

**CITY OF SEATTLE**

**ORDINANCE 126311**

**COUNCIL BILL 120024**

AN ORDINANCE relating to surveillance technology implementation; authorizing approval of uses and accepting the surveillance impact report for the Seattle Police Department’s use of 911 Logging Recorder technology.

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 technology in use by the Seattle Police Department (SPD); and

WHEREAS, SPD conducted policy rule review and community review as part of the development of the SIR; and

WHEREAS, Seattle Municipal Code Section 14.18.080, enacted by Ordinance 125679, also requires review of the SIR 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 SIR and review by the Working Group have been completed; and

WHEREAS, Ordinance 126233 created a new Community Safety and Communications Center to include, effective the earlier of June 1, 2021 or 30 days after the Executive receives the Originating Agency Identifier (ORI), the 9-1-1 dispatch center currently housed within SPD and the SIR will need to be updated to reflect the new organizational structure;

NOW, THEREFORE,

1 **BE IT ORDAINED BY THE CITY OF SEATTLE AS FOLLOWS:**

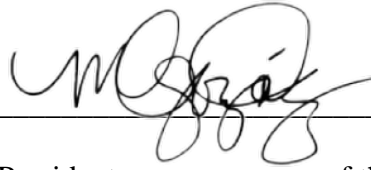
2           Section 1. Pursuant to Ordinances 125376 and 125679, the City Council approves use of  
3 the 911 Logging Recorder technology and accepts the Surveillance Impact Report (SIR), for this  
4 technology, attached to this ordinance as Attachment 1 and the Executive Overview, for the same  
5 technology, attached to this ordinance as Attachment 2.

6

1 Section 2. The Council requests the Seattle Police Department to report no later than the  
2 end of the third quarter of 2021 on the metrics provided to the Chief Technology Officer for use  
3 in the annual equity assessments of the 911 Logging Recorder technology.

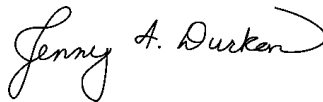
4 Section 3. This ordinance shall take effect and be in force 30 days after its approval by  
5 the Mayor, but if not approved and returned by the Mayor within ten days after presentation, it  
6 shall take effect as provided by Seattle Municipal Code Section 1.04.020.

7 Passed by the City Council the 19th day of April, 2021,  
8 and signed by me in open session in authentication of its passage this 19th day of  
9 April, 2021.

10 

11 President \_\_\_\_\_ of the City Council

12  Approved /  returned unsigned /  vetoed this 23rd day of April, 2021.

13 

14 Jenny A. Durkan, Mayor

15 Filed by me this 23rd day of April, 2021.

16 

17 Monica Martinez Simmons, City Clerk

18 (Seal)

- 1 Attachments:
- 2 Attachment 1 – 911 Logging Recorder SIR
- 3 Attachment 2 – 911 Logging Recorder Executive Overview

2019 Surveillance Impact Report

# 911 Logging Recorder

Seattle Police Department

# Table of Contents

<b>Submitting Department Memo .....</b>	<b>3</b>
<b>Surveillance Impact Report (“SIR”) overview .....</b>	<b>5</b>
<b>Privacy Impact Assessment .....</b>	<b>6</b>
<b>Financial Information.....</b>	<b>24</b>
<b>Expertise and References.....</b>	<b>26</b>
<b>Racial Equity Toolkit (“RET”) and Engagement for Public Comment Worksheet</b>	<b>27</b>
<b>Privacy and Civil Liberties Assessment .....</b>	<b>38</b>
<b>CTO Response.....</b>	<b>42</b>
<b>Appendix A: Glossary .....</b>	<b>50</b>
<b>Appendix B: Meeting Notice(s) .....</b>	<b>52</b>
<b>Appendix C: Meeting Sign-in Sheet(s) .....</b>	<b>60</b>
<b>Appendix D: Department of Neighborhood Focus Group Notes .....</b>	<b>85</b>
<b>Appendix E: All Comments Received from Members of the Public .....</b>	<b>136</b>
<b>Appendix F: Department Responses to Public Inquiries .....</b>	<b>140</b>
<b>Appendix G: Letters from Organizations or Commissions.....</b>	<b>141</b>
<b>Appendix H: Comment Analysis Methodology .....</b>	<b>165</b>
<b>Appendix I: Supporting Policy Documentation .....</b>	<b>168</b>
<b>Appendix J: CTO Notification of Surveillance Technology.....</b>	<b>185</b>

## Submitting Department Memo

# Memo

**Date:** April 29, 2019

**To:** City Council

**From:** Deputy Chief Garth Green, 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.



# 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”.

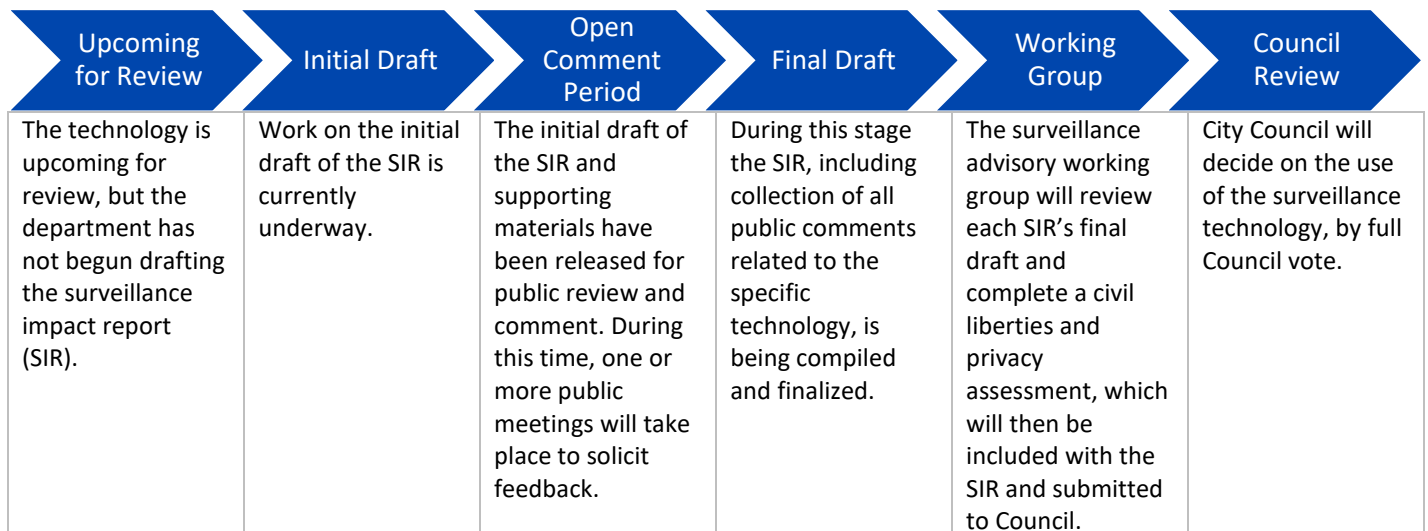
## How this Document is Completed

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.



# 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](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. Secondly, 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) 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 FBI's 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 FBI's 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 FBI's 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 FBI's 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 CJIS or systems with access to CJIS). The system shall automatically lock the account/node for a 10 minute time period unless released by an administrator.

- When CJJ 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 CJJ.
- When CJJ 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 CJJ 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 CJJ 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 CJJ.

## 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

# 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 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

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

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?

The 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.

#### 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.”<sup>1</sup> 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 (JAACL)
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 <a href="http://seattle.gov/privacy">seattle.gov/privacy</a> . 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.

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

## 2.4 Scheduled Focus Group Meeting(s)

### Meeting 1

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

### Meeting 2

<b>Community Engaged</b>	Entre Hermanos
<b>Date</b>	Thursday, February 28, 2019

### Meeting 3

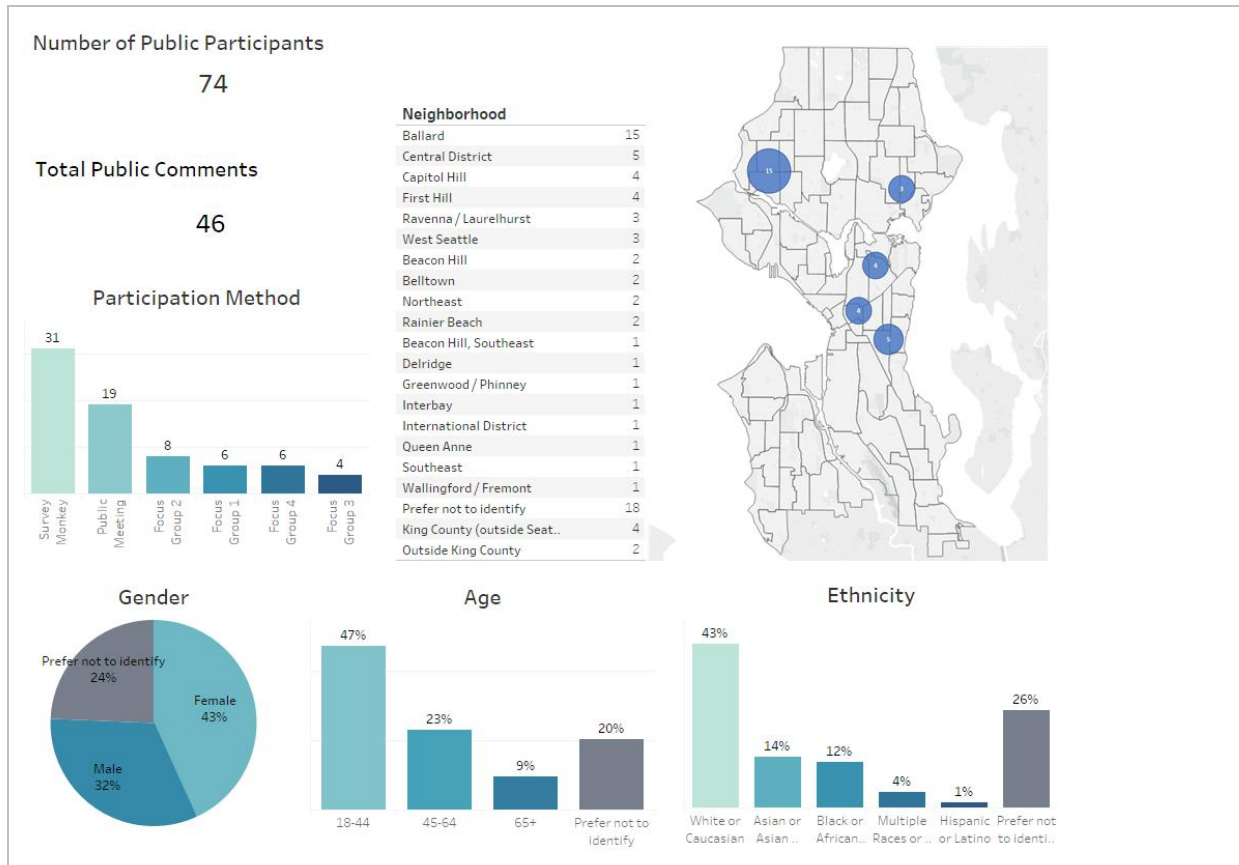
<b>Community Engaged</b>	Byrd Barr Place
<b>Date</b>	Thursday, February 28, 2019

### Meeting 4

<b>Community Engaged</b>	Friends of Little Saigon
<b>Date</b>	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 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.

## 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.<sup>1</sup>

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.”<sup>2</sup>

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<sup>3</sup> and with SPD receiving 900,000 calls per year,<sup>4</sup> 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.<sup>5</sup> 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.<sup>6</sup>
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)<sup>7</sup> states:

---

<sup>1</sup> Privacy Impact Assessment, Surveillance Impact Report, 911 Logging Recorder, SPD, page 8.

<sup>2</sup> Privacy Impact Assessment, Surveillance Impact Report, 911 Logging Recorder, SPD, page 16.

<sup>3</sup> Submitting Department Memo, Surveillance Impact Report, 911 Logging Recorder, SPD, page 3-4.

<sup>4</sup> <https://www.seattle.gov/police/about-us/about-policing/9-1-1-center>

<sup>5</sup> Appendix G: Letters from Organizations or Commissions, Surveillance Impact Report, 911 Logging Recorder, page 114.

<sup>6</sup> Privacy Impact Assessment, Surveillance Impact Report, 911 Logging Recorder, SPD, page 7.

<sup>7</sup> 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.**<sup>8</sup> A severe vulnerability discovered in 2014 allowed unauthorized users full access to a NICE customer’s databases and audio recordings.<sup>9</sup> Again, in 2017, a NICE-owned server was set up with public permissions, exposing phone numbers, names, and PINs of 6 million Verizon customers.<sup>10</sup> 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.

---

<sup>8</sup> Appendix G: Letters from Organizations or Commissions, Surveillance Impact Report, 911 Logging Recorder, page 114.

<sup>9</sup> <https://krebsonsecurity.com/2014/05/backdoor-in-call-monitoring-surveillance-gear/>

<sup>10</sup> <https://www.techspot.com/news/70106-nice-systems-exposes-14-million-verizon-customers-open.html>

## 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. Secondly, 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 CJS 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 FBI’s 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 CJJ 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 CJJ.

## 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 Surveillance Technology Fair

February 27, 2018

6:00 p.m. – 8:00 p.m.

Bertha Knight Landes Room, 1<sup>st</sup> Floor City Hall  
600 4<sup>th</sup> 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](http://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](mailto:Surveillance@seattle.gov) if you need any accommodations. For more information, visit [Seattle.gov/privacy](http://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](http://Seattle.gov/privacy). All comments submitted will be included in the Surveillance Impact Report.





# 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](http://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](mailto:Surveillance@seattle.gov) nếu  
quý vị cần bất kỳ điều chỉnh nào. Để có thêm thông tin, hãy truy cập  
[Seattle.gov/privacy](http://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](http://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.



## 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](http://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](mailto:Surveillance@seattle.gov) kung kailangan mo ng anumang tulong. Para sa higit pang impormasyon, bumisita sa [Seattle.gov/privacy](http://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](http://Seattle.gov/privacy). Isasama ang lahat ng isinumiteng komento sa Surveillance Impact Report (Ulat sa Epekto ng Pagmamanman).



# 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](http://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](mailto:Surveillance@seattle.gov) si necesita adaptaciones especiales. Para obtener más información, visite [seattle.gov/privacy](http://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](http://Seattle.gov/privacy). Todos los comentarios enviados se incluirán en el Informe del efecto de la vigilancia.



## 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](http://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](mailto:Surveillance@seattle.gov) hadaad  
ubaahantahay hooy laguusii qabto. Wixii macluumaad dheeri ah,  
booqo [Seattle.gov/privacy](http://Seattle.gov/privacy).**

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



# 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, 1<sup>st</sup> Floor City Hall  
600 4<sup>th</sup> 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](http://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](mailto:Surveillance@seattle.gov) 联系我们。  
要获得更多信息，请访问 [Seattle.gov/privacy](http://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](http://Seattle.gov/privacy)。提交的所有意见都将包含在监控影响报告内。



# 도시 감시 기술 박람회

2019년 2월 27일

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](http://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 2019년 2월 5일 - 3월 5일입니다.

편의사항이 필요하신 경우 [Surveillance@seattle.gov](mailto:Surveillance@seattle.gov) 로 문의해 주시기 바랍니다.

자세한 정보는 [Seattle.gov/privacy](http://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](http://Seattle.gov/privacy) 를 방문하시기 바랍니다. 제출된 모든 의견은 감시 영향 보고서에 수록됩니다.



# 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](http://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](mailto:Surveillance@seattle.gov) 聯絡我們。要獲得  
更多資訊，請造訪 [Seattle.gov/privacy](http://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](http://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





**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



**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

**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

**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

**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*

**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



*Queen Anne*

**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

**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

**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

**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





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

**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

**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

**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

**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

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

**Age**

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

- Southeast
- Southwest
- South Park
- Wallingford / Fremont
- West Seattle
- King county (outside Seattle)
- Outside King County

**Gender**

- Female
- Male
- Transgender
- Prefer not to identify



Survey Sign-in Sheet

**Neighborhood**

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

**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

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

**Age**

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

- Southeast
- Southwest
- South Park
- Wallingford / Fremont
- West Seattle
- King county (outside Seattle)
- Outside King County

**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

**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

**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

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

**Age**

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

- Southeast
- Southwest
- South Park
- Wallingford / Fremont
- West Seattle
- King county (outside Seattle)
- Outside King County
- 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

SE KING COUNTY

**Age/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

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

**Age**

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

- Southeast
- Southwest
- South Park
- Wallingford / Fremont
- West Seattle
- King county (outside Seattle)
- Outside King County
- 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

**Neighborhood**

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

**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

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

**Age**

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

- Southeast
- Southwest
- South Park
- Wallingford / Fremont
- West Seattle
- King county (outside Seattle)
- Outside King County

**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

**Neighborhood**

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

**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

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

**Age**

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

- Southeast
- Southwest
- South Park
- Wallingford / Fremont
- West Seattle
- King county (outside Seattle)
- Outside King County

**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

**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

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

**Age**

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

- Southeast
- Southwest
- South Park
- Wallingford / Fremont
- West Seattle
- King county (outside Seattle)
- Outside King County

**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



## Appendix D: Department of Neighborhood Focus Group Notes

### Friends of Little Saigon (FOLS)

Please select which technology you wish to comment on:

<input type="checkbox"/> SCL: Binoculars	<input type="checkbox"/> SCL: Sensorlink Transformer Meter (TMS)	<input type="checkbox"/> SFD: Computer-Aided Dispatch	<input type="checkbox"/> SPD:9-11 Call Recorder
<input type="checkbox"/> SCL: Sensorlink Ampstik	<input type="checkbox"/> SDOT: Acyclica	<input type="checkbox"/> SPD: Computer-Aided Dispatch	<input checked="" type="checkbox"/> 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:

<input type="checkbox"/> SCL: Binoculars	<input type="checkbox"/> SCL: Sensorlink Transformer Meter (TMS)	<input type="checkbox"/> SFD: Computer-Aided Dispatch	<input checked="" type="checkbox"/> SPD:9-11 Call Recorder
<input type="checkbox"/> SCL: Sensorlink Ampstik	<input type="checkbox"/> SDOT: Acyclica	<input checked="" type="checkbox"/> SPD: Computer-Aided Dispatch	<input type="checkbox"/> 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 it seems like it presents more cons than pros, and what is the 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 holes in the system. Is this a right wing Donald trump agenda to watch neighbors of color and surveillance
  - I think I'm 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 out 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 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 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 way 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

## Entre Hermanos

Please select which technology you wish to comment on:

<input type="checkbox"/> SCL: Binoculars	<input type="checkbox"/> SCL: Sensorlink Transformer Meter (TMS)	<input type="checkbox"/> SFD: Computer-Aided Dispatch	<input type="checkbox"/> SPD:9-11 Call Recorder
<input type="checkbox"/> SCL: Sensorlink Ampstik	<input checked="" type="checkbox"/> SDOT: Acyclica	<input type="checkbox"/> SPD: Computer-Aided Dispatch	<input type="checkbox"/> 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 necesidad 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:

<input checked="" type="checkbox"/> SCL: Binoculars	<input checked="" type="checkbox"/> SCL: Sensorlink Transformer Meter (TMS)	<input type="checkbox"/> SFD: Computer-Aided Dispatch	<input type="checkbox"/> SPD:9-11 Call Recorder
<input type="checkbox"/> SCL: Sensorlink Ampstik	<input type="checkbox"/> SDOT: Acyclica	<input type="checkbox"/> SPD: Computer-Aided Dispatch	<input type="checkbox"/> 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:

<input type="checkbox"/> SCL: Binoculars	<input type="checkbox"/> SCL: Sensorlink Transformer Meter (TMS)	<input type="checkbox"/> SFD: Computer-Aided Dispatch	<input type="checkbox"/> SPD:9-11 Call Recorder
<input type="checkbox"/> SCL: Sensorlink Ampstik	<input type="checkbox"/> SDOT: Acyclica	<input type="checkbox"/> SPD: Computer-Aided Dispatch	<input checked="" type="checkbox"/> 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 transcurencia 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 beneficiosa?

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 ciudad?
- ¿Qué preocupación les causa el uso que se le dará a este sistema?
- ¿Qué recomendarían a el grupo de políticos de la ciudad 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?

- Sería 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 Acrylica?

- Participante no cree que allí se ocupan.

Hablaron sobre la necesidad de puntos estratégicos y calles con más necesidad de ayuda por causa del tráfico.

**Presentador:** Crees que Acrylica 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.

**Tecnología #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 ciudad/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.

### **Tecnología #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 transcurencia 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.**

## Entre Hermanos (Translated)

Entre hermanos (Between Brothers)

**Please select which technology you wish to comment on:**

- |  |  |   |  |
|--|--|---|--|
| <input type="checkbox"/> SCL: Binoculars         | <input type="checkbox"/> SCL: Sensorlink Transformer Meter (TMS) | <input type="checkbox"/> SFD: Computer-Aided Dispatch | <input type="checkbox"/> SPD: 9-11 Call Recorder |
| <input type="checkbox"/> SCL: Sensorlink Ampstik | <input checked="" type="checkbox"/> SDOT: Acyclica               | <input type="checkbox"/> SPD: Computer-Aided Dispatch | <input type="checkbox"/> SPD: CopLogic           |

- 1. What concerns, if any, do you have about the use of this technology?**

The use of Wi-Fi in Acyclica, because they can obtain all the information from the phones.

The investment is worth it.

Focusing on the group: The technology is already installed. What concerns you about it's use?

The traffic remains the same.

Who uses or stores the information.

Data collection is the concern.

The main concern is the collection and storage of information.

Data collection is not alarming but rather the resources (money used) since the or [sic] the technology are not working because traffic remains the same. There is not change with the new technology. Those expenses are not valid because there are no results. Those expenses could be used for the community.

You also have to see if the technology emits radiation or any other thing that is damaging or harmful to health.

The government has all the data.

They don't need this technology to have the data because there already are methods for that, even applications or some other thing.

The other group concern is that there is no change in the problem they are trying to resolve. In the case of Acrylica [sic], it would be improving traffic.

- Technologies like this one need to collect more expert opinions.
- It would be good for the information to be shared with the community. (Transparency in the purposes and objectives of the technology and data stored, implemented tactics.)

## **2) What do you want City leadership to consider about the use of this technology?**

They are not required in some places. They are not needed in some parts of Magnolia, Queen Anne, Northgate.

Question follow-up: How much is Acyclica needed in the neighborhoods where Latinos live?

The participant doesn't believe they are needed there.

They talked about the need for strategic points and streets with a higher need for help due to the traffic.

## **What do you think about this technology in particular?**

Well, technology helps with vehicle speed or movement.

Information is stored and they analyze where you travel or how many times you cross that search [sic].

If it's only to see the traffic, it's okay.

It's okay in some parts. It might be something good. But it is possible that this technology may share personal information that can be used in other ways, especially if there is a hacking (negative way, data use).

The technology in itself is not large enough (in size) to be something that is visually unpleasant. Information collected through these methods could help manage traffic better, but it could also collect personal information.

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

The technology is not a router, but a data collection for urban planning.

Participant: "I want to believe" "convince myself" that the sensors are there to help with the traffic.

Their installation date is unknown, the results should be public. If the technology is there to alleviate traffic flow, then why don't they extend the program? Or why isn't traffic improving?

**Alternatives to this technology**

- Some sort of screen that indicates alternative routes can replace this.
- Speed limit changes may alleviate traffic flow.
- Stop building so much.
- Redesigning streets would help with traffic flow.
- Redesigning roads would serve future generations.

Page Break

**Please select which technology you wish to comment on:**

- |   |   |   |   |
|---|---|---|---|
| <input checked="" type="checkbox"/> SCL: Binoculars | <input checked="" type="checkbox"/> SCL: Sensorlink Transformer Meter (TMS) | <input type="checkbox"/> SFD: Computer-Aided Dispatch | <input type="checkbox"/> SPD:9-11 Call Recorder |
| <input type="checkbox"/> SCL: Sensorlink Ampstik    | <input checked="" type="checkbox"/> SDOT: Acyclica                          | <input type="checkbox"/> SPD: Computer-Aided Dispatch | <input type="checkbox"/> SPD: CopLogic          |

Entre hermanos (Between Brothers)

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

The binoculars are concerning if the person has no ethics. It is concerning to have a person looking through binoculars for a technology to measure electrical power use [sic].

The use of binoculars makes the group uncomfortable.

The concern with Sensorlynk specifically would be that it takes somebody's job away.

If it is to detect theft, the group believes there are other ways to know who steals.

That it won't be only to read electricity but also to obtain other types of information, if cameras are used.

## **2) What value, if any, do you see in the use of this technology?**

Energy saving

More precise records and data

Work opportunity for the person using the binoculars

It stabilizes electrical power prices.

## **3) What do you want City leadership to consider about the use of this technology?**

: Use background check, use uniforms for the workers, binocular camera.

### **What do you think about this technology in particular?**

Sensorlink Si

The binoculars are invasive.

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

Is the trust on these meters trustworthy? Are they effective?

The use of binoculars could be complemented by adding a camera.

### **Alternatives to this technology**

A type of scanner on the energy meters. Install sensors on an electrical power post to record only energy related data/information.

Page Break



**Please select which technology you wish to comment on:**

- |   |   |  |  |
|---|---|--|--|
| <input type="checkbox"/> SCL: Binoculars            | <input type="checkbox"/> SCL: Sensorlink<br>Transformer Meter (TMS) | <input type="checkbox"/> SFD: Computer-Aided<br>Dispatch | <input type="checkbox"/> SPD:9-11 Call<br>Recorder |
| <input type="checkbox"/> SCL: Sensorlink<br>Ampstik | <input checked="" type="checkbox"/> SDOT: Acyclica                  | <input type="checkbox"/> SPD: Computer-Aided<br>Dispatch | <input checked="" type="checkbox"/> SPD: CopLogic  |
| Entre hermanos (Between Brothers)                   |   |  |  |

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

Electronic [sic] failures are worrisome, especially for police reports.

The concerns are that the report did not come out. It didn't arrive for any reason.

Not everybody will be able or know how to use the computers.

The algorithm failures for each demand are alarming.

What determines the response urgency and when.

Persons fear police officers. And this media can help decrease the fear.

The automatic selection of each case or the way in which the person wrote the report and the way the computer understood it is alarming.

## **2) What value, if any, do you see in the use of this technology?**

The automatic selection of each case or the way in which the person wrote the report and the way the computer understood it is alarming.

Using computers is okay for the reports.

If people use this technology and it is analyzed in real time by other people, there's no problem.

It's another method to file a report.

Agrees with the use of computers to report, but not everybody is able to use this method/technology.

Page Break

## **3) What do you want City leadership to consider about the use of this technology?**

That it should be multilingual, implement audio, implement systems that help multiple persons with diverse abilities and or needs

If it is used adequately and as they have stated, it's okay.

The use of technology is good to respond to everything and to every person.

## **What do you think about this technology in particular?**

The group agrees with it's use.

It may save a life.

The risks and actions determine the urgency of police interruption [sic].

Some people feel more able to file a complaint through this system. The technology in use is valid.

Good for domestic violence.

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

The computer will decide the importance and/or urgency of the report/emergency implementing emergency actions.

The severity of the emergency is determined by technology.

The definition of emergency is different for each person.

Each one has the definition of surveillance, but, what about the definition of emergency?

**SITUATIONS TO APPLY ITS USE**

A street fight, physical discomfort, life related matters, domestic abuse

Based on the definition of emergency, the use will be implemented or limited only to instances of immediate danger only when we are in immediate danger or in minimal time / alarming/dangerous passing [sic].

To report something that already happened or is recurrent.

Based on the concept of emergency, persons can select the adequate method to report their case and through the necessary media.

The reports are not anonymous.

The data is collected anyway, notwithstanding the selected option.

**Alternatives to this technology**

A type of scanner on the energy meters. Install sensors on an electrical power post to record only energy related data/information.

Page Break

Entre hermanos (Between Brothers)

**City of Seattle  
Surveillance**

**Start**

Summary: The neighborhood department wants to know the opinion of this group. They will watch one and a half minute videos and will find brochures on their tables, where they'll find more information about what they saw.

**Demographics:**

Eight persons participated, one from West Seattle, one from First Hill, two from Ravenna/Laurelhurst and four from King County (outside Seattle).

Four persons were considered Hispanic or Latino, one Native American or Alaskan native, and three did not give their opinion.

Five persons marked 18-44 as their age range, two marked 45-64 as theirs, and one did not give his/her opinion.

Five persons marked male as their gender, one marked transgender, one marked feminine, and one did not give his/her opinion.

**Other important information:**

- Questions will be asked.
- There will be a sheet to talk about videos of interest.
- They were thanked for coming.
- The concept of surveillance will be handled like the City of Seattle manages it.
- Tom: Thanked the invitees for coming

**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.”

**Presenter:** Asked if the conversation in English was understood.

**Group:** Agreed.

**Tom:** Do not let information on videos stop you from making comments or raising questions.

**Presenter:** Explained the concept of surveillance as it has been interpreted by the City of Seattle. It was analyzed this way: “Surveillance is defined as technologies that observe or analyze the movements, behavior or actions of identifiable individuals in a way that reasonably raises concerns about civil liberties, freedom of expression or association, racial equality or social justice”.

- People movement is observed through this technology, and this may be uncomfortable for some persons.
- Police cameras do not qualify as surveillance technologies in this subject.
- The presentation shown on the screen using videos shall be in English.
- Everybody was asked to treat each other with respect and to provide their opinion, and to mention their name and even the neighborhood where they live.

**The Group:**

The participant came because he wants to obtain more information and give his/her opinion. He/she is from Seattle.

The participant came from Shoreline/Seattle to see how much the technology enters affects [sic].

The participant came because he/she wants to know what information is collected by the government and what the information is used for. Maybe the information obtained could be used to persecute persons of color/minorities/marginated persons.

The participant came from First Hill, because he/she wants to know the city's point of view and see what opinions come up.

The participant came from Seatac because he/she is interested in the subject and because safety is important and he/she wants to know where the information goes.

The participant came from Ravenna/Northgate. He/she wants to know how trustworthy the technology is and what it will be used for. Harmful or beneficial?

The participant came from Seatac and came because it is a very interesting subject since he/she needs to know/keep informed of what government leaders do.

The participant came from Burien due to the importance of the subject and privacy.

**Presenter:** The technology is not new. It is already being used. And they want to know the format for future technology to have [sic].

**The Acyclica Seattle Department of Transportation video was shown**

This technology is a sensor that detects the Wi-Fi. It's a sensor that detects the Wi-Fi technology.

**Seattle Metering Tool was shown**

Nobody in the group knows about the subject, plus the presenter will not talk about this in depth to avoid influencing opinions.

**The Fire Department's Computer Aided Dispatch video was shown****The 9-1-1 logging recorder video was shown**

Clarification: Printed information was provided to explain each of the technologies.

**Coplogic video was shown**

The group did not know that you can file a report with the police using their page / online.

**The Police Computer Aided Dispatch video was shown**

This technology is similar to the one the Fire Department uses.

**Those present were asked which video they were interested in analyzing.****They agreed to analyze Acyclica, Binoculars/Sensorlink, and Coplogic****The following are the questions to be asked:**

What do you think of this technology system specifically and the reason for using it?

What do you think this technology will contribute to the city?

What concerns does the use of this system bring up?

What would you recommend to the group of city politicians responsible for making decisions about implementing these technologies?

What other way can we solve the problem that this technology is designed to solve?

## Acyclica

**Question:** What do you think of this technology system specifically and the reason for using it?  
(How it is used and what the use is)

- Well, technology helps with vehicle speed or movement.
- Information is stored and they analyze where you travel or how many times you cross that search [sic].
- If it's only to see the traffic, it's okay.
- It's okay in some parts. It might be something good. But it is possible that this technology may share personal information that can be used in other ways, especially if there is a hacking (negative way, data use).
- The technology in itself is not large enough (in size) to be something that is visually unpleasant. Information collected through these methods could help manage traffic better, but it could also collect personal information.

**Question:** What does this technology contribute to the city?

- The contribution would be good in terms of traffic agility only if the technology is synchronized with traffic lights, otherwise it is not useful, if it does not contribute to the improvement of traffic.
- The participant says there are alternatives to avoid traffic.
- The participant believes that the technology is interesting since it uses google maps, and agrees with traffic improvement.
- If the objective is to improve traffic, he/she agrees. But he/she also wants to know where the devices will be placed, if some people will receive more benefits than others.



**Question:** What concerns do you have with the possible use / potential use of this technology?

- He/she is worried about the use of Wi-Fi in Acylica, because they can obtain all the information from the phones.
- If the potential can be applied to the investment.

**Focusing on the group:** The technology is already installed. What concerns you about it's use?

- The traffic remains the same.
- Who uses or stores the information.
- Data collection is the concern.

**More than half the group believes that (information storage and collection) is the concern.**

- The participant does not agree. Data collection is not alarming but rather the resources (money used) since the or [sic] the technology are not working because traffic remains the same. There is not change with the new technology. Those expenses are not valid because there are no results. Those expenses could be used for the community.
- You also have to see if the technology emits radiation or any other thing that is damaging or harmful to health.
- The government has all the data.
- Opinion of another participant: They don't need this technology to have the data because there already are methods for that, even applications or some other thing.

**The other group concern is that there is no change in the problem they are trying to resolve. In the case of Acrylica [sic], it would be improving traffic.**

- Technologies like this one need to collect more expert opinions.

- It would be good for the information to be shared with the community. (Transparency in the purposes and objectives of the technology and data stored, implemented tactics.)

**Question:** Would you tell the politicians anything about the locations of these devices?

- They are not required in some places. They are not needed in some parts of Magnolia, Queen Anne, Northgate.

**Question follow-up:** How much is Acyclica needed in the neighborhoods where Latinos live?

- The participant doesn't believe they are needed there.

They talked about the need for strategic points and streets with a higher need for help due to the traffic.

**Presenter:** Do you believe that Acyclica [sic] is like the Google router?

- The technology is not a router, but a data collection for urban planning.
- Participant: "I want to believe" "convince myself" that the sensors are there to help with the traffic.
- Their installation date is unknown, the results should be public. If the technology is there to alleviate traffic flow, then why don't they extend the program? Or why isn't traffic improving?

**Another Question:** Is there any other technology that can be used instead of Acyclica?

**Alternatives:**

- Some sort of screen that indicates alternative routes can replace this.
- Speed limit changes may alleviate traffic flow.
- Stop building so much.

- Redesigning streets would help with traffic flow.
- Redesigning roads would serve future generations.

## Technology #2

### Sensorlink/Binoculars

**Question:** What does the group think about the technology?

- The binoculars are concerning if the person has no ethics. It is concerning to have a person looking through binoculars for a technology to measure electrical power use [sic].
- A sensor that detects electricity would be better.
- The use of binoculars makes the group uncomfortable.

**Question:** What do you think about the electricity meter technology (sensorlink) and about it being used at your home?

- Two participants are not made uncomfortable or affected by it.
- The concern would be that it takes somebody's job away.
- The binoculars are invasive.
- Why use binoculars if you can go to the home and see the meter in person, by asking permission? If the technology is used to see if persons steal electricity, do you believe that they don't know who steals?
- The group believes they do know.

**Question:** What do you think this technology will contribute?

- The video says that it saves 3 million dollars.

**Question:** In what way does this benefit the city / citizens / community?

- Energy stealing is concerning.
- If they already keep the record and they let the community know, they might save money.
- The use of binoculars could provide a person with a job, and money can be saved with this technology.
- Does the technology cause the spending of electricity in order to see electrical power expenses? If the goal is to avoid theft, then electricity bill expenses should continue to be stable.

**Question:** Is the trust on these meters trustworthy? Are they effective?

- It helps with precision, to lower prices.
- Removing the binoculars would be a suggestion, or using binoculars that video record.
- If they already have a record of the energy (consumption, expenses, etc.), energy theft is not sufficient to establish this type of technology, since the theft or some other anomaly can be identified depending on the high or low or sudden level analyzed / seen / detected by means of conventional already established methods.
- Another Recommendation: Use background check, use uniforms for the workers, binocular camera.
- A type of scanner on the energy meters. Install sensors on an electrical power post to record only energy related data/information.
- The concern is that it won't be only to read electricity but also to obtain other types of information, if cameras are used.

### Technology #3 Coplogic

- This technology not only saves time, but also police time, since they would work on other things.
- Using computers is okay for the reports.
- If people use this technology and it is analyzed in real time by other people, there's no problem.

**Focus:** What we want to discuss is the use of internet and the reports.

- It's another method to file a report.
- Agrees with the use of computers to report, but not everybody is able to use this method/technology.

**Question:** How does it help the community?

- Why use these methods?
- The group agrees with it's use.
- It may save a life.
- The risks and actions determine the urgency of police interruption [sic].
- Some people feel more able to attend through this system. The technology in use is valid.
- Good for domestic violence.
- Electronic [sic] failures are worrisome, especially for police reports.
- The concerns are that the report did not come out. It didn't arrive for any reason.
- Not everybody will be able or know how to use the computers.

- The algorithm failures or when or what promotes the urgency of each demand is alarming.
- Demand criteria and what type of parameter concern is trustworthy must be questioned / analyzed, and what / who deserves priority or importance or help.

**Question:** In what way would this use benefit the community?

- Persons can be discriminated.
- Persons fear police officers. And this media can help decrease the fear.
- The computer will decide the importance and/or urgency of the report /emergency implementing emergency actions.
- The severity of the emergency determines the use of technology.

**Question:** Any concern about the use of this technology?

- The automatic selection of each case or the way in which the person wrote the report and the way the computer understood it is alarming.

**Question:** In what situation will you use this technology?

- A street fight, physical discomfort, life related matters, domestic abuse
- Each person has the definition of surveillance, but, what about the definition of emergency?
- The definition of emergency is different for each person.
- Based on the definition of emergency, the use will be implemented or limited only to instances of immediate danger only when we are in immediate danger or in minimal time / alarming/dangerous passing [sic].

**Question:** What is the purpose of the computer report?

- To report something that already happened or is recurrent.

- Based on the concept of emergency, persons can select the adequate method to report their case and through the necessary media.
- The reports are not anonymous.
- The data is collected anyway, notwithstanding the selected option.

**Question:** What would you recommend to the politicians?

- That it should be multilingual, implement audio, implement systems that help multiple persons with diverse abilities and or needs

**Question:** Any other general comment about the surveillance technology?

- If it is used adequately and as they have stated, it's okay.
- The use of technology is good to respond to everything and every person.

**Advice:**

- Provide information, more information about what you are doing (transparency/disclosure of information)
- There should be more transparency.

**Be transparent about data collection, so there are discussions and informed decisions for all implemented technologies and technologies to be implemented.**

## 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 reader 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: 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



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



## 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<sup>1</sup> 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)<sup>2</sup>, only a computerized system could meet the state's response reporting guidelines established in RCW 35A.92.030<sup>3</sup>.

CentralSquare provides the dispatch service used by SFD. CentralSquare is a new entity resulting from the merger of Superior, TriTech, Zuercher, and Aptean<sup>4</sup> in September 2018.

### Recommendations

- Trittech, 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 Trittech as SFD's CAD solution.
- Trittech 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.

---

<sup>1</sup> "NFPA Standard 1710." <https://services.prod.iaff.org/ContentFile/Get/30541>

<sup>2</sup> "2017 annual report - Seattle.gov."

[https://www.seattle.gov/Documents/Departments/Fire/FINAL%20Annual%20Report\\_2017.pdf](https://www.seattle.gov/Documents/Departments/Fire/FINAL%20Annual%20Report_2017.pdf)

<sup>3</sup> "RCW 35A.92.030: Policy statement—Service ... - Access WA.gov."

<https://app.leg.wa.gov/rcw/default.aspx?cite=35A.92.030>

<sup>4</sup> "Superior, TriTech, Zuercher, and Aptean's Public Sector Business to " 5 Sep. 2018,

<https://www.tritech.com/news/superior-tritech-zuercher-and-aptians-public-sector-business-to-form-centr>  
[a](#)



## 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<sup>5</sup>. Seattle ranks sixth in the nation for traffic congestion<sup>6</sup>. The need for intelligent traffic shaping and development has never been greater. Acyclica, a service provided by Western Systems and now owned by FLIR<sup>7</sup>, 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.

<sup>5</sup> "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/>

<sup>6</sup> "INRIX Global Traffic Scorecard." <http://inrix.com/scorecard/>

<sup>7</sup> "FLIR Systems Acquires Acyclica | FLIR Systems, Inc." 11 Sep. 2018, <http://investors.flir.com/news-releases/news-release-details/flir-systems-acquires-acyclica>



## 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<sup>8</sup> 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.

---

<sup>8</sup> "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>



## 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<sup>9</sup>. Again, in 2017, a NICE-owned server was set up with public permissions, exposing phone numbers, names, and PINs of 6 million Verizon customers<sup>10</sup>.

### 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<sup>11</sup>, 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.

---

<sup>9</sup> "Backdoor in Call Monitoring, Surveillance Gear — Krebs on Security." 28 May. 2014, <https://krebsonsecurity.com/2014/05/backdoor-in-call-monitoring-surveillance-gear/>

<sup>10</sup> "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>

<sup>11</sup> "9-1-1 Center - Police | seattle.gov." <https://www.seattle.gov/police/about-us/about-policing/9-1-1-center>



## 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<sup>12</sup>. 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<sup>13</sup>. 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.

---

<sup>12</sup> “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>

<sup>13</sup> “Welcoming Cities Resolution - Council | seattle.gov.”

<http://www.seattle.gov/council/issues/past-issues/welcoming-cities-resolution>



## 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<sup>14</sup>. Such sensitive information should not be protected by trust alone.

---

<sup>14</sup> "Privacy Policy | LexisNexis." 7 May. 2018, [https://www.lexisnexis.com/en-us/terms/privacy-policy\\_page](https://www.lexisnexis.com/en-us/terms/privacy-policy_page)

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)



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),<sup>1</sup> 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.<sup>2</sup> In the case of Acyclica's operation in Seattle, the dataset is comprised of MAC addresses recorded on at least 301 intersections,<sup>3</sup> 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

---

<sup>1</sup> 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.

<sup>2</sup> Montjoye, Y., Hidalgo, C., Verleysen, M., and Blondel, V. 2013. Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports*. 3:1375.

<sup>3</sup> 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.<sup>4</sup> ICE also now has agency-wide access to a nationwide network of license plate readers controlled by Vigilant Solutions,<sup>5</sup> 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,<sup>6</sup> as well as discrepancies between the SIR, the information shared at the technology fair (the first public meeting to discuss the Group 2 technologies),<sup>7</sup> 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.<sup>8</sup> As of March 2019, FLIR has discontinued Acyclica RoadTrend sensors.<sup>9</sup> 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,

<sup>4</sup> <https://crosscut.com/2018/02/immigration-officials-subpoena-city-light-customer-info>

<sup>5</sup> <https://www.theverge.com/2018/3/1/17067188/ice-license-plate-data-california-vigilant-solutions-alpr-sanctuary>

<sup>6</sup> Explained in further detail in 1. Acyclica – SDOT Major Concerns below.

<sup>7</sup> <http://www.seattle.gov/tech/initiatives/privacy/events-calendar/#?i=3>

<sup>8</sup> <https://www.crunchbase.com/acquisition/flir-systems-acquires-acyclica-e6043a1a#section-overview>

<sup>9</sup> <https://www.flir.com/support/products/roadtrend#Specifications>

short, and impose no meaningful restrictions on the purposes for which Acyclica devices may be used.<sup>10</sup> 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.

---

<sup>10</sup> 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,<sup>11</sup> 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,<sup>12</sup> 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.<sup>13</sup> 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

---

<sup>11</sup> Included in Appendix 1.

<sup>12</sup> As noted in 1. Acyclica – SDOT Background above.

<sup>13</sup> <https://www.flir.com/support/products/roadtrend#Specifications>

RoadTrend sensors (e.g., camera technology and thermal imaging)<sup>14</sup> 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

---

<sup>14</sup> <https://www.flir.com/support/products/trafione#Resources>

Department of Transportation)?<sup>15</sup>

- 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**

---

<sup>15</sup> <https://www.ftwa.dot.gov/publications/research/operations/its/06108/03.cfm>

### *Background*

CopLogic (LexisNexis’s Desk Officer Reporting System-DORS)<sup>16</sup> 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.

---

<sup>16</sup> <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<sup>17</sup> 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.<sup>18</sup>

*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.

---

<sup>17</sup> <https://www.aclu-wa.org/docs/aclu-letter-king-county-council-regarding-mark-43>

<sup>18</sup> 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 Versatarm) 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**



February 6<sup>th</sup>, 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,

 A handwritten signature in black ink, appearing to read "Daniel Benhammou", with a long horizontal flourish extending to the right.

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 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 CJ 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  
Interim Chief Technology Officer  
Seattle Information Technology Department

Date Feb 2, 2018

  
\_\_\_\_\_  
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.

## 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.

<b>Item:</b>	1
<b>Section Name:</b>	Personnel Security
<b>Question:</b>	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? ( <i>CJIS Security Policy, Version 5.5, Section 5.12.1.1</i> )  Yes  Please provide the SID numbers for all the IT personnel.
<b>Agency Response:</b>	List emailed 05/16/17

<b>Item:</b>	2
<b>Section Name:</b>	Personnel Security
<b>Question:</b>	Have all your agency and/or county/city IT personnel viewed the technical security awareness training (Level 4) in CJIS Online? ( <i>CJIS Security Policy, Version 5.5, Section 5.2</i> )  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: <a href="https://www.cjisonline.com/">https://www.cjisonline.com/</a>
<b>Agency Response:</b>	Sent email 05/16/17

<b>Item:</b>	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](mailto: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 CJ? (*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 CJ encrypted? (*CJIS Security Policy, Version 5.5 Section 5.10.1.2*)

**User Answer:** No

**Compliance Response:** CJ 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

<b>Item:</b>	5
<b>Section Name:</b>	Event Logging
<b>Question:</b>	Does your agency have an established audit trail capable of monitoring the following: <ul style="list-style-type: none"><li>- Successful and unsuccessful log on attempts</li><li>- Successful and unsuccessful password changes</li><li>- Successful and unsuccessful attempts to access, create, write, delete or change permissions on a user account, file, directory or other system resources</li><li>- Successful and unsuccessful actions by privileged accounts</li><li>- Successful and unsuccessful attempts for users to access, modify, or destroy audit log files</li></ul> (CJIS Security Policy, Version 5.5, Section 5.4.1.1)
<b>User Answer:</b>	No
<b>Compliance Response:</b>	Please advise when your agency will have an established audit trail capable of monitoring the following: <ul style="list-style-type: none"><li>- Successful and unsuccessful log on attempts</li><li>- Successful and unsuccessful password changes</li><li>- Successful and unsuccessful attempts to access, create, write, delete or</li></ul>

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

**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 privileged accounts
- Successful and unsuccessful attempts for users to access, modify, or destroy audit log files

<b>Item:</b>	6
<b>Section Name:</b>	Identification and Authentication
<b>Question:</b>	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. <i>(CJIS Security Policy, Version 5.5, Section 5.6.2.2)</i>
<b>User Answer:</b>	Yes
<b>Compliance Response:</b>	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.
<b>Agency Response:</b>	<p>Full policy emailed to ACCESS on 04/23/18:</p> <p>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).</p> <p>*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</p>

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 toCJI.

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 anytime.
- 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 CJ I or when all personnel will be virtually escorted or a policy prohibiting remote access from an unsecure location is established.

**Agency Response:** See #6



**Item:** 7

**Section Name:** Cloud Computing

**Question:** Does the agency utilize a cloud provider to host or store CJ 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 CJ encrypted prior to entering the cloud?

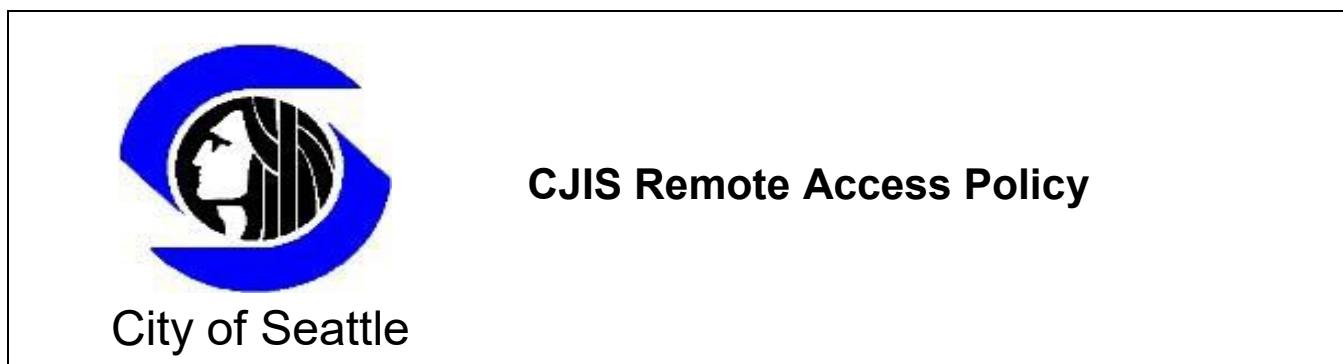
**User Answer:** No

**Compliance Response:** Please advise when the CJ that goes to the cloud will be encrypted.

**Agency Response:** Seattle is utilizing Office 365 and CJ 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



June 1<sup>st</sup>, 2018

### **Overview**

The CJIS 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 CJJ.
- 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 CJJ and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJJ.
- 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 CJJ. 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 CJJ 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 CJJ 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 CJJ.

**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
<b>Automated License Plate Recognition (ALPR)</b>	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
<b>Booking Photo Comparison Software (BPCS)</b>	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 <a href="#">SPD Manual §12.045</a> .	2
<b>Forward Looking Infrared Real-time video (FLIR)</b>	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
<b>Undercover/ Technologies</b>	<p>The following groups of technologies are used to conduct sensitive investigations and should be reviewed together.</p> <ul style="list-style-type: none"> <li>• <b>Audio recording devices:</b> 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 (<a href="#">RCW 9A.73.200</a>).</li> <li>• <b>Camera systems:</b> 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.</li> <li>• <b>Tracking devices:</b> 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.</li> </ul>	<p>4</p>
<b>Computer-Aided Dispatch (CAD)</b>	<p>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.</p>	<p>5</p>

Technology	Description	Proposed Review Order
<b>CopLogic</b>	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
<b>Hostage Negotiation Throw Phone</b>	A set of recording and tracking technologies contained in a phone that is used in hostage negotiation situations to facilitate communications.	7
<b>Remotely Operated Vehicles (ROVs)</b>	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
<b>911 Logging Recorder</b>	System providing networked access to the logged telephony and radio voice recordings of the 911 center.	9
<b>Computer, cellphone and mobile device extraction tools</b>	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
<b>Video Recording Systems</b>	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
<b>Washington State Patrol (WSP) Aircraft</b>	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
<b>Washington State Patrol (WSP) Drones</b>	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
<b>Callyo</b>	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
<b>I2 iBase</b>	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
<b>Parking Enforcement Systems</b>	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 <a href="#">SMC 11.35</a> .	16
<b>Situational Awareness Cameras Without Recording</b>	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
<b>Crash Data Retrieval</b>	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
<b>Maltego</b>	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

**2020 Surveillance Impact Report Executive Overview**

# **911 Logging Recorder**

**Seattle Police Department**

## 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.

## 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.**

## 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.