-emergency numbers, including all outbound calls placed by 9-1-1 call takers and dispatchers and all radio traffic between dispatchers and police personnel including police officers, parking enforcement officers, and police detectives utilizing the police radio system.

Requests for audio recordings are initiated by detective units investigating a crime, legal counsel, and other outside entities. Recordings may also be initiated by the public using the Public Disclosure Process.

4.0 Data Minimization & Retention

Operational Policy:

> **Audio recordings that have not been requested within 90 days of their capture are deleted. Recordings requested for law enforcement and public disclosure are downloaded and maintained for the retention period related to the incident type**.

SPD policy contains multiple provisions to avoid improperly collecting data. SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a GO Report. SPD Policy 7.090 specifically governs the collection and submission of photographic evidence. Evidence is submitted to the Evidence Unit and associated with a specific GO Number and investigation. And, SPD Policy 7.110 governs the collection and submission of audio recorded statements. It requires that officers state their name, the Department name, the General Offense number, date and time of recording, the name of the interviewee, and all persons present at the beginning of the recording.

5.0 Access & Security

Operational Policies:

> **Verified users access the system to capture and disseminate audio recordings based on the requests received from detective units, outside legal entities, and the public.**
>
> **Data is securely input and used on SPD's password-protected network with access limited to authorized detectives and identified supervisory personnel.**

DRAFT

Access

Authorized SPD users may access the recordings by logging into the NICE 9-1-1 Logging Recorder utilizing a unique username and password. Access for personnel into the system is predicated on state and federal law governing access to criminal justice information systems. This includes thorough background investigations for each user, appropriate access and permissions dependent on the personnel role, and an audit of access and transaction logs within the system.

Only authorized SPD users can access the system, technology, or the data. Access to the application is limited to SPD personnel via password-protected login credentials. Supervisors and commanding officers are responsible for ensuring compliance with SPD policies. Data is securely input and used on SPD's password-protected network with access limited to authorized detectives and identified supervisory personnel

Security

The data is stored in the NICE system, much of the NICE system is physically housed at the SPD 9-1-1 center, with some of the servers hosted virtually on SPD network in SPD section of the city data center. Data collect is located on the server's storage in the above locations. Extracted data is stored on file shares for SPD and City Law (these reside SPD Network Storage or Law storage system managed by Seattle ITD). Extracted data is electronically sent to Law, Discovery or as redacted material in response to PDR (posted to the City PDR system, GOVQA).

6.0 Data Sharing and Accuracy

Operational Policy:

> **No person, outside of SPD and Seattle IT, has direct access to the application or the data.**

Data obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law.

Per City of Seattle's Privacy Statement, outlining commitments to the public about how we collect and manage their data: *We do not sell personal information to third parties for marketing purposes or for their own commercial use.* The full Privacy Statement may be found **here.**

7.0 Equity Concerns

Operational Policy:

> **SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.**

The NICE 9-1-1 Logging Recorder is used to record all calls placed to 9-1-1 and the police non-emergency numbers without regard to where the call originates from. There is no distinction in the levels of service this system provides to the various and diverse neighborhoods, communities, or individuals within the city.

DRAFT

City of Seattle

2020 Surveillance Impact Report Executive Overview

Parking Enforcement Systems (Including ALPR)

Seattle Police Department

DRAFT

City of Seattle

Overview

The Operational Policy statements in this document represent the only allowable uses of the equipment and data collected by this technology.

This Executive Overview documents information about the collection, use, sharing, security and access controls for data that is gathered through Seattle Police Department's (SPD) Parking Enforcement Systems including Automated License Plate Reader (ALPR). All information provided here is contained in the body of the full Surveillance Impact Review (SIR) document but is provided in a condensed format for easier access and consideration.

Note: All use of ALPR as described in this document and the SIR is governed by SPD Policy 16.170

1.0 Technology Description

Parking enforcement ALPR hardware consists of high definition infrared digital cameras that are mounted on three vehicles designated for scofflaw enforcement (these boot vans carry boot devices that can be mounted to immobilize vehicles in violation of scofflaw), and five Parking Enforcement vehicles – for a total of eight ALPR-equipped vehicles that are utilized for Parking Enforcement. The other 39 ticketing vehicles are not equipped with ALPR

2.0 Purpose

Operational Policies:

ALPR systems will only be deployed for official law enforcement purposes. These deployments are limited to:

1. **Locating stolen vehicles;**
2. **Locating stolen license plates;**
3. **Locating wanted, endangered or missing persons; or those violating protection orders;**
4. **Canvassing the area around a crime scene;**
5. **Locating vehicles under SCOFFLAW; and**
6. **Electronically chalking vehicles for parking enforcement purposes.**

Seattle Police Department (SPD) facilitates the flow of traffic, assists with the collection of revenue related to parking violations in the City of Seattle, and recovers stolen vehicles through a number of means. Among these is Parking Enforcement Systems technology, which is used by SPD as a necessary tool in the following ways:

1. Scofflaw – SPD employs three vehicles (two vans, and one truck) with ALPR systems to identify parked vehicles in violation of the City Scofflaw Ordinance. Vehicles in violation are subject to booting, pending payment of past due balances.
2. Time-Restricted Parking Areas – 47 sedans, 54 scooters, 2 vans, and 1 truck are utilized to monitor time-restricted parking within the City. Five of the sedans are equipped with ALPR systems and operated by civilian employees to digitally "chalk" vehicles parked in time-restricted zones. Utilizing GPS location and stem-valve

DRAFT

comparison technology, the system alerts on those vehicles that are in violation of the time zone restriction upon a second pass. The remaining vehicles are used in traditional pay to park enforcement, and for manually chalking vehicle tires in time-restricted locations.
3. Restricted Parking Zones ("RPZ") means a portion of the street commonly used for vehicular parking where vehicles properly displaying a permit or other authorization are exempt from the posted RPZ. Seattle Department of Transportation provides SPD with a list of vehicles permitted to park in an RPZ. Parking Enforcement Officers may use ALPR to determine that a vehicle does not have the appropriate permit or authorization to park in an RPZ.
4. Parking Enforcement Officers may use ALPR using a list of vehicles reported stolen or sought in connection with criminal investigation to identify those vehicles and report their location to Dispatch.

3.0 Data Collection and Use

Operational Policy:

ALPR technology collects digital images of license plates and associated license plate numbers. The technology collects the date and time that the license plate passes a digital-image site where an ALPR is located.

Data collected from ALPR include license plate image, computer-interpreted read of the license plate number, date, time, and GPS location. ALPR on Parking Enforcement vehicles takes a burst of 26 pictures of each parked vehicle, for visual photo comparison when the same vehicle is later examined for time zone violation.

4.0 Data Minimization & Retention

Operational Policies:

ALPR will not be used to intentionally capture images in private area or areas where a reasonable expectation of privacy exists, nor shall it be used to harass, intimidate or discriminate against any individual or group.

Metadata and images of detections will be deleted from the server within 24 hours of collection.

When the ALPR system registers a hit, the user must verify accuracy before taking any action. In Parking Enforcement, users verify first that a vehicle hit for Scofflaw violation is still actively in violation by checking for updated information in Bootview before booting a vehicle. Parking Enforcement Officers then visually verify that a vehicle suspected of time-zone restriction or metered parking violation is, in fact, in violation prior to issuing a ticket. Images captured serve as “evidence” that the system and the user are not in error.

Unless a hit has been exported for investigation and exported from the database for this purpose, all data captured by the five ALPR-equipped parking enforcement sedans is retained in the same database as ALPR data collected by ALPR-equipped patrol vehicles and is retained until automatically deleted after 90 days, per department retention policy.

5.0 Access & Security

Operational Policies:

1. **Only Employees Trained in the Use of ALPR Equipment Will Use and Access ALPR Devices and Data**
2. **Employees Accessing ALPR Data Must Login Through the ALPR Password-Protected System**
3. **Employees Conducting Searches in the ALPR System Will Provide a Case Number and Justification for the Search**
4. **Employees Will Not Share ALPR Passwords and Login Credentials**
5. **The Department will store ALPR data in a secured law enforcement facility with multiple layers of security protection. Firewalls, authentication and other reasonable security measures will be utilized. Only trained Department employees can access stored ALPR data and all data search requests are logged within the system.**
6. **ALPR data maintained on BOSS will only be accessed by trained, SPD employees for official law enforcement purposes. This access is limited to:**
   - **(a) Search of specific or partial plate(s) and/or vehicle identifiers as related to:**
   - **(b) A crime in-progress;**
   - **(c) A search of a specific area as it relates to a crime in-progress;**
   - **(d) A criminal investigation; or**
   - **(e) A search for a wanted person; or**
   - **(f) Community caretaking functions such as, locating an endangered or missing person.**
   - **(g) Officers/detectives conducting searches in the system will complete the Read Query screen documenting the justification for the search and applicable case number.**
   - **(h) Administration and maintenance.**

Access

Prior to gaining access to the ALPR system, potential users must be trained by other trained SPD Parking Enforcement officers. Once this training has been verified with the Parking Enforcement Supervisor, users are given access and must log into the system with unique login and password information whenever they employ the technology. They remain logged into the system the entire time that the ALPR system is in operation. The login is logged and auditable.

DRAFT

Parking Enforcement Officers are assigned the vehicles to use while on-shift, as well as a specific zone to monitor for time-restricted parking violations.

Security

All data collected for Parking Enforcement systems are hosted on City SPD servers and are not accessible by vendors without knowledge and/or permission of City personnel. Only authorized users can access the data collected by ALPR for Parking Enforcement. Also, all activity by users in the AutoVu ALPR system is logged and auditable. Data removed from the system/technology and entered into investigative files is securely input and used on SPD's password-protected network with access limited to authorized SPD personnel.

6.0 Data Sharing and Accuracy

Operational Policy:

> **ALPR data will only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law.**

Unlike some ALPR systems, SPD's systems do not "pool" SPD's ALPR data with that collected by other agencies.

Data obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law. Seattle's Scofflaw Ordinance and Traffic Code require that SPD share information with Seattle Municipal Court. Data may be shared without outside entities in connection with criminal prosecutions.

Per City of Seattle's Privacy Statement, outlining commitments to the public about how we collect and manage their data: *We do not sell personal information to third parties for marketing purposes or for their own commercial use.* The full Privacy Statement may be found **here.**

DRAFT

7.0 Equity Concerns

Operational Policy:

> **ALPR will not be used to intentionally capture images in private area or areas where a reasonable expectation of privacy exists, nor shall it be used to harass, intimidate or discriminate against any individual or group.**

ALPR is content-neutral; it does not identify the race of the driver or the registered owner of the vehicle. To ensure that SPD continues to build trust with community members and increase racial equity, SPD must continue to follow its policy of limiting use of the ALPR cars to strictly routine patrol and use of collected ALPR data to specific criminal investigations or community caretaking functions, as well as limiting access to the ALPR system to authorized SPD personnel. Further, SPD must also continue to audit the system on a regular basis to provide a measure of accountability. In doing so, SPD can mitigate the appearance of disparate treatment of individuals based on factors other than true criminal activity and minimize perceived oversurveillance of areas where historically targeted communities reside or congregate.

DRAFT

City of Seattle

2020 Surveillance Impact Report Executive Overview

Automated License Plate Readers (ALPR) (Patrol)

Seattle Police Department

DRAFT

Overview

The Operational Policy statements in this document represent the only allowable uses of the equipment and data collected by this technology.

This Executive Overview documents information about the collection, use, sharing, security and access controls for data that is gathered through Seattle Police Department's (SPD) Automated License Plate Reader (ALPR) system. All information provided here is contained in the body of the full Surveillance Impact Review (SIR) document but is provided in a condensed format for easier access and consideration.

Note: All use of ALPR as described in this document and the SIR is governed by SPD Policy 16.170

1.0 Technology Description

The Seattle Police Department has nineteen vehicles with ALPR. Eleven of these are Patrol vehicles and three are Scofflaw Enforcement vehicles. ALPR hardware consists of high definition infrared digital cameras that are mounted on eleven Patrol cars (one of which is unmarked).

The high-speed cameras capture images of license plates as they move into view, and associated software deciphers the characters on the plate, using optical character recognition. This interpretation is then immediately checked against any license plate numbers that have been uploaded into the onboard, in-vehicle software system.

2.0 Purpose

Operational Policies:

> **ALPR systems will only be deployed for official law enforcement purposes. These deployments are limited to:**
>
> 1. **Locating stolen vehicles;**
> 2. **Locating stolen license plates;**
> 3. **Locating wanted, endangered or missing persons; or those violating protection orders;**
> 4. **Canvassing the area around a crime scene; and**
> 5. **Locating vehicles under SCOFFLAW**

Seattle Police Department uses Automated License Plate Reader (ALPR) technology to recover stolen vehicles, to locate subjects of Amber and Silver Alerts and fugitives where vehicle license plate information is available, to assist with active investigations, to facilitate the flow of traffic (by monitoring and enforcing City parking restrictions) and for Scofflaw Ordinance enforcement.

DRAFT

Patrol ALPR assists the City in locating and recovering stolen vehicles. ALPR systems may assist with active investigations by helping to determine the location of vehicles of interest – specifically those that have been identified as being associated with an investigation. SPD uses ALPR to recover stolen vehicles, which are often used by thieves in committing other crimes.

3.0 Data Collection and Use

Operational Policy:

> **ALPR technology collects digital images of license plates and associated license plate numbers. The technology collects the date and time that the license plate passes a digital-image site where an ALPR is located.**

Data collected from ALPR include license plate image, computer-interpreted read of the license plate number, date, time, and GPS location.

All ALPR-equipped vehicles upload a daily HotList from the Washington State Patrol that contains national stolen vehicle plate data published daily by the FBI. The Washington State Patrol places the HotList file on a server available through ACCESS to those agencies that have a specific and signed agreement with WSP to access and use the information. The receiving local law enforcement may supplement the list with additional information, such as vehicles sought with reasonable suspicion that they are involved in an incident or vehicles sought pursuant to a warrant.

4.0 Data Minimization & Retention

Operational Policies:

> **ALPR will not be used to intentionally capture images in private area or areas where a reasonable expectation of privacy exists, nor shall it be used to harass, intimidate or discriminate against any individual or group.**

When the ALPR system registers a hit, a match to a license plate number listed on the HotList (as described in 2.3 above), the user must verify accuracy before taking any action. For instance, when the system registers a hit on a stolen vehicle, the user must visually verify that the system accurately read the license plate and, if so, must then contact Dispatch to verify accuracy of the hit – that the vehicle is actually listed as stolen. Only then does the user act.

Unless a hit has been flagged for investigation and exported from the database for this purpose, all captured data is automatically deleted after 90 days, per department retention policy. Data related to a flagged hit is downloaded and maintained with the investigation file for the retention period related to the incident type.

DRAFT

5.0 Access & Security

Operational Policies:

1. **Only Employees Trained in the Use of ALPR Equipment Will Use and Access ALPR Devices and Data**
2. **Employees Accessing ALPR Data Must Login Through the ALPR Password-Protected System**
3. **Employees Conducting Searches in the ALPR System Will Provide a Case Number and Justification for the Search**
4. **Employees Will Not Share ALPR Passwords and Login Credentials**
5. **The Department will store ALPR data in a secured law enforcement facility with multiple layers of security protection. Firewalls, authentication and other reasonable security measures will be utilized. Only trained Department employees can access stored ALPR data and all data search requests are logged within the system.**
6. **ALPR data maintained on BOSS will only be accessed by trained, SPD employees for official law enforcement purposes. This access is limited to:**
   - **(a) Search of specific or partial plate(s) and/or vehicle identifiers as related to:**
   - **(b) A crime in-progress;**
   - **(c) A search of a specific area as it relates to a crime in-progress;**
   - **(d) A criminal investigation; or**
   - **(e) A search for a wanted person; or**
   - **(f) Community caretaking functions such as, locating an endangered or missing person.**
   - **(g) Officers/detectives conducting searches in the system will complete the Read Query screen documenting the justification for the search and applicable case number.**
   - **(h) Administration and maintenance**

Access

Prior to gaining access to the ALPR system, potential users must be trained by other trained officers. Once this training has been verified with the ALPR administrator, users are given access and must log into the system with unique login and password information whenever they employ the technology. They remained logged into the system the entire time that the ALPR system is in operation. The login is logged and auditable. Officers are assigned the vehicles to use while on-shift.

Security

All data collected from the ALPR system is stored, maintained, and managed on premises. ALPR systems maintain access logs on backend servers that are accessible for audit The Office of Inspector General may access all data and audit for compliance at any time.

DRAFT

6.0 Data Sharing and Accuracy

Operational Policy:

> **ALPR data will only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law.**

SPD has no data sharing partners for ALPR. No person, outside of SPD, has direct access to the PIPS system or the data while it resides in the system or technology. ALPR data will only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law. SPD does not pool its ALPR data with any other agency's data.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed by the Legal Unit pursuant to the applicable Rules of Civil or Criminal Discovery or the Washington Public Records Act, **Chapt. 42.56 RCW**. The Legal Unit will maintain requests for ALPR data by non-law enforcement or non-prosecutorial agencies.

Per City of Seattle's Privacy Statement, outlining commitments to the public about how we collect and manage their data: *We do not sell personal information to third parties for marketing purposes or for their own commercial use.* The full Privacy Statement may be found **here.**

7.0 Equity Concerns

Operational Policy:

> **ALPR will not be used to intentionally capture images in private area or areas where a reasonable expectation of privacy exists, nor shall it be used to harass, intimidate or discriminate against any individual or group.**

ALPR is content-neutral; it does not identify the race of the driver or the registered owner of the vehicle. To ensure that SPD continues to build trust with community members and increase racial equity, SPD must continue to follow its policy of limiting use of the ALPR cars to strictly routine patrol and use of collected ALPR data to specific criminal investigations or community caretaking functions, as well as limiting access to the ALPR system to authorized SPD personnel. Further, SPD must also continue to audit the system on a regular basis to provide a measure of accountability. In doing so, SPD can mitigate the appearance of disparate treatment of individuals based on factors other than true criminal activity and minimize perceived oversurveillance of areas where historically targeted communities reside or congregate.

DRAFT

City of Seattle

2020 Surveillance Impact Report Executive Overview

Computer-Aided Dispatch (CAD)

Seattle Police Department

DRAFT

Overview

The Operational Policy statements in this document represent the only allowable uses of the equipment and data collected by this technology.

This Executive Overview documents information about the collection, use, sharing, security and access controls for data that is gathered through Seattle Police Department's Computer-Aided Dispatch. All information provided here is contained in the body of the full Surveillance Impact Review (SIR) document but is provided in a condensed format for easier access and consideration.

1.0 Technology Description

CAD (Computer Aided Dispatch) software, made by Versaterm, consists of a set of servers and software deployed on dedicated terminals in the 9-1-1 center, on SPD computers, and as an application on patrol vehicles' mobile data computers (MDCs) and on some officers' smart phones.

When a request for police service is initiated by a 9-1-1 call or an officer on-viewing an incident, a CAD event is created by the 9-1-1 Center staff, and a unique CAD event ID number is automatically generated. Information related to that CAD event is entered into the CAD system. A call taker assigns the CAD event a specific type code and priority associated with the type of police service requested. The location of the event is entered, and CAD validates the address, locates the address electronically, and then plots it on a map. Based on this information, the call taker routes the CAD call to the appropriate dispatcher. The dispatcher then assigns patrol officers to the service request and records this information in the CAD event. Each of the assigned patrol officers then log their activities related to that request for service into CAD using established codes. When the request for service is completed, the primary officer assigned closes the CAD call. Based upon the codes used to close the CAD call, the system then automatically routes the information recorded into SPD's Records Management System (RMS) where additional information, such as police reports and supplementary material, is stored.

2.0 Purpose

Operational Policy:

> **CAD is the system used by SPD to coordinate and document, in real-time, requests for police service and SPD's response to those requests.**

The Seattle Police Department's 9-1-1 Center is the primary Public Safety Answering Point (PSAP) for emergency 9-1-1 calls placed within the City of Seattle. Computer Aided Dispatch (CAD) is a software package utilized by the Seattle Police Department's 9-1-1 Center. It assists 9-1-1 Center call takers and dispatchers with receiving requests for police services, collecting information from 9-1-1 callers, and providing dispatchers with real-time patrol unit availability so dispatchers may dispatch appropriate patrol resources to requests for police service. CAD software also enables real-time documentation of the Seattle Police Department's response to calls for service, including relevant information obtained by responding officers.

DRAFT

3.0 Data Collection and Use

Operational Policy:

> **Data collected by the CAD system is collected for the purpose of requesting police service or dispatching emergency response**

When an individual places a call to 9-1-1, the telephone number they are calling from, the location they are calling from, the name associated with the phone number (if available from the phone company), and the type of telephone service (landline, cell phone, VOIP phone) are provided by the West VIPER telephone system and automatically entered into CAD when a CAD call is initiated by the call taker.

Non-emergency calls, and associated phone numbers, are not automatically entered into CAD. If the call is determined to be a request for police services, call takers and dispatchers then manually enter additional information into CAD, such as the nature of the emergency, and create a CAD event to facilitate a police response. Call takers and dispatchers may add supplemental information into CAD regarding scene safety, descriptions of individuals, vehicles, and premises. Much of the privacy-sensitive information entered into CAD is provided by 9-1-1 or non-emergency callers or by officers or dispatchers who input information into the CAD system when responding to a call.

4.0 Data Minimization & Retention

Operational Policy:

> **SPD retains CAD data that is not case specific (i.e. not related to an investigation) for 90 days.**

Case specific data is maintained for the retention period applicable to the specific case type.

The CAD system documents information provided by the participants and witnesses in the event being reported, as input by SPD personnel. The system itself does not check for accuracy of the information that is provided by personnel. Instead, the Department may later determine that the information provided was not accurate and can provide updated information.

5.0 Access & Security

Operational Policies:

> **SPD's authorized users of CAD include all sworn personnel, 9-1-1 Center staff, and other civilian staff whose business needs require access to this data. Additionally, Seattle IT provides client services and operational support for IT technologies and applications.**

DRAFT

All authorized users of CAD must be CJIS certified and must maintain Washington State ACCESS certification. SPD Policy 12.050 defines the proper use of criminal justice information systems.

Access

Only authorized SPD users can access the system, technology, or the data. Access to the application is limited to SPD personnel via password-protected login credentials. All activity within CAD (including timeline of commands issued) generates a log that is auditable. Authorized SPD users, may have access to the system to document, review, or report on police activity pursuant to law and policy, to extract information for use in court or administrative proceedings as required by law, to respond to appropriate requests for information, to make aggregate information available to the public, and to provide information to oversight bodies on issues such as stop and detention rates, for example.

Security

Data is securely input and used on SPD's password-protected network with access limited to authorized users. The entire system is located on the SPD network that is protect by industry standard firewalls. ITD performs routine monitoring of the SPD network.

All the data in CAD is held in SPD/ITD servers, located on City premises on SPD networks. All data that goes to mobile clients are encrypted to FIP 140-2 standards and is therefore CJIS compliant.

6.0 Data Sharing and Accuracy

Operational Policies:

No person, outside of SPD and Seattle IT, has direct access to the application or the data.

Data obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law.

Data sharing is not an automatic component of the CAD system. Instead, discrete pieces of data may be shared with outside agencies and individuals only within the context of the situations outlined. Data sharing may be necessary for SPD to provide coordinated, rapid responses to 911 incidents, particularly reducing the amount of time needed to contact individuals, thereby improving outcomes.

Discrete pieces of data collected by CAD may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by SPD Policy 12.050 and 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayoral Directive, dated February 6, 2018.

Per City of Seattle's Privacy Statement, outlining commitments to the public about how we collect and manage their data: *We do not sell personal information to third parties for marketing purposes or for their own commercial use.* The full Privacy Statement may be found **here.**

7.0 Equity Concerns

Operational Policy:

> **SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.**

The CAD system is used to assist in the dispatch of police resources and document SPDs response to requests for service throughout the city of Seattle. There is no distinction in the levels of service this system provides to the various and diverse neighborhoods, communities, or individuals within the city.

DRAFT

City of Seattle

2020 Surveillance Impact Report Executive Overview

CopLogic

Seattle Police Department

DRAFT

Overview

The Operational Policy statements in this document represent the only allowable uses of the equipment and data collected by this technology.

This Executive Overview documents information about the collection, use, sharing, security and access controls for data that is gathered through Seattle Police Department's CopLogic system. All information provided here is contained in the body of the full Surveillance Impact Review (SIR) document but is provided in a condensed format for easier access and consideration.

1.0 Technology Description

CopLogic is a crime reporting software tool that allows members of the public to submit police reports online through a web-based interface. CopLogic is a Software as a Service (SaaS) owned and maintained by LexisNexis. SPD utilizes this technology in two ways: 1) An online public interface allows individuals to report a low-level crime in which no known or describable suspect is available, and for which individuals may need proof of police reporting (i.e., for insurance purposes), without waiting for an officer to dispatch and take a report; 2) An online password-protected interface allows retailers to enter information about retail theft on their property in which a suspect is known and suspect information is available.

2.0 Purpose

Operational Policies:

Individuals may use CopLogic to report a crime online when:

1) **The crime is within one of these categories:**
    a. **Property crimes including property destruction, graffiti, car break ins, theft of auto accessories, theft, shoplifting;**
    b. **Drug activity, harassing phone calls, credit card fraud, wage theft, identity theft, or lost property**
2) **The situation is non-emergency**
3) **The crime occurred within Seattle city limits (exception for identity theft);**
4) **No known suspects or information about the crime would allow for additional investigation.**

Retailers may use CopLogic to report a retail theft on their property when:

1) **The retailer participates in SPD's Retail Theft Program and has obtained a unique login identifier and password;**
2) **They have detained the suspect;**
3) **The suspect does not have any outstanding warrants; and**
4) **They verify the identification of the suspect and upload copies of the suspect's identification, if available.**

DRAFT

CopLogic is used by the public, including retailers, and, thus, its use is triggered whenever an individual instigates the submission of an online report. An SPD reviewer checks the submission for completion and does one of the following:

1) Sends a generic email to the submitter asking for additional information; or

2) Pushes the report to SPD's records management system, providing the report a General Offense ("GO") number, which is then sent back to the submitter.

3.0 Data Collection and Use

Operational Policy:

No information is collected from a source other than the individual instigating the submission of a report.

Public Interface: Individuals wishing to file a report visit Seattle Police Department's Online Reporting page (https://www.seattle.gov/police/need-help/online-reporting) and follow the prompts to enter information about low-level, non-emergency crimes for which no known suspects exist. CopLogic then generates a report and the reporter receives a temporary unique identification number. An SPD employee, the reviewer, verifies that the report is sufficient and complete. If further information or clarification is needed, the reviewer generates a generic email to the reporter, informing them that the report is missing information that must be included before the file is officially submitted, and providing a link to follow for updates. Once a reviewer determines that the report is complete, the information is electronically transferred into SPD's records management system and receives a general offense (GO) number. This GO number is then provided to the reporter for their records and for insurance purposes.

Retail Theft Interface: Retailers who participate in the Seattle Police Department's Retail Theft Program and wish to report a theft first contact the Seattle Police Department's non-emergency number to receive a case number. Then, they access the Retail Theft online page with unique password-protected login information and fill out the Retail Theft online report, which includes information about the retailer, the theft, and the suspect. In most circumstances, retailer security has detained the suspect and included copies of identification with the report that they then submit online.

4.0 Data Minimization & Retention

Operational Policy:

After a report is made, police officers assigned to the Internet and Telephone Reporting Unit (I-TRU) log in to the CopLogic web portal, utilizing individual user log-in IDs, to access the submitted reports.

DRAFT

Once the report is screened by an officer in the I-TRU unit, SPD utilizes an integration server to transfer reports generated in the CopLogic tool into SPD's Records Management System.

Before anyone is permitted to file a report online, they are prompted to answer a series of questions to determine if online reporting is appropriate for the event they wish to report. In addition, the Seattle Police Department provides guidelines to individuals reporting an event about what information they will need to submit to file a report online. Finally, an authorized SPD employee reviews each submission before accepting the report to ensure that appropriate and adequate information has been provided.

Retail security collects only information that is necessary to document and investigate the crime as required on the Retail Theft Reporting form. No other information is requested.

5.0 Access & Security

Operational Policies:

Only authorized SPD users can access the system, technology, or the data. Access to the application is limited to SPD personnel via password-protected login credentials.

Once data is input by individuals and retail users of CopLogic on the public-facing website, it is accessed and used on SPD's password-protected network.

Access

SPD reviewers within the I-TRU unit have access to the reports for the purposes of verifying accuracy and initiating the process of transferring the approved reports into the records management system with a case number (as is assigned to all SPD reports).

Collected data is securely viewed on SPD's password-protected network with access limited to authorized detectives and identified supervisory personnel within the I-TRU unit. Once a reported incident has been reviewed by SPD personnel, it is electronically transferred into the SPD records management system.

SPD reviewers within the I-TRU unit have access to the reports for the purposes of verifying accuracy and initiating the process of transferring the approved reports into the records management system with a case number (as is assigned to all SPD reports). Additionally, Seattle IT provides client services and operational support for IT technologies and applications. In supporting SPD systems, operational and application services deploy and service SPD technology systems.

DRAFT

Security

CopLogic data is stored remotely and managed by the technology provider, Lexis Nexis. Lexis Nexis is Privacy Shield Certified and adheres to the RELX Group Privacy Shield Principles. Per Lexis Nexis: "We use a variety of administrative, physical and technical security measures to help safeguard your personal information." Additionally, SPD's contract with Lexis Nexis includes a clause for audit, in which the "Consultant shall permit the City and any other governmental agency funding the Work, to inspect and audit all pertinent books and records."

SPD personnel can only access CopLogic data when authorized and provided a username and password for the system. CopLogic creates an audit log that records all activity in the system with usernames and timestamps.

6.0 Data Sharing and Accuracy

Operational Policy:

> **SPD has no data sharing partners for CopLogic. No person, outside of SPD, has direct access to the application or the data and all requests for information from CopLogic are processed based on existing SPD policies, legal guidelines, and as required by law.**

CopLogic is owned and maintained by Lexis Nexis. There are no data sharing agreements between SPD and any other entities for CopLogic data. Further, the contract between the City and LexisNexis provides that LexisNexis may only "use, transmit, distribute, modify, reproduce, display, and store the City Data solely for the purposes of (i) providing the Services as contemplated in [its contract with the City]; and (ii) enforcing its rights under [the contract]."

Per City of Seattle's Privacy Statement, outlining commitments to the public about how we collect and manage their data: *We do not sell personal information to third parties for marketing purposes or for their own commercial use.* The full Privacy Statement may be found **here.**

7.0 Equity Concerns

Operational Policy:

> **SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.**

Because the information received through the CopLogic portal comes from community members there is a risk that racial or ethnicity-based biased information may be entered. All the information entered is screened by authorized and trained SPD personnel.

DRAFT

SUMMARY and FISCAL NOTE*

Department:	Dept. Contact/Phone:	CBO Contact/Phone:
SPD / ITD	Rebecca Boatwright / Jonathan Porat / 206-256-5520	Jennifer Breeze/206-256-5972

** Note that the Summary and Fiscal Note describes the version of the bill or resolution as introduced; final legislation including amendments may not be fully described.*

1. BILL SUMMARY

Legislation Title: AN ORDINANCE relating to surveillance technology implementation; authorizing approval of uses and accepting the 2019 surveillance impact reports for the Seattle Police Department's use of surveillance technologies.

Summary and background of the Legislation: Per SMC Chapter 14.18 (also known as the Surveillance Ordinance), authorizing the approval of the surveillance impact reports for Seattle Police Department's use of existing technologies: 911 Logging Recorder, Computer Aided Dispatch, CopLogic, and Automated License Plate Reader (ALPR) for Patrol and ALPR for Parking Enforcement.

2. CAPITAL IMPROVEMENT PROGRAM

Does this legislation create, fund, or amend a CIP Project? ___ Yes _X_ No

3. SUMMARY OF FINANCIAL IMPLICATIONS

Does this legislation amend the Adopted Budget? ___ Yes _X_ No

Does the legislation have other financial impacts to the City of Seattle that are not reflected in the above, including direct or indirect, short-term or long-term costs?
This technology is currently in use by the Seattle Police Department and no additional costs, either direct or indirect, will be incurred based on the continued use of the technology. However, should it be determined that SPD should cease use of the technology, there would be costs associated with decommissioning the technologies. Additionally, there may be potential financial penalty related to breach of contract with the technology vendors.

Is there financial cost or other impacts of *not* implementing the legislation?
Per the Surveillance Ordinance, the City department may continue use of the technology until legislation is implemented. As such, there are no financial costs or other impacts that would result from not implementing the legislation.

4. OTHER IMPLICATIONS

a. Does this legislation affect any departments besides the originating department?
This legislation does not affect other departments. The technology under review is used exclusively by the Seattle Police Department.

b. Is a public hearing required for this legislation?
A public hearing is not required for this legislation.

c. Is publication of notice with *The Daily Journal of Commerce* and/or *The Seattle Times* required for this legislation?
No publication of notice is required for this legislation.

d. Does this legislation affect a piece of property?
This legislation does not affect a piece of property.

e. Please describe any perceived implication for the principles of the Race and Social Justice Initiative. Does this legislation impact vulnerable or historically disadvantaged communities? What is the Language Access plan for any communications to the public?
The Surveillance Ordinance in general is designed to address civil liberties and disparate community impacts of surveillance technologies. Each Surveillance Impact Review included in the attachments, as required by the Surveillance Ordinance, include a Racial Equity Toolkit review adapted for this purpose.

f. Climate Change Implications

1. **Emissions: Is this legislation likely to increase or decrease carbon emissions in a material way?**
   No.

2. **Resiliency: Will the action(s) proposed by this legislation increase or decrease Seattle's resiliency (or ability to adapt) to climate change in a material way? If so, explain. If it is likely to decrease resiliency in a material way, describe what will or could be done to mitigate the effects.**
   No.

g. If this legislation includes a new initiative or a major programmatic expansion: What are the specific long-term and measurable goal(s) of the program? How will this legislation help achieve the program's desired goal(s).
There is no new initiative or programmatic expansion associated with this legislation. It approves the continuation of use for the specific technologies under review.

List attachments/exhibits below:

SEATTLE CITY COUNCIL
CENTRAL STAFF

February 25, 2021

MEMORANDUM

To: Transportation and Utilities Committee
From: Lise Kaye, Analyst
Subject: Council Bill 120004 Seattle Police Department Surveillance Technologies

On Wednesday, March 3, 2021 the Transportation and Utilities Committee will discuss Council Bill (CB) 120004. The proposed bill is intended to meet the requirements of Seattle Municipal Code Chapter 14.18, Acquisition and Use of Surveillance Technologies.[1] (Attachment 1 to this memo summarizes these requirements and the process by which the Executive develops the required Surveillance Impact Reports.) The proposed bill would approve the Seattle Police Department's (SPD's) continued use of the following technologies:

1. **Automated License Plate Readers**
2. **Parking Enforcement System**
3. **Computer-Aided Dispatch**
4. **CopLogic**
5. **911 Logging Recorder**

Passage of the bill would also accept the Surveillance Impact Reports (SIRs) for these technologies, as further detailed in each section of this memo. As required by SMC 14.18.020(3), the Executive conducted a public engagement process to receive public comments and/or concerns about this technology. In addition, the Community Surveillance Working Group ("Working Group") has completed a Privacy and Civil Liberties Impact Assessment ("Impact Assessment") of the technology, and the City's Chief Technology Officer (CTO) has provided his response ("Response") to the Impact Assessment.

This memo provides summaries of each of the five SIRs in the order listed above. Each summary includes a brief synopsis of the potential civil liberties impacts from the technology and the public engagement processes for each, as reported in the SIRs. The summaries also describe concerns and recommendations from the Working Group's Impact Assessments and the CTO's Response. Finally, each section identifies policy considerations for possible Council action.

Committee Action

Options for Council action are as follows:

1. Pass CB 120002, 120003 and/or 120004 as transmitted;
2. Request Central Staff to prepare amendments to the Council Bill and/or to one or more of the SIRs to address additional concerns or issues; or
3. Take no action.

[1] (Ord. 125679 , § 1, 2018; Ord. 125376 , § 2, 2017.)

1. Automated License Plate Readers

CB 120004 would approve SPD's continued use of and accept the SIR for Automated License Plate Readers, which employ a combination of high definition infrared digital cameras (Neology PIPs) and locational software (Neology Back Office System Software, or "BOSS"). SPD uses Automated License Plate Readers to check a vehicle against a "HotList" of license plate numbers from the Washington Crime Information Center, the FBI's National Crime Information Center, and SPD's investigations to identify stolen vehicles, and vehicles wanted in conjunction with felonies or associated with wanted persons or Amber and Silver Alerts (abducted children and missing people). Officers must verify that the system accurately read the license plate and ask Dispatch to verify that a vehicle is listed as stolen before taking any action. SPD retains data from Automated License Plate Readers for 90 days, or in investigative files, for the retention period related to the incident in question.

SPD Policy 16.170 directs that Automated License Plate Readers are only to be used for the following purposes:

- Locating stolen vehicles;
- Locating stolen license plates;
- Locating wanted, endangered or missing persons; or those violating protection orders;
- Canvassing the area around a crime scene;
- Locating vehicles under SCOFFLAW[2]; and
- Electronically chalking vehicles for parking enforcement purposes.

SPD Policy 16.170 also limits access to data maintained on the Back Office System Software to the following purposes:

- Search of specific or partial plate(s) and/or vehicle identifiers as related to:
- A crime in-progress;
- A search of a specific area as it relates to a crime in-progress;
- A criminal investigation; or
- A search for a wanted person; or
- Community caretaking functions such as, locating an endangered or missing person.
- Officers/detectives conducting searches in the system will complete the Read Query screen documenting the justification for the search and applicable case number.

Civil Liberties and Potential Disparate Impacts on Historically Marginalized Communities

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit (RET) to inform the SIR public engagement process and to highlight and mitigate impacts on racial equity from the use of the technology. The RET for the Automated License Plate

[2] See Ordinance 124558 relating to vehicle immobilization due to unpaid tickets for parking infractions

Readers identifies a potential civil liberties impact as the risk that, without appropriate policy, license plate data could be used to identify individuals without reasonable suspicion of having committed a crime or to search for information that is not incidental to any active investigation. The RET also cites the potential concern that SPD would over-surveil vulnerable or historically targeted communities, deploying the Automated License Plate Reader to diverse neighborhoods more often than to other areas of the City.

In response to concerns expressed during development of the SIR, SPD updated its relevant policies (SPD Policy 16.170) in January 2019 by adding definitions of the terms used in the operation of the Automated License Plate Reader technology, detailing authorized and prohibited uses, expanding on the required training for employees prior to access and use, defining response to alerts, detailing how Automated License Plate Reader equipment is to be handled, detailing data storage and retention, and detailing policy around the release or sharing of Automated License Plate Reader data. SPD also updated its policy related to Foreign Nationals, emphasizing that SPD has no role in immigration enforcement and will not inquire about any person's immigration status. The RET states that response to these updated policies will be "compiled and analyzed" as part of the CTO's annual equity assessments.

Public Engagement

The Executive accepted public comments on this technology from October 8, 2018 through November 5, 2018 and conducted three public meetings to solicit public comment on this SIR and the SIR for SPD's Parking Enforcement Systems on October 22, 29 and 30, 2018. In addition, the Department of Neighborhoods conducted two focus groups on November 8 and November 20, 2018. Appendix B in the SIR includes a statistical analysis of public comments (specific to Automated License Plate Readers) and demographics (including all Group 1 SIR Comments); Appendix E contains comments and survey results received from members of the public, some which expressed support for this technology and others expressing a wide range of privacy concerns, including with respect to surveillance overall; Appendix F contains letters from three organizations concerned about issues including use of data, data retention, data sharing and transparency; and Appendix G contains letters submitted from the public expressing concern about surveillance in general and about issues including data access, retention, sharing, and transparency.

Privacy and Civil Liberties Impact Assessment – Automated License Plate Reader

The Working Group's Impact Assessment identifies eight concerns about the allowable use of data, data access, collection, retention and sharing, system audits, the relation of this technology and the effectiveness of the technology in solving crimes.[3] It also recommends that Council adopt five specific policies. The following sections summarize the CTO's Response to the concerns and describe whether and how the SIRs as drafted would address the Working Group's recommended policies.

[3] The Impact Assessment states that the SIR does not include the new policies or indicate whether the new policies have been adopted by SPD. However, the updated SIR states that the new SPD Automated License Plate Reader policy went into effect on February 1, 2019 and references to the new policy are noted in the updated SIR next to the original policy references.

Key Concerns and the CTO's Response. Table 1 summarizes CTO's response to each of the Working Group's concerns. The Response concludes that SPD's updated policy, training and limitations from the technology itself provide adequate mitigation for the potential privacy and civil liberty concerns raised by the Working Group.

Table 1. CTO Response to Privacy and Civil Liberties Impact Assessment of SPD's Automated License Plate Reader Technology

Working Group Concern	CTO Response
1. Does not impose meaningful restrictions on the purposes for which Automated License Plate Reader data may be collected or used	SPD Policy outlines the specific situations or use cases that Automated License Plate Reader can be both used for and under which the data can be accessed.[4] The specific limitations on use preclude a scenario of "dragnet" use where Automated License Plate Reader is constantly in use as a patrol vehicle moves throughout the City.
2. Does not justify SPD's 90-day retention period.	SPD must follow State requirements for retention of criminal justice data.[5]
3. Does not limit data sharing by policy or statute.	SPD's revised policy 16.170 addresses data sharing and states, "Automated License Plate Reader data will only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law."[6]
4. Does not make clear whether and how audits of inquiries to the system can be conducted (see SIR Sections 4.10 and 8.2, for example).	SPD's Policy 16.170 outlines that the Office of Inspector General (OIG) is responsible for conducting periodic audits of the Automated License Plate Reader system.[7]

[4] See SPD Policy 16.170

[5] Washington State's law enforcement agency retention requirements vary by type of record (e.g. case status and type of investigation)

[6] See also additional references in the SIR to SPD Policy 12.050 for public records requests, SPD Policy 12.055 allowing data sharing with authorized criminal justice researchers, and SPD Policy 12.080 pertaining to requests for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies

[7] Per SPD Policy 16.170, The Office of the Inspector General "may audit Department records at any time to ensure compliance with this policy."

5. Does not make clear how and to what degree Patrol and Parking Enforcement Automated License Plate Reader systems are separated, and whether SPD's policies on Automated License Plate Reader apply to the Parking Enforcement Systems	Parking Enforcement's AutoVu data[8] and Patrol's Automated License Plate Reader data have different retainage policies and separate administrators. Parking Enforcement Officers (PEOs) do not have access to stored Automated License Plate Reader data in the Patrol system.[9]
6. Does not include measures to minimize false matches.	This concern is adequately covered in the SIR, including confirmation and verification measures.
7. Does not include systematic tracking to assess how many crimes each year are actually solved using Automated License Plate Reader data.	The Office of Inspector General for Public Safety's Annual Surveillance Usage Review should address usage patterns of this technology.
8. Does not create clear restrictions on who can access the data.	SPD Policy clearly states that only authorized users within the Department can access the data collected by Automated License Plate Reader; all access is logged and auditable.

Recommended Policies. The Impact Assessment recommends that Council ensure that SPD adopt "clear and enforceable policies that ensure, at a minimum, the following:

1. The purposes of Automated License Plate Reader use must be clearly defined, and operation and data collected must be explicitly restricted to those purposes only.
2. Dragnet, suspicionless [sic] use of Automated License Plate Reader must be outlawed.
3. Data collected should be limited to license plate images, and no images of vehicles or occupants should be collected.
4. Data retention should be limited to the time needed to effectuate the purpose defined.
5. Data sharing with third parties must be limited to those held to the same restrictions as agency deploying the system."

Table 2 describes how the SIRs as drafted would address these recommendations. Areas not fully addressed are included in the "Policy Considerations" section.

[8] AutoVu is used for Scofflaw enforcement (i.e. vehicle impoundment due to unpaid parking fines), enforcement of time-restricted parking areas and restricted parking zones, and also for identifying stolen vehicles or vehicles sought in connection with criminal investigation.

[9] Section 1.1 of the Privacy Assessment in the SIR states that Parking Enforcement and Patrol are held to the same rules and policies for use of Automated License Plate Readers.

Table 2. Working Group Recommendations Addressed in the SIR

Working Group Recommendation	Whether/How Addressed in SIR
1. Define the purposes of Automated License Plate Reader use and restrict its operation and data collection use to those purpose.	**Executive Overview.** Operational Policies represent the only allowable uses of the equipment and data collected by this technology. Note: the Executive Overview is not adopted by CB 120004. *See "Policy Considerations"*
2. Outlaw "dragnet, suspicionless [sic]" use of the Automated License Plate Reader	**3.20** The use of Automated License Plate Readers is limited to the "search of specific or partial plate(s) and/or vehicle identifiers as related to: a crime in progress, a search of a specific area as it relates to a crime in-progress, a criminal investigation, a search for a wanted person, or community caretaking functions such as locating an endangered or missing person."
3. Limit data collection to license plate images; prohibit collection of vehicle or occupants' images	**3.20** The use of Automated License Plate Readers is limited to the "search of specific or partial plate(s) and/or vehicle identifiers **4.9** The Automated License Plate Reader will not be used to intentionally capture images in private area or areas where a reasonable expectation of privacy exists, nor shall it be used to harass, intimidate or discriminate against any individual or group.
4 Limit data retention to the time needed to effectuate the defined purpose	**5.1** All Automated License Plate Reader data is deleted after 90 days unless it is related to a criminal investigation and exported in support of that investigation prior to 90 days[10]
5 Limit data sharing with third parties to those held to the same restrictions as the agency deploying the system	**6.3** Law enforcement agencies receiving criminal history information are subject to state and federal data sharing regulations.[11] Once disclosed in response to Public Records Act request, there are no restrictions on non-City data use; however, applicable exemptions will be applied prior to disclosure to any requestor who is not authorized to receive exempt content.

[10] This is consistent with LE2010-054 and LE2010-055 of Washington State's Law Enforcement Records Retention Schedule for Violations and Traffic Enforcement.
[11] Federal regulations include 28 CFR Part 20. Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

Policy Consideration

Central Staff has identified the following potential policy consideration relative to the Working Group's key concerns and recommendations:

1. Restrictions on use. SPD's policies do not concisely specify the allowable uses of the Automated License Plate Reader technology. Council may wish to amend the proposed Council Bill to also adopt the Executive Overview of the SIR which identifies specific language as constituting the enforceable policies and procedures applicable to the technology.

2. Parking Enforcement Systems

CB 120004 would approve SPD Parking Enforcement Officers' continued use of and accept the SIR for Genetec's AutoVu Automated License Plate Reader hardware. The SIR states that all rules and policies that govern Patrol's use of Automated License Plate Reader technology are "applicable in the same manner" as they are when it is used by Parking Enforcement. An October 2018 version of the SIR was updated in January 2019 to align with revised SPD policies pertaining to Patrol's use of Automated License Plate Readers. References to the new policies are noted in the updated SIR next to the original policy references.

Parking Enforcement Officers use the AutoVu hardware with the following software and devices, which the SIR describes as "non-surveillance technologies":

- Genetec's Patroller software, the interface and backend server through which retention periods are set (and auditable), user permissions are managed, user activity is tracked and logged, and camera "read" and "hit" data is accessible.
- Samsung devices allow Officers to access the software required to write tickets and enter ticket information.
- Gtechna software prints citations for vehicles found in violation of scofflaw, overtime zone parking, and metered parking.

When this SIR was prepared, eight parking enforcement vehicles carried Automated License Plate Reader equipment, including high definition infrared digital cameras on three vehicles designated for "scofflaw enforcement" – immobilization of vehicles with multiple unpaid parking tickets. All data collected from those cameras is retained in the "BOSS" database[1] for 90 days, unless a record is related to a parking violation or criminal investigation. The other five vehicles are equipped to digitally "chalk" vehicles parked in time-restricted zones, using GPS location and stem-valve comparison technology. All data collected from those five vehicles is deleted from the system at the end of each shift, except for records identified as being related to a parking violation or criminal investigation and exported during the shift it was captured.[2]

<u>Civil Liberties and Potential Disparate Impacts on Historically Marginalized Communities</u>

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit (RET) to inform the SIR public engagement process and to highlight and mitigate impacts on racial equity from the use of the technology. The RET for SPD's Parking Systems Enforcement identifies the same civil liberties risks as for Automated License Plate Reader technology. These include the risk that, without appropriate policy, license plate data could be used to identify individuals without reasonable suspicion of having committed a crime, or to search for information that is not incidental to any active investigation. It also cites the same potential concern that SPD would over-surveil vulnerable or historically targeted communities, deploying Automated License Plate Readers to diverse neighborhoods more often than to other areas of the City.

[1] Neology Back Office System Software, or "BOSS"
[2] SPD currently has six sedans, two vans and one truck.

In addition to the updated Automated License Plate Reader Polices described above, the SIR describes the following actions by which SPD will ensure that parking enforcement occurs equitably throughout the City: follow policy limiting use of Automated License Plate Reader technology to routine parking enforcement; delete all data collected by parking enforcement vehicles with Automated License Plate Reader technology at the end of the parking enforcement officer's shift; ensure that collected data is used for legitimate law-enforcement purposes; continue to audit the system on a regular basis.

Public Engagement

The Executive accepted public comments on this technology from October 8, 2018 through November 5, 2018 and conducted three public meetings to solicit public comment on this SIR and the SIR for SPD's Parking Enforcement Systems on October 22, 29 and 30, 2018. In addition, the Department of Neighborhoods conducted two focus groups on November 8 and November 20, 2018. Appendix B in the SIR includes a statistical analysis of public comments a (specific to Parking Enforcement Systems) and demographics (including all Group 1 SIR Comments); Appendix E contains comments and survey results received from members of the public, some which expressed support for this technology and others which expressed a wide range of privacy concerns including data retention, equitable enforcement, and surveillance in general; Appendix F contains letters from three organizations concerned about issues including integration with the Patrol's Automated License Plate Reader technology, data access, retention and sharing, and transparency; and Appendix G contains letters submitted from the public expressing concern about surveillance in general and about issues including integration with the Patrol's Automated License Plate Reader technology data and data retention.

Privacy and Civil Liberties Impact Assessment – Parking Enforcement Systems

The Working Group's Impact Assessment states that the same concerns identified about SPD's patrol officers' use of Automated License Plate Readers apply equally to its Impact Assessment of Parking Enforcement Systems. In addition, the Impact Assessment identifies three concerns about the use of SPD's Parking Enforcement Systems technology and recommends that Council adopt four specific policies. The concerns include questions about the allowable use of these systems and the data collected by them, over-collection and over-retention of data, and sharing of data with third parties. The following sections summarize the CTO's Response to the concerns and describe whether and how the SIR as drafted would address the Working Group's recommended policies.

Working Group Concerns and the CTO's Response. Table 3 summarizes CTO's response to each of the Working Group's concerns. The Response concludes that SPD's updated policy, training and limitations from the technologies themselves provide adequate mitigation for the potential privacy and civil liberty concerns raised by the Working Group.

Table 3. CTO Response to Privacy and Civil Liberties Impact Assessment of SPD's Parking Enforcement Systems Technology

Working Group Concern	CTO Response
1. The use of these systems and the data collected by them for purposes other than those intended.	Appropriate policies and technology are in place to restrict data use and access.
2. Over-collection and over-retention of data	SPD must follow State requirements for retention of criminal justice data. Data collected by AutoVu (parking enforcement system) is not retained after the end of the officer's shift.
3. Sharing of data with third parties (such as federal law enforcement agencies)	SPD's revised policy 16.170 addresses data sharing and states, "Automated License Plate Reader data will only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law."

Recommended Policies. The Impact Assessment makes the following recommendations:

- SPD's policy must require that the data collected by Parking Enforcement Automated License Plate Reader systems is not shared with Patrol Automated License Plate Reader systems.
- SPD's policy must require all data-sharing relationships to be disclosed to the public in clear terms, and, as stated above in the Automated License Plate Reader-Patrol Section, SPD's policy must limit sharing of Automated License Plate Reader data to third parties that have a written agreement holding those third parties to the same use, retention, and access rules as SPD, and requiring disclosure of to whom and under what circumstances the data are disclosed.
- SPD's policy must require detailed records of Automated License Plate Reader scans, hits, and revenue generated specifically attributable to those hits, as well as an accounting of how Automated License Plate Reader use varies by neighborhood and demographic.
- SPD's policy must make explicit what photos are taken by the Automated License Plate Reader on Parking Enforcement vehicles, and require the same 48-hour maximum retention period for all photos.

Table 4 describes how the SIR as drafted would address these recommendations. Areas not fully addressed are included in the "Policy Considerations" section.

Table 4. Working Group Recommendations Addressed in the SIR

Working Group Recommendation	Whether/How Addressed in SIR
1. Data collected by Parking Enforcement Automated License Plate Reader systems must not be shared with Patrol Automated License Plate Reader systems.	**2.5** Parking enforcement ALPR data collected by Scofflaw enforcement boot vans is stored with Patrol ALPR data in the Neology Back Office System Software (BOSS). **4.4** Parking enforcement officers upload Automated License Plate Reader data from their shift to the BOSS server prior to shutting down their computer. *See "Policy Considerations"*
2. Disclose all data-sharing relationships to the public and limit data sharing with third parties to those held via written agreement to the same restrictions as SPD	**6.1** This section of the SIR lists all the outside entities with whom parking enforcement data may be shared. **6.3** Law enforcement agencies receiving criminal history information are subject to state and federal regulations.[3] Once disclosed in response to Public Records Act request, there are no restrictions on non-City data use; however, applicable exemptions will be applied prior to disclosure to any requestor who is not authorized to receive exempt content.
3. Keep detailed records of Automated License Plate Reader scans, hits, and revenue generated specifically attributable to those hits, as well as an accounting of how Automated License Plate Reader use varies by neighborhood and demographic.	**2.2** This section of the SIR provides the revenue collected from parking citation sin 2016 and 2017. **2.5** Parking enforcement ALPR data collected by Scofflaw enforcement boot vans is stored with Patrol ALPR data in the Neology Back Office System Software (BOSS). **4.10** All activity in the AutoVu system is logged and can be audited.
4. Make explicit what photos are taken by the Automated License Plate Reader on Parking Enforcement vehicles, and require the same 48-hour maximum retention period for all photos	**4.1** Automated License Plate Readers on Parking Enforcement vehicles take a burst of 26 pictures of each parked vehicle, for visual photo comparison when the same vehicle is later examined for time zone violation. **4.9** Automated License Plate Readers will not be used to intentionally capture images in private area or areas where a reasonable expectation of privacy exists, nor shall it be used to harass, intimidate or discriminate against any individual or group. **4.4** Parking enforcement officers upload Automated License Plate Reader data from their shift to the BOSS server prior to shutting down their computer. **4.2** All data collected by the Parking Enforcement sedans is deleted after 90 days unless it is related to a criminal investigation and exported in support of that investigation prior to 90 days[4]

[3] Federal regulations include 28 CFR Part 20. Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

[4] This is consistent with LE2010-054 and LE2010-055 of Washington State's Law Enforcement Records Retention Schedule for Violations and Traffic Enforcement.

Policy Considerations

Central Staff has identified the following potential policy consideration relative to the Working Group's key concerns and recommendations:

1. Restrictions on use. SPD's policies do not concisely specify the allowable uses of the Parking Enforcement Systems technology. Council may wish to amend the proposed Council Bill to also adopt the Executive Overview of the SIR which identifies specific language as constituting the enforceable policies and procedures applicable to the technology.
2. Data Sharing between Patrol and Parking Enforcement. SPD's current policies and practice provide for data sharing between the automated license plate reader systems used during Patrol and Parking Enforcement operations. Council may wish to amend the SIR to restrict such sharing.
3. Parking Enforcement System – Equitable Enforcement. The SIR describes a series of actions that Parking Enforcement Officers will take that will ensure that parking enforcement occurs equitably throughout the City, but the SIR does not describe whether the Parking Enforcement System technologies are being used in such a way as to ensure equitable enforcement. Council may wish to request that the Office of Inspector General review this issue as part of its Annual Surveillance Usage Review.
4. Parking Enforcement System – Genetec Patroller Software. Section 1.1 of the SIR describes Genetec's Patroller software as "non-surveillance" technology. However, this software is used for storing and retaining data once it is captured by the AutoVu hardware, which has been classified as surveillance technology. Section 2.3 of the SIR states that Patroller is used to set retention periods, manage user permissions, track and log user activity and access camera data. Section 4.10 of the SIR describes safeguards for protecting data both in the AutoVu system and in "Parking Enforcement software systems." Council may wish to amend the SIR to include the Patroller software in the definition of the Parking Enforcement Systems surveillance technology.

3. Computer-Aided Dispatch

CB 120004 would approve SPD's continued use of and accept the SIR for software, made by Versaterm, used by SPD's 911 center and patrol officers to respond to 911 calls. The software collects information from 911 callers, informs dispatchers as to patrol unit availability and documents SPD's response to the calls, after which the information is stored in SPD's Records Management System. SPD retains this data for 90 days, unless it is related to an investigation, in which case it is maintained for the retention period applicable to the type of case. Authorized SPD users can extract information for use in legal proceedings and to respond to requests for information.

Discrete pieces of data may be shared with other law enforcement agencies, but all requests for data from Federal Immigration and Customs Enforcement are referred to the Mayor's Office Legal Counsel, per the Mayoral Directive dated February 6, 2018. If a non-emergency call requires police services, officers or dispatchers will enter relevant information manually into the Computer-Aided Dispatch system. SPD's dispatch center transfers calls requiring a fire or medical response that do not also require a police response to the Seattle Fire Alarm Center; those calls are not entered into SPD's Computer-Aided Dispatch system.

Civil Liberties and Potential Disparate Impacts on Historically Marginalized Communities

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit (RET) to inform the SIR public engagement process and to highlight and mitigate impacts on racial equity from the use of the technology. The RET for the SPD's Computer-Aided Dispatch identifies potential civil liberties impacts from disclosure of personally identifiable information gathered during 911 calls. The SIR states that SPD mitigates the risk of unintentional release of privacy data through data security processes and by requiring state ACCESS certification (A Central Computerized Enforcement Service System) and federal CJIS (Criminal Justice Information Services) certification for all CAD users.

The SIR also identifies data sharing, storage and retention as having the potential to contribute to structural racism, thereby creating a disparate impact on historically targeted communities.[1] The SIR states that SPD mitigates this risk through policies regarding the dissemination of data in connection with criminal prosecutions, the Washington Public Records Act, and other authorized researchers. In addition, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures. The RET does not identify metrics to be used as part of the CTO's annual equity assessments.[2]

---

[1] Historical community or department practices could produce data in a CAD system that would portray certain communities as higher in crime than in other neighborhoods or elevate the involvement in potential criminal events by certain demographic groups. An approach to storage, retention, and integration of these data that was not cognizant of these possibilities might allow for the continuation of these perceptions, with potential disparate enforcement responses.

[2] SMC 14.18.050B requires that the CTO produce and submit to the City Council a Surveillance Technology Community Equity Impact Assessment and Policy Guidance Report that addresses whether Chapter 14.18 of the SMC is effectively meeting the goals of the Race and Social Justice Initiative, any recommended adjustments to laws and policies to achieve a more equitable outcome, and any new approaches and considerations for the SIRs.

Public Engagement

The Executive accepted public comments on this technology from February 5 – March 5, 2019 and conducted one public meeting for multiple SIRs on February 27, 2019.[3] In addition, the Department of Neighborhoods conducted four focus groups in partnership with organizations serving communities of color and other marginalized communities.[4] The SIR includes all notes from the focus groups (Appendix D); comments pertaining solely to these technologies received from members of the public (Appendix E), department responses to public inquiries (Appendix F); and, letters from organizations or commissions (Appendix G). Of the very few public comments received about this technology, concerns included support for the technology, concerns about security of data, and concern about the distribution of an all-points bulletin known as "BOLO" (be on the lookout) via the system. Letters from organizations expressed concern about the need for limitations on the use of data, data retention and sharing, and about the age of the system.

Privacy and Civil Liberties Impact Assessment – Computer-Aided Dispatch

The Impact Assessment identifies three concerns about the use of SPD's Computer-Aided Dispatch technology and recommends that Council adopt four specific policies. The concerns include the lack of a policy defining the purpose of the technology and limiting its use to that purpose, data retention and access to data. The following sections summarize the CTO's Response to the concerns and describe whether and how the SIR as drafted would address the Working Group's recommended policies

Key Concerns and the CTO's Response. Table 5 summarizes CTO's response to each of the Working Group's concerns. In his response to the Impact Assessment, the City's CTO found that that the SIR provided information specific to each concern.

Table 5. CTO Response to Privacy and Civil Liberties Impact Assessment of SPD's Computer-Aided Dispatch Technology

Working Group Concern	CTO Response
1. No policy defining the purpose of the technology and limiting its use to that purpose	SPD policies and limitations pertaining to the purpose and use of data collected through the CAD system are clearly outlined in the SIR response.
2. Unclear whether and what data is retained within the Computer-Aided Dispatch and Records Management Systems	The specifics about retention of data collected by law enforcement are clearly provided in the SIR.

[3] The February 27, 2019 City Surveillance Technology Fair solicited comments on three Seattle Police Department Technologies: 911 Call Logging Recorder, Computer-Aided Dispatch, and CopLogic; Seattle Fire Department's Computer-Aided Dispatch technology; Seattle City Light's Current Diversion Technologies; and Seattle Department of Transportation's Acyclica travel time measurement technology. The Fair flyer in the SIR erroneously lists the year of the meeting as "2018" instead of "2019."

[4] Appendix D contains notes from these focus group meetings, which were conducted as part of a "World Café" pilot project in collaboration with the Council on American-Islamic Relations, Entre Hermanos, Byrd Barr Place, and Friends of Little Saigon. Notes from Entre Hermanos are in Spanish; Executive staff are reviewing options to translate these notes into English.

3. Unclear which internal and third parties have access to SPD's Computer-Aided Dispatch Data	Details about legal obligations, SPD policy and technology access controls for data access and sharing are provided in the SIR.

Recommended Policies. The Impact Assessment recommends that Council ensure that SPD adopt "clear and enforceable policies that ensure, at a minimum, the following:

1. The purpose of use must be clearly defined as emergency operations, and the operation and data collected by the tool must be explicitly restricted to that purpose only.
2. Data retention within CAD, to the extent there is any, must be limited to the time needed to effectuate the emergency operations purpose defined.
3. Data sharing with third parties, if any, must be limited to those held to the same restrictions.
4. Clear policies must govern operation, and all operators should be trained in those policies."

Table 6 describes how the SIR as drafted would address these recommendations. Areas not fully addressed are included in the "Policy Considerations" section.

Table 6. Working Group Recommendations Addressed in the SIR

Working Group Recommendation	Whether/How Addressed in SIR
1. Define the purpose of Computer-Aided Dispatch (SPD) as emergency operations and restrict its operation and data collected to that purpose.	**Executive Overview.** Operational Policies represent the only allowable uses of the equipment and data collected by this technology. Note: the Executive Overview is not adopted by CB 120003. *See "Policy Considerations"*
2. Limit retention of data within CAD to the time needed to effectuate the emergency operations purpose	SPD must follow State requirements for retention of criminal justice data.
3. Limit data sharing with third parties to those held to the same restrictions as the agency deploying the system	**6.3** Law enforcement agencies receiving criminal history information are subject to state and federal regulations.[5] Once disclosed in response to a Public Records Act request, there are no restrictions on non-City data use; however, applicable exemptions will be applied prior to disclosure to any requestor who is not authorized to receive exempt content.
4. Operation of Computer-Aided Dispatch should be governed by clear policies in which all operators have been trained.	**7.2** SPD Dispatchers undergo training on the use of CAD, which includes privacy training. All authorized users of CAD must be CJIS certified and must maintain Washington State ACCESS certification.

[5] Federal regulations include 28 CFR Part 20. Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

Policy Considerations

Central Staff has identified the following potential policy considerations relative to the Working Group's key concerns and recommendations:

1. Restrictions on use. SPD's policies do not concisely specify the allowable uses of Computer-Aided Dispatch and its data. Council may wish to amend the proposed Council Bill to also adopt the Executive Overview of the SIR which identifies specific language as constituting the enforceable policies and procedures applicable to the Computer-Aided Dispatch technology.
2. Annual equity assessment metrics. SPD has not finalized metrics to be used in evaluating the Computer Aided Dispatch Technology as part of the CTO's annual equity assessments. These assessments are intended to play a key role in determining whether the City's surveillance legislation is meeting the goals of the Race and Social Justice Initiative. Council may wish to request a report on the proposed metrics by a date certain and/or Council may wish to defer approval of this SIR, pending completion of these metrics.

4. CopLogic

CB 120004 would approve SPD's continued use of and accept the SIR for CopLogic, a crime reporting software tool owned by LexisNexis. The software has two applications: 1) individuals may report a low-level crime[1] in which no known or describable suspect is available, and for which individuals may need proof of police reporting (i.e., for insurance purposes), and 2) businesses that participate in SPD's Retail Theft Program may enter information about retail theft on their property in which a suspect is known and suspect information is available.[2] Reports from individuals are assigned a general offense number for their records and for insurance purposes.

Businesses complete an online Security Incident Report, which may include copies of identification if security personnel have detained the suspect. The business issues a written trespass warning to the suspect, photographs the suspect and then may release the individual or turn them over to the police. An SPD detective reviews the Security Incident Report and submits the reviewed case to the City Attorney's Office to be reviewed for charges. Once either type of report has been screened and accepted by SPD personnel, it is transferred into SPD's Records Management System.

The SIR includes historical data on CopLogic's effectiveness from 2012, with 2018 figures showing a reduction of 20,356 police hours and savings over $1 million by eliminating the need for a patrol officer to respond in person to these incidents.

Civil Liberties and Potential Disparate Impacts on Historically Marginalized Communities

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit (RET) to inform the SIR public engagement process and to highlight and mitigate impacts on racial equity from the use of the technology. The RET for the CopLogic technology identifies two potential civil liberties risks: 1) that information from the system could be disseminated intentionally or unintentionally in ways that could negatively impact peoples' civil liberties; and 2) the risk that racial or ethnicity-based biased information may be entered into the system. The SIR states that SPD mitigates those risks by screening information entered into the system[3] and by virtue of the fact that SPD employees are subject to multiple department policies pertaining to computer and records access, dissemination of data and policies prohibiting bias-based policing.[4] The SIR also identifies data sharing, storage and retention as having the potential to contribute to structural racism, thereby creating a disparate impact on historically

[1] The crime must be within one of these categories of crime: a. Property crimes including property destruction, graffiti, car break ins, theft of auto accessories, theft, shoplifting; or b. Drug activity, harassing phone calls, credit card fraud, wage theft, identity theft, or lost property

[2] SPD's Retail Theft webpage reports that approximately 120 stores participate in this program.

[3] Screeners do not edit the information received through CopLogic, other than accidentally incorrect information that the reviewing officer or reporting party identifies.

[4] All SPD employee access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services. SPD Policy 5.140 forbids bias-based policing.

targeted communities. The SIR states that SPD mitigates this risk through policies regarding the dissemination of data in connection with criminal prosecutions, the Washington Public Records Act, and other authorized researchers. The RET also reports that SPD had not yet finalized the metrics to be used as part of the CTO's annual equity assessments.[5]

Public Engagement

The Executive accepted public comments on this technology from February 5 – March 5, 2019 and conducted one public meeting for multiple SIRs on February 27, 2019.[6] In addition, the Department of Neighborhoods conducted four focus groups in partnership with four organizations serving communities of color and other marginalized communities.[7] The SIR includes all notes from the focus groups (Appendix D); comments pertaining solely to these technologies received from members of the public (Appendix E), department responses to public inquiries (Appendix F); and, letters from organizations or commissions (Appendix G). Comments included support for and concerns about the technologies. Several of the supportive comments included requests for the technology to be available in languages other than English. Concerns included uneven access to the programs for those without computers or English fluency, the potential for racial bias in both kinds of reporting and for inaccurate reports, unfair treatment of individuals suspected of shoplifting, the potential for LexisNexis to use inaccurate information for crime mapping, and questions about data collection, retention and sharing.

Privacy and Civil Liberties Impact Assessment – CopLogic

The Impact Assessment identifies three concerns about the use of SPD's CopLogic technology and recommends that Council adopt specific policies and contract provisions. The concerns include data retention, civil liberty impacts of the retail theft program, and third-party data sharing. The following sections summarize the CTO's Response to the concerns and describe whether and how the SIR as drafted would address the Working Group's recommended policies.

In his response to the Privacy and Civil Liberties Impact Assessment, the City's CTO found that that SPD's policy, training and limitations from the technology itself outlined in the SIR provide

[5] SMC 14.18.050B requires that the CTO produce and submit to the City Council a Surveillance Technology Community Equity Impact Assessment and Policy Guidance Report that addresses whether Chapter 14.18 of the SMC is effectively meeting the goals of the Race and Social Justice Initiative, any recommended adjustments to laws and policies to achieve a more equitable outcome, and any new approaches and considerations for the SIRs.
[6] The February 27, 2019 City Surveillance Technology Fair solicited comments on three Seattle Police Department Technologies: 911 Call Logging Recorder, Computer-Aided Dispatch, and CopLogic; Seattle Fire Department's Computer-Aided Dispatch technology; Seattle City Light's Current Diversion Technologies; and Seattle Department of Transportation's Acyclica travel time measurement technology. The Fair flyer in the SIR erroneously lists the year of the meeting as "2018" instead of "2019."
[7] Appendix D contains notes from these focus group meetings, which were conducted as part of a "World Café" pilot project in collaboration with the Council on American-Islamic Relations, Entre Hermanos, Byrd Barr Place, and Friends of Little Saigon. Notes from Entre Hermanos are in Spanish; Executive staff are reviewing options to translate these notes into English.

adequate mitigation for the potential privacy and civil liberty concerns raised by the Working Group. Table 7 summarizes CTO's response to each of the Working Group's concerns.

Table 7. CTO Response to Privacy and Civil Liberties Impact Assessment of SPD's CopLogic Technology

Working Group Concern	CTO Response
1. Lack of specific data retention policies	SPD has adequately addressed the policies and practices in place regarding data retention for the information collected through CopLogic.
2. Civil liberties concerns about the retail track	Validation of retail owner reports through the investigative process mitigates the potential for bias or civil liberties infringement through raw information provided by residents into CopLogic
3. Lack of prohibition about LexisNexis data retention and third-party sharing	Data use policies and limitations to data access is detailed in the SIR

Recommended Policies. The Impact Assessment recommends that Council ensure that SPD adopt "clear and enforceable policies that ensure, at a minimum, the following:

1. CopLogic data may be used only for purposes of allowing community members to file police reports or investigating and, as appropriate, prosecuting crimes.
2. The contract between the City of Seattle and LexisNexis must include the following minimum provisions:
    a. LexisNexis may not use CopLogic data for any purpose other than providing the CopLogic tool to the City of Seattle and interfacing it with Mark43[8].
    b. LexisNexis must immediately delete all CopLogic data after that data has been transferred to SPD's records management system (RMS). LexisNexis must delete all CopLogic data within 30 days of its creation regardless of whether such a transfer has taken place.
    c. LexisNexis must not share CopLogic data with any third party.
    d. LexisNexis and any third party that has access to CopLogic data must be held to the same purpose and use restrictions as SPD.
3. The retail track of CopLogic must be discontinued. Retailers should still be allowed to access and use CopLogic to provide information as any other member of the public would."

Table 8 describes how the SIR as drafted would address these recommendations. Areas not fully addressed are included in the "Policy Considerations" section.

[8] "Mark43" appears to refer to SPD's records management system.

Table 8. Working Group Recommendations Addressed in the SIR

Working Group Recommendation	Whether/How Addressed in SIR
1. CopLogic data may be used only for purposes of allowing community members to file police reports or investigating and, as appropriate, prosecuting crimes.	The SIR allows for use by individuals to report a low-level crime and by retailers to report retail theft. *See "Policy Considerations"*
2. Add restrictions pertaining to the purpose and use, retention and sharing of CopLogic data to the City's contract with LexisNexis; data sharing with third parties must be held to the same purpose and use restrictions as SPD.	**4.8** There are no data sharing agreements between SPD and any other entities for CopLogic data. The contract between the City and LexisNexis provides that LexisNexis may only "use, transmit, distribute, modify, reproduce, display, and store the City Data solely for the purposes of (i) providing the Services as contemplated in [its contract with the City]; and (ii) enforcing its rights under [the contract]." *See "Policy Considerations"*
3. Discontinue the "retail track" of CopLogic.	The SIR allows for use by individuals to report a low-level crime and by retailers to report retail theft. *See "Policy Considerations"*

Policy Considerations

Central Staff has identified the following potential policy considerations relative to the Working Group's key concerns and recommendations:

1. Discontinue retail theft reporting component of CopLogic. If Council wishes to discontinue the retail theft reporting component of CopLogic, the SIR and Executive Overview would need to be amended.
2. Restrictions on use. SPD's policies do not concisely specify the allowable uses of CopLogic and its data and currently allow for retailers to report retail theft. If Council wishes to discontinue the retail theft reporting component of CopLogic, the SIR and Executive Overview would need to be amended. Council could then adopt an amended Executive Overview of the SIR which identifies specific language as constituting the enforceable policies and procedures applicable to a more restricted use of the CopLogic technology.
3. Lexis-Nexis Contract Provisions. The SIR does not have an explicit policy that third parties with whom SPD shares data must comply with the same privacy provisions as SPD. Council may wish to direct SPD to incorporate this requirement and other restrictions pertaining to the purpose and use, retention and sharing of CopLogic data requirement into its written agreements, where feasible.
4. Annual equity assessment metrics. SPD has not finalized metrics to be used in evaluating the CopLogic Technology as part of the CTO's annual equity assessments. These assessments are intended to play a key role in determining whether the City's surveillance legislation is meeting the goals of the Race and Social Justice Initiative. Council may wish to request a report on the proposed metrics by a date certain and/or Council may wish to defer approval of this SIR, pending completion of these metrics.

5. 911 Logging Recorder

CB 120004 would approve SPD's continued use of and accept the SIR for software that records all telephone calls to SPD's 911 communications center and to the police non-emergency phone line, as well as police radio traffic. Authorized personnel also use this technology to retrieve recordings for law enforcement or public disclosure purposes. The audio recordings are routinely used in criminal prosecutions and within the 911 Center for training and quality control purposes and some information from the recordings may be stored for future reference in emergency situations. Use of the technology for any other purpose is subject to SPD disciplinary action. SPD Policy requires deletion of audio recordings not requested within 90 days of their capture.[1] SPD downloads and maintains recordings requested for law enforcement and public disclosure for the retention period related to the incident type.

Civil Liberties and Potential Disparate Impacts on Historically Marginalized Communities

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit (RET) to inform the SIR public engagement process and to highlight and mitigate impacts on racial equity from the use of the technology. The RET for the 911 Logging Recorder identifies potential civil liberties impacts from disclosure of personally identifiable information gathered during 911 calls. The SIR states that SPD mitigates the risk of unintentional release of privacy data through data security processes and by requiring state ACCESS certification (A Central Computerized Enforcement Service System) and federal CJIS (Criminal Justice Information Services) certification for all CAD users.

The SIR also identifies data sharing, storage and retention as having the potential to contribute to structural racism, thereby creating a disparate impact on historically targeted communities.[2] The SIR states that SPD mitigates this risk through policies regarding the dissemination of data in connection with criminal prosecutions, the Washington Public Records Act, and other authorized researchers. In addition, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures. The RET reports that SPD had not yet finalized the metrics to be used as part of the CTO's annual equity assessments.[3]

---

[1] LE06-01-03 Rev 1 in Washington State Law Enforcement Records Retention Schedule establishes a 90-day retention period for recordings of radio transmissions between law enforcement and dispatch staff regarding requests for resources, status changes and/or incident-related activity. This also matches the retention requirements for Emergency Communications (911) Records Retention.

[2] Historical community or department practices could – could produce data in a CAD system that would portray certain communities as higher in crime than in other neighborhoods or elevate the involvement in potential criminal events by certain demographic groups. An approach to storage, retention, and integration of these data that was not cognizant of these possibilities might allow for the continuation of these perceptions, with potential disparate enforcement responses.

[3] SMC 14.18.050B requires that the CTO produce and submit to the City Council a Surveillance Technology Community Equity Impact Assessment and Policy Guidance Report that addresses whether Chapter 14.18 of the SMC is effectively meeting the goals of the Race and Social Justice Initiative, any recommended adjustments to laws and policies to achieve a more equitable outcome, and any new approaches and considerations for the SIRs.

Public Engagement

The Executive accepted public comments on this technology from February 5 – March 5, 2019 and conducted one public meeting for multiple SIRs on February 27, 2019.[4] In addition, the Department of Neighborhoods conducted four focus groups in partnership with four organizations serving communities of color and other marginalized communities.[5] The SIR includes all notes from the focus groups (Appendix D); comments pertaining solely to these technologies received from members of the public (Appendix E), and letters from organizations or commissions (Appendix G). The Executive received very few comments on this technology. Two of the three public comments specific to the 911 Logging Recorder were supportive of the technology, the third raised several technical issues, including challenges that could be presented by Voice over Internet protocols. Other concerns included data use, retention and sharing.

Privacy and Civil Liberties Impact Assessment – 911 Logging Recorder

The Impact Assessment identifies three concerns about the use of SPD's 911 Logging Recorder and recommends that Council adopt four specific policies. The concerns include restrictions on the purpose and use of the technology, as well as data retention and data sharing. The following sections summarize the CTO's Response to the concerns and describe whether and how the SIR as drafted would address the Working Group's recommended policies.

In his response to the Privacy and Civil Liberties Impact Assessment, the City's CTO found that that SPD's policy, training and limitations from the technology itself outlined in the SIR provide adequate mitigation for the potential privacy and civil liberty concerns raised by the Working Group. Table 9 summarizes CTO's response to each of the Working Group's concerns.

Table 9. CTO Response to Privacy and Civil Liberties Impact Assessment of SPD's 911 Logging Recorder Technology

Working Group Concern	CTO Response
1. Lack of clear policy defining the purpose and allowable uses of the Logging Recorder Data.	The responses in the appropriate sections of the SIR provide clear and detailed information about the laws and policies regarding the use and access to this system.
2. Justification for the 90-day data retention period for Logging Recorder data.	This period of time provides adequate time for any investigation, review, audit or litigation that may occur regarding the recordings.

[4] The February 27, 2019 City Surveillance Technology Fair solicited comments on three Seattle Police Department Technologies: 911 Call Logging Recorder, Computer-Aided Dispatch, and CopLogic; Seattle Fire Department's Computer-Aided Dispatch technology; Seattle City Light's Current Diversion Technologies; and Seattle Department of Transportation's Acyclica travel time measurement technology. The Fair flyer in the SIR erroneously lists the year of the meeting as "2018" instead of "2019."

[5] Appendix D contains notes from these focus group meetings, which were conducted as part of a "World Café" pilot project in collaboration with the Council on American-Islamic Relations, Entre Hermanos, Byrd Barr Place, and Friends of Little Saigon. Notes from Entre Hermanos are in Spanish; Executive staff are reviewing options to translate these notes into English.

3. Lack of clarity about third-party data sharing content and purpose or justification.	SPD provides clear and adequate details about third party agencies with whom the 911 logging recording data is shared and for what purposes. Specification and compliance to the agreements between departments and agencies are provided in the SIR, including information about the Washington Public Records Act and possible redaction or exemptions.

Recommended Policies. The Impact Assessment recommends that Council ensure that SPD adopt "clear and enforceable policies that ensure, at a minimum, the following:

1. The purpose and allowable uses of the Logging Recorder data must be clearly defined, and both SPD and NICE (the vendor of the technology) must be restricted to those uses.
2. NICE must delete all Logging Recorder data after seven days.
3. There must be a clear designation of what data collected by the Logging Recorder is shared with third parties and for what purposes.
4. NICE or any other third party that has access to Logging Recorder data must be held to the same restrictions as SPD, including industry best practice security standards."

Table 10 describes how the SIR as drafted would address these recommendations. Areas not fully addressed are included in the "Policy Considerations" section.

Table 10. Working Group Recommendations Addressed in the SIR

Working Group Recommendation	Whether/How Addressed in SIR
1. Purpose and use of the Logging Recorder data must be defined and both SPD and NICE (the vendor) must be restricted to those uses.	**Executive Overview.** Operational Policies represent the only allowable uses of the equipment and data collected by this technology. Note: the Executive Overview is not adopted by CB 120004. *See "Policy Considerations"*
2. NICE (the vendor) must delete all Logging Recorder data after seven days	**4.2** Audio recordings that have not been requested within 90 days of their capture are deleted. Recordings requested for law enforcement and public disclosure are downloaded and maintained for the retention period related to the incident type.
3. Clearly designate third-party data sharing and for what purposes	**6.1** Identifies data sharing with other agencies, entities or individuals within legal guidelines or as required by law.
4. NICE or any other third party that has access to Logging Recorder data must be held to the same restrictions as SPD, including industry best practice security standards	**6.1** Data obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law. *See "Policy Considerations"*

Policy Considerations

Central Staff has identified the following potential policy considerations relative to the Working Group's key concerns and recommendations:

1. Restrictions on use - SPD. SPD's policies do not concisely specify the allowable uses of the Automated License Plate Reader technology. Council may wish to amend the proposed Council Bill to also adopt the Executive Overview of the SIR which identifies specific language as constituting the enforceable policies and procedures applicable to the technology.
2. Restrictions on use – NICE. The SIR does not have an explicit policy that third parties with whom SPD shares data must comply with the same privacy provisions as SPD. Council may wish to direct SPD to incorporate this requirement into its contract with NICE or other third parties who have access to Logging Recorder data, where feasible.
3. Annual Equity Assessment Metrics. SPD has not finalized metrics to be used in evaluating the 911 Logging Recorder Technology as part of the CTO's annual equity assessments. These assessments are intended to play a key role in determining whether the City's surveillance legislation is meeting the goals of the Race and Social Justice Initiative. Council may wish to request a report on the proposed metrics by a date certain and/or Council may wish to defer approval of this SIR, pending completion of these metrics.

Attachments:

1. Background Summary and Surveillance Impact Report Process

cc: Dan Eder, Interim Director
Aly Pennucci, Budget and Policy Manager

Attachment 1 - Background Summary and Surveillance Impact Report Process

Recent Legislative History

Ordinance 125376, passed by Council on July 31, 2017, required City of Seattle departments intending to acquire surveillance technology to obtain advance Council approval, by ordinance, of the acquisition and of a surveillance impact report (SIR).[1] Departments must also submit a SIR for surveillance technology in use when Ordinance 125376 was adopted (referred to in the ordinance as "retroactive technologies"). The Executive originally included 28 "retroactive technologies," on its November 30, 2017 Master List but revised that list to 26 in December 2019. The Council has approved two SIRs and twice extended the initial March 3, 2020 deadline for completion of SIRs for all 26 technologies: first by six months to accommodate extended deliberation of the first two SIRS; and then by a second six months due to COVID-related delays. Either the Chief Technology Officer or the Council may determine whether a specific technology is "surveillance technology" and thus subject to the requirements of SMC 14.18. Each SIR must describe protocols for a "use and data management policy" as follows:

- How and when the surveillance technology will be deployed or used and by whom, including specific rules of use
- How surveillance data will be securely stored
- How surveillance data will be retained and deleted
- How surveillance data will be accessed
- Whether a department intends to share access to the technology or data with any other entity
- How the department will ensure that personnel who operate the technology and/or access its data can ensure compliance with the use and data management policy
- Any community engagement events and plans
- How the potential impact of the surveillance on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities have been taken into account; and a mitigation plan
- The fiscal impact of the surveillance technology

Community Surveillance Working Group

On October 5, 2018, Council passed Ordinance 125679, amending SMC 14.18, creating a "community surveillance working group" charged with creating a Privacy and Civil Liberties Impact Assessment for each SIR.[2] At least five of the seven members of the Working Group

[1] As codified in SMC 14.18.030, Ordinance 125376 identified a number of exemptions and exceptions to the required Council approval, including information voluntarily provided, body-worn cameras and cameras installed in or on a police vehicle, cameras that record traffic violations, security cameras and technology that monitors City employees at work.

[2] Ordinance 125679 also established a March 31, 2020 deadline for submitting SIRs on technologies already in use (referred to as "retroactive technologies") when Ordinance 125376 was passed, with provision to request a six-month extension.

must represent groups that have historically been subject to disproportionate surveillance, including Seattle's diverse communities of color, immigrant communities, religious minorities, and groups concerned with privacy and protest.[3] Each Privacy and Civil Liberties Impact Assessment must describe the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities and will be included in the SIR. Prior to submittal of a SIR to Council, the Chief Technology Officer may provide a written statement that addresses privacy rights, civil liberty or other concerns in the Working Group's impact assessment.

Executive Overviews

In May 2019, members of the Governance, Equity, and Technology Committee requested that IT staff prepare a summary section for each of the two lengthy SIR documents under review at that time. The Committee then accepted the resultant "Condensed Surveillance Impact Reports (CSIRs) together with the complete SIRs. The Executive has continued this practice with subsequent SIRs but has renamed the documents "Executive Overviews." The Operational Policy Statements in the Executive Overview represent the only allowable uses of the subject technology.

SIR Process

Chart 1 is a visual of the SIR process from inception to Council Review:

Chart 1. Surveillance Impact Report (SIR) Process

Department drafts SIR about technology use, privacy, and data security.	Draft SIR made public. One or more public meetings scheduled to solicit feedback.	Working Group reviews SIR; creates Impact Assessment, documenting privacy and civil liberty concerns.	City's Chief Technology Officer addresses any Working Group concerns.	Council reviews Executive's proposed ordinance reflecting the SIR, authorizing the use of existing or new technology.

[3] The Mayor appoints four members and Council appoints three members.

Group 2 Surveillance Impact Report (SIR) Legislation

Transportation & Utilities Committee

March 3, 2021

Presentation by Seattle IT Privacy Office

City of Seattle

Surveillance Impact Report (SIR) Overview

- 2017: Ordinance 125376 took effect Sept 4th, revising the law to address the intended use of technologies with potential to impact civil liberties
- 2017: City identifies 29 technologies in use by 4 departments, later reduced to 26 technologies
- 2018: Ordinance amended to add an external Surveillance Advisory Working group
- 9/23/2019: Group 1 SIR legislation approved by Council (Ordinance 125936)
- 2020: Deadline extension from 9/1/2020 to 3/1/2021 due to COVID-19 delays
- **1/20/2021: Presented Overview of Surveillance Ordinance at the Transportation and Utilities Committee**
- **1/26/2021: Group 2 SIR legislation transmitted to Council**
- **2/22/2021: Group 3 SIR legislation transmitted to City Clerk**

Surveillance Criteria

Definition: *Technology whose primary purpose is to observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice. Identifiable individuals also include individuals whose identity can be revealed by license plate data when combined with any other record.*

Exclusions

- Consents to provide the data
- Opt-out notice
- Body-worn cameras
- Police vehicle cameras
- Cameras installed pursuant to state law…or to record traffic violations
- Security cameras
- City infrastructure protection cameras
- Technology that monitors only City employees

Inclusions

- Disparately impacts disadvantaged groups
- PII shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service
- Collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection
- Raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice

Surveillance Impact Report (SIR) Process

- Submitted for all retroactive and newly proposed technologies that meet the definition and have no exclusion criteria
- Created by the Departments with project management from IT

1. Privacy Impact Assessment
2. Financial Information
3. Racial Equity Toolkit
4. Public Engagement Comments and Analysis
5. Privacy and Civil Liberties Impact Assessment
6. CTO Response
7. Appendices & Supporting Documentation

General SIR Creation Timeline

1) Draft & Review SIRs	2) Public Comment Period	3) Public Comment Analysis	4) Working Group Review	5) CTO Response	6) Executive Overview	7) Council Review
Staff from the department requesting the technology completes SIR content	The initial draft released for public review and comment. One or more public meetings will take place to solicit feedback.	City staff compiles public comments and finalizes the SIR content.	The Surveillance Advisory Working Group reviews each SIR, complete an Assessment included in SIR submission	The CTO responds to the Privacy and Civil Liberties Assessment.	City Staff creates condensed version of the SIR for submission to Council (formerly called the Condensed SIR – CSIR)	City Council will decide on the use of the surveillance technology, by full Council vote.

8-9 months

Group 2 Surveillance Impact Reports (CB 120002, CB 120003, CB 120004)

1	**Binoculars / Spotting Scope (SCL)**	The spotting scope is used to read meters from a distance when direct access to the meter is obstructed.
2	**Check Meter Device (SCL)**	This device measures the total amount of power being consumed at a service location where current diversion is confirmed or suspected. The device is set at the transformer and is used when a prolonged reading is desired by the Current Diversion team.
3	**SensorLink Amp Fork (SCL)**	The SensorLink Amp Fork is used by SCL's Current Diversion team to measure the load online-side entrance conductors, allowing SCL to determine the total amount of power being consumed at a service location. This tool provides an instantaneous reading to the group conducting the investigation.
4	**Computer Aided Dispatch (SFD)**	Computer-aided dispatch (CAD) is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.
5	**Computer Aided Dispatch (SPD)**	CAD is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field.
6 / 7	**Automated License Plate Reader (ALPR) for Patrol and Parking Enforcement (SPD)**	ALPRs are computer-controlled, high-speed camera systems mounted on parking enforcement or police vehicles that automatically capture an image of license plates that come into view and converts the image of the license plate into alphanumeric data that can be used to locate vehicles reported stolen or otherwise sought for public safety purposes and to enforce parking restrictions.
8	**CopLogic (SPD)**	System allowing individuals to submit police reports on-line for certain low-level crimes in non-emergency situations where there are no known suspects or information about the crime that can be followed up on. Use is opt-in, but individuals may enter personally identifying information about third-parties without providing notice to those individuals.
9	**911 Logging Recorder (SPD)**	System providing networked access to the logged telephony and radio voice recordings of the 911 center.

Group 2 SIR Public Engagement

Short 1-2 minute video overview of each technology provided on SIR website.

Binoculars / Spotting Scope (City Light)

The spotting scope is used to read meters from a distance when direct access to the meter is obstructed. Scopes are used by SCL's Current Diversion team to conduct investigations. Use of this technology may occur without informing a domicile's resident(s).

View Summary Watch Review View Full Report

Check Meter Device (City Light)

This device measures the total amount of power being consumed at a service location where current diversion is confirmed or suspected. The device is set at the transformer and is used when a prolonged reading is desired by the Current Diversion team. Use of this technology may occur without informing a domicile's resident(s).

View Summary Watch Review View Full Report

SensorLink AmpFork (City Light)

The SensorLink Amp Fork is used by SCL's Current Diversion team to measure the load on line-side entrance conductors, allowing SCL to determine the total amount of power being consumed at a service location. This too provides an instantaneous reading to the group conducting the investigation. Use of this technology may occur without informing a domicile's resident(s).

View Summary Watch Review View Full Report

Computer Aided Dispatch (CAD) (Fire)

Computer-aided dispatch (CAD) is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.

View Summary Watch Review View Full Report

Computer Aided Dispatch (CAD) (Police)

CAD is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field.

View Summary Watch Review View Full Report

Automated License Plate Readers (Police)

ALPRs are computer-controlled, high-speed camera systems mounted on parking enforcement or police vehicles tha automatically capture an image of license plates that come into view and converts the image of the license plate into alphanumeric data that can be used to locate vehicles reported stolen or otherwise sought for public safety purpose and to enforce parking restrictions.

View Summary Watch Review View Full Report View Policy Appendix

CopLogic (Police)

System allowing individuals to submit police reports on-line for certain low-level crimes in non-emergency situatio where there are no known suspects or information about the crime that can be followed up on. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.

View Summary Watch Review View Full Report

911 Logging Recorder (Police)

System providing networked access to the logged telephony and radio voice recordings of the 911 cente

View Summary Watch Review View Full Report

Group 2 SIR Public Engagement

- February 5th – March 26th, 2019
- Technology Fair Style Event
- Recorded presentations and posted online
- Produced 2-minute video overviews of technologies

Engagement Method	(Approximate) Number of Individuals Participating	Number of Comments Received	Number of Questions Received
Focus Groups	18	12	13
Public Meeting	19	1	0
Online Comments	16	16	29
Letter	4	4	0
Email	2	2	0
Total	59	35	42

SEATTLE CITY COUNCIL
CENTRAL STAFF

Group 2 Surveillance Impact Reports

LISE KAYE, COUNCIL CENTRAL STAFF

TRANSPORTATION AND UTILITIES COMMITTEE| MARCH 3, 2021

Proposed Council Bills

I. Bills would approve the continuing use of specific surveillance technologies and accept Surveillance Impact Reports (SIRs) on those technologies

   a. CB 120002: Seattle City Light Current Diversion (3 SIRs)

   b. CB 120003: Seattle Fire Dept Computer-Aided Dispatch (1 SIR)

   c. CB 120004: Seattle Police Department (5 SIRs)

II. Committee Options

   a. Pass CB 120002, 120003 and/or 120004 as transmitted;

   b. Request Central Staff to prepare amendments to the Council Bill and/or to one or more of the SIRs to address additional concerns or issues; or

   c. Take no action

Proposed Council Bills – Today's Agenda

I. Introduction

II. Executive Overview

III. CB 120002: Seattle City Light Current Diversion (3 SIRs)

   a. Central Staff Summary
   b. Council Q&A

IV. CB 120003: Seattle Fire Dept Computer-Aided Dispatch (1 SIR)

   a. Central Staff Summary
   b. Council Q&A

V. CB 120004: Seattle Police Department (5 SIRs)

   a. Central Staff Summary
   b. Council Q&A

Elements to Consider

1. Purpose and Use of Each Technology
2. Civil Liberties and Potential Disparate Impacts on Historically Marginalized Communities (Racial Equity Toolkit)
3. Public Engagement
4. Privacy and Civil Liberties Impact Assessment
5. Chief Technology Officer's Response

Elements to Consider

- Policy Considerations
  - Primarily areas where Working Group's recommendations go beyond the mitigations described in the SIRs – not intended as staff recommendations
  - Incomplete information in a SIR
  - Legal and logistical parameters around addressing Working Group concerns (e.g. holding third-parties to City privacy standards; state mandated data retention schedules)

CB 120002: Seattle City Light Current Diversion technologies – 3 SIRs

Used to investigate potential electricity theft

- Binoculars/Spotting Scope
- Check Meter Device
- SensorLink AmpFork

SCL Current Diversion Technologies

- Civil Liberties and Potential Disparate Impacts
  - None anticipated
  - Equity analysis of past enforcement locations – not yet complete
  - Metrics for CTO's annual equity assessments – not identified
- Public comments: some support; concerns about outdated technology and invasion of privacy

SCL Current Diversion Technologies

- Impact Assessment issues:
  - Allowable uses
  - Data protection
  - Data retention
- CTO's Response: SCL's policy and training and limitations of the technologies provide adequate mitigation for Working Group concerns

SCL Current Diversion Technologies

- Policy Considerations
  - Restrictions on use
  - Annual equity assessment metrics
  - Title of Binoculars/Spotting Scope SIR

CB 120003: Seattle Fire Department Computer-Aided Dispatch – 1 SIR

Supports personnel who dispatch Fire and Emergency Medical Services units in emergency situations.

SFD Computer-Aided Dispatch

- Civil Liberties and Potential Disparate Impacts
  - Potential disclosure of personally identifiable information
  - Sensitive information could be used by law enforcement to target of members of historically marginalized communities or track locations and history of service requests
  - Metrics for CTO's annual equity assessments – not identified
- Public comments: some support; concerns about outdated technology and invasion of privacy

SFD Computer-Aided Dispatch

- Impact Assessment issues:
  - Allowable uses
  - Data accessibility, retention and sharing
  - Operators trained to policies
  - Continuity of contractual terms and privacy policies through merger
- CTO's Response: SFD's policy and training and limitations of the technologies provide adequate mitigation for Working Group concerns

SFD Computer-Aided Dispatch

- Policy Considerations
  - Restrictions on use
  - Data retention
  - Third-party data sharing
  - Annual equity assessment metrics

CB 120004: Seattle Police Department surveillance technologies – 5 SIRs

- Automated License Plate Readers
- Parking Enforcement System
- Computer-Aided Dispatch
- CopLogic
- 911 Logging Recorder

CB 120004: Automated License Plate Readers

Assist in identification of stolen vehicles, and vehicles wanted in conjunction with felonies or associated with wanted persons or Amber and Silver Alerts (abducted children and missing people).

* SIR updated in January 2019, with new policies effective February 1, 2019

SPD Automated License Plate Readers

- Civil Liberties and Potential Disparate Impacts
  - Could be used to identify individuals without reasonable suspicion of having committed a crime
  - Could be used to search for information that is not incidental to any active investigation
  - Could over-surveil vulnerable or historically targeted communities
- Public comments: support, concerns about data retention, security, privacy, potential for error or misuse, surveillance in general

SPD Automated License Plate Readers

- Impact Assessment issues:
  - Allowable use of data
  - Data access, collection, retention and sharing,
  - System audits,
  - Role/effectiveness of this technology in solving crimes
- CTO's Response: SPD's updated policies and training and limitations of the technologies provide adequate mitigation for Working Group concerns

SPD Automated License Plate Readers

- Policy Considerations
  - Restrictions on use

CB 120004: Parking Enforcement Systems

Enforce parking laws, such as vehicle impoundment for unpaid fines, time-restricted parking areas, and restricted parking zones. Identify stolen vehicles or those sought in connection with a criminal investigation using specialized license plate reader software.

* SIR updated in January 2019, with new policies effective February 1, 2019

SPD Parking Enforcement Systems

- Civil Liberties and Potential Disparate Impacts
  - Could be used to identify individuals without reasonable suspicion of having committed a crime
  - Could be used to search for information that is not incidental to any active investigation
  - Could over-surveil vulnerable or historically targeted communities
- Public comments: some support, concerns included data retention, equitable enforcement and surveillance in general

SPD Parking Enforcement Systems

- Impact Assessment issues:
  - Allowable use of data
  - Data access, collection, retention and third-party sharing,
  - Data sharing between Patrol and Parking Enforcement
  - System audits; financial and operational records, including use by neighborhood and demographic
  - Role/effectiveness of this technology in solving crimes
- CTO's Response: SPD's updated policies and training and limitations of the technologies provide adequate mitigation for Working Group concerns

SPD Parking Enforcement Systems

- Policy Considerations
  - Restrictions on use
  - Data Sharing between Patrol and Parking Enforcement
  - Equitable Enforcement
  - Genetec Patroller Software as “non-surveillance” technology

CB 120004: Computer-Aided Dispatch

Supports personnel who dispatch SPD Patrol units in emergency situations.

SPD Computer-Aided Dispatch

- Civil Liberties and Potential Disparate Impacts
  - Potential disclosure of personally identifiable information
  - Potential to contribute to structural racism through data sharing, storage and retention, thereby creating a disparate impact on historically targeted communities
  - Metrics for CTO's annual equity assessments – not identified
- Public comments: some support; concerns included data security

SPD Computer-Aided Dispatch

- Impact Assessment issues:
  - Allowable use of data
  - Data access
  - Data retention
  - Operators trained to policies
- CTO's Response: SIR provided information specific to each concern

SPD Computer-Aided Dispatch

- Policy Considerations
  - Restrictions on use
  - Annual equity assessment metrics

CB 120004: CopLogic

Crime-reporting software with two applications:

1) Individual reporting of low-level crimes
2) Retail theft reporting

SPD CopLogic

- Civil Liberties and Potential Disparate Impacts
  - Information could be disseminated in ways that could negatively impact peoples' civil liberties
  - Racial or ethnicity-based information may be entered into the system
  - Potential to contribute to structural racism through data sharing, storage and retention, thereby creating a disparate impact on historically targeted communities
  - Metrics for CTO's annual equity assessments – not identified

SPD CopLogic

- Public comments:
  - Some support
  - Request for technology to be available in languages other than English
  - Concerns about: uneven access to the programs, potential for racial bias in reports and for inaccurate reports, unfair treatment of suspects, data collection, retention and sharing

SPD CopLogic

- Impact Assessment issues:
  - Allowable use of data
  - Data retention
  - Civil liberty impacts of the retail theft program; recommend discontinuing the program
  - Third-party data sharing
- CTO's Response: SPD's policies and training and limitations of the technologies provide adequate mitigation for Working Group concerns

SPD CopLogic

- Policy Considerations
  - Retail theft reporting component of CopLogic
  - Lexis-Nexis contract provisions: purpose and use restrictions, data retention, data sharing
  - Annual equity assessment metrics

CB 120004: 911 Logging Recorder

Automatically records all telephone calls received by the Seattle Police Department's 9-1-1 Center as well as all radio traffic between dispatchers and SPD patrol officers.

SPD 911 Logging Recorder

- Civil Liberties and Potential Disparate Impacts
  - Potential disclosure of personally identifiable information
  - Potential to contribute to structural racism through data sharing, storage and retention, thereby creating a disparate impact on historically targeted communities
  - Metrics for CTO's annual equity assessments – not identified
- Public comments: some support; concerns included data use, retention and sharing

SPD 911 Logging Recorder

- Impact Assessment issues:
  - Allowable use of data
  - Data retention and sharing
  - Data retention
  - Vendor and third-party contract provisions
- CTO's Response: SIR provided information specific to each concern

SPD 911 Logging Recorder

- Policy Considerations
  - Restrictions on use (internal to City)
  - Third-party restrictions on use
  - Annual equity assessment metrics – not included