City of Seattle

2024 Surveillance Impact Report

Real-Time Crime Center

Seattle Police Department

Surveillance Impact Report ("SIR") overview

About the Surveillance Ordinance

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

How this Document is Completed

This document is completed by the requesting department staff, support and coordinated by the Seattle Information Technology Department ("Seattle IT"). As Seattle IT and department staff complete the document, they should keep the following in mind.

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

Surveillance Ordinance Review Process

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

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

Privacy Impact Assessment

Purpose

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

When is a Privacy Impact Assessment Required?

A PIA may be required in two circumstances.

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

1.0 Abstract

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

Gun violence, human trafficking, and other persistent felony crimes are concentrated at specific geographic places in the city. This concentrated crime is often anchored at these places and requires a holistic crime-prevention strategy.

The Crime Prevention Technology pilot is one component of an overall strategy of addressing felony crime at specific places. These technologies will be coupled with police patrols, continued investments in community-based initiatives, and enhanced lighting and cleaning.

This SIR covers the Real-Time Crime Center (RTCC) software, one part of this pilot, and provides a centralized location for real-time information and analysis. At its core, RTCC software integrates dispatch, camera, officer location, 911 calls, records management systems, and other information into one "pane of glass" (a single view). The software is used to alert RTCC staff to a serious criminal event, see multiple streams of information overlaid on a map view, and convey information to officers responding in the field.

The purpose of RTCC software is to provide situational awareness to increase officer and community safety and reactively investigate incidents. Having real-time, accurate information in one place helps increase reliability regarding the location of victims and suspects – enabling quicker aid and safer apprehension. Having better visual and spatial suspect information helps reduce unnecessary stops by officers, focusing their efforts on verified locations and accurate descriptions. RTCC also aids in investigations by aggregating multiple

data sources into one location, helping provide detectives with actionable information that increases the quality of investigations and prosecutions, leading to increased accountability for criminal offenders.

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

The City's police staffing crisis, now in its fourth year, has resulted in over 700 officers leaving SPD since 2019. As of January 2024, 913 police officers are available for deployment in the city, the lowest number of in-service officers since 1991 and significantly below per-capita staffing relative to comparative jurisdictions. Low staffing levels also affect investigations, which hinders police effectiveness in solving cases and holding violent criminals accountable.

Gun violence, human trafficking, and other serious felony crimes are often concentrated at specific geographic places, and long-time efforts to prevent these crimes have not been consistently successful. Implementing technology tools to bolster policing capabilities, as one part of a holistic crime prevention and reduction plan is essential to address ongoing gun violence, vehicle theft, human trafficking, and persistent felony crime at specific places, including within our most victimized communities.

Real-time crime center software brings several technologies deemed surveillance technologies (CCTV, ALPR, etc.) into one platform. In addition, some RTCC software uses non-generative AI, such as object detection, to analyze those surveillance technologies, if enabled. As a note, SPD will not use AI facial recognition technologies. Finally, the software stores information from these technologies either in the cloud or on-premise, creating some risks around data security and retention.

Due to these factors, the City of Seattle Privacy Office has deemed the technology surveillance technology, which triggered this review.

2.0 Project / Technology Overview

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

2.1 Describe the benefits of the project/technology.

The theory of change supporting the pilot project is that these technologies (1) bolster police effectiveness in public places where crime is concentrated when used with other crime prevention efforts, including increased police patrols, enhanced lighting, graffiti mitigation, and others (CPTED), (2) deter criminal behavior when public notice is posted, and (3) gather evidence to hold offenders accountable. These efforts can improve public safety and enhance the public's confidence in the city government's ability to maintain safe neighborhoods.

Serious felony crimes are often concentrated at specific geographic locations in Seattle and long-time efforts to prevent these crimes have not been consistently successful. Police

effectiveness is further hindered due to unprecedented patrol and investigation staffing shortages in the Seattle Police Department.

RTCC software can help mitigate staffing shortages for both patrol officers and detectives by providing more reliable and accurate data on incidents in real-time.

The benefits of the RTCC for a victim(s):

- RTCC staff can use multiple technologies (CCTV, etc.) to pinpoint the location of crimes and identify the location of victims.
- RTCC staff can assess the scene before officers responding, helping speed up the deployment of emergency aid or lifesaving assistance.

Increased investigative information helps lead to justice for victims. The benefits of RTCC technology for a community:

- Increased investigative evidence can aid in the capture and prosecution of offenders, leading to reduced violence and fewer firearms on the street. Increased evidence can also help exonerate the innocent.
- Integration with CCTV cameras and real-time crime center software can provide detectives with precise information about suspect vehicle, appearance, and location, increasing correct identification of suspects and reducing unnecessary traffic stops and adverse interactions with the public.

The benefits of RTCC technology for an officer:

- Real-time crime center software can facilitate a coordinated, precise response to suspect apprehension, increasing the safety of arrests for all involved. The technology provides a data-driven orientation to police response and staffing.

Here is one example of how SPD might use the RTCC software to more efficiently utilize separate data sources to aid victims, capture dangerous suspects, and help remove firearms from the streets:

> A RTCC officer receives an alert through CAD and the RTCC software that there are gunshots on Aurora Avenue North. The software shows a map of the area on her monitor, with the associated dispatch call superimposed on the screen. Her map screen also automatically shows the feeds of the closest three CCTV cameras, as well as nearby patrol car locations. She uses the RTCC software to enlarge the feed for the cameras north of the incident and sees a black Honda Civic moving at a high rate of speed in a northerly direction on Aurora.
>
> Using the software, she quickly pulls up the camera recording where the gunshots were reported and visually ascertains that the shots were fired from a black Honda and that there is a person down on the ground. She advises over SPD radio that there is a possible gunshot victim and gives a description of the Honda and the license plate. She sees from the live camera feeds that the Honda is turning west on 125th Street,

and that there is a patrol vehicle on that street 10 blocks west of Aurora and one 15 blocks south of the scene on Aurora. She advises over the radio that the suspect is heading west on 125th St. She goes back to the live camera view and surveys the shooting scene. The person is still down. No one else is at the scene. She relays via radio what she has seen through the RTCC software.

After the incident, she uses the RTCC software to create clips of all scenes showing the incident and the vehicle travel before, during and after the incident and uploads them from the RTCC software to the SPD digital evidence system.

At the same time this is happening, the officer driving north on Aurora gets dispatched to a possible shooting scene. The dispatcher informs her that there is a victim on the ground and the RTCC officer has observed no other people around the victim. The officer arrives on scene, exits her vehicle, takes a quick scan of the scene to confirm that the scene is secure. She grabs a first aid kit in her trunk, then runs to the victim on the ground and renders aid. In the background, she can hear the Fire Department sirens coming toward her. She radios dispatch and tells them the scene is secure for the arriving paramedics.

After the shooting scene is secure, a homicide detective arrives at the scene. Officers are using their flashlights and struggling to find bullet casings. The detective pulls up the RTCC application on his phone and brings up the information for the incident. He walks towards the officers and shows them the video – they move up the road a bit and eventually find the casings judgeing by the location of the vehicle in the video. The detective is satisfied there were no witnesses after watching the video again and proceeds with his work at the scene.

2.2 Provide any data or research demonstrating anticipated benefits.

Academic research related to the effect of real-time crime centers is limited because of their fairly recent implementation; however, a 2023 John Jay College of Criminal Justice study showed that a real-time crime center in Chicago, IL increased case clearance rates 5% for violent crime, 12% for property crime, and 11% for overall crime. The authors concluded that "RTCCs may provide investigative benefits to police through the integration of technologies and data, thus enhancing case solvability."

An extensive evaluation of the Chicago Police Department's use of a RTCC was completed by the RAND in 2019. This evaluation is meaningful because it highlighted the successes and failures of the CPD centers and made specific recommendations to increase their effectiveness.

Other studies on the effects of technologies integrated with RTCC software, such as CCTV, are discussed in their respective Surveillance Impact Reports.

SPD will evaluate the efficacy of the RTCC implementation through standard performance measures already in use: violent crime rate, priority one response time, patrol coverage when not responding to calls (over/under policing), equity, perceptions of trust, perceptions

of safety. Successful implementation of this suite of technologies (CCTV/RTCC/enhanced ALPR) will be indicated by a decrease in violent crime, priority one response time, no increase or a decline in measures of police over-presence, measure of disparate impact, and an increase in perceptions of trust and safety.

This pilot will be data-informed and guided. It will terminate if data suggests the technology is ineffective. Utilizing the abilities of the Performance Analytics and Research Unit, the Seattle Police Department has a plan to actively manage performance measures reflecting the "total cost of ownership of public safety," Equity, Accountability, and Quality ("EAQ"), which includes measures of disparate impact and over-policing. In addition to a robust Continuous Intervention Assessment designed to inform, in real-time, the active development of a safer, more effective, Evidence-Based Policing (EBP) competency, the EAQ program assures just right policing is achieved with undue collateral harm.

2.3 Describe the technology involved.

The core functionality of RTCC software involves integrating multiple sources of information into a single "pane of glass" (a single view). The sources of information that are being integrated with the software are current or expected SPD technologies such as the department's CAD system (computer-aided dispatch), closed-circuit television cameras (CCTV), automatic vehicle location (AVL) system, body and in-car video cameras, automated license plate readers (ALPR), digital evidence platforms, and 911 call systems.

Most of the technology comes into play around a mapping function which provides the overlay for all the other technologies. The mapping system includes roads, building layouts (when provided), and other layers like beat/sector boundaries. Most RTCC vendors provide this service via cloud-based web applications, as well as mobile applications for use in the field.

While most integrations between RTCC software and department applications occur between vendor APIs, some RTCC vendors use hardware for CCTV cameras that allow for the recording of the camera video, providing the ability to playback CCTV in the RTCC environment. RTCC software for CCTV cameras can also provide in-application video analytics that use machine-learned algorithms to analyze camera feeds and, using object recognition, locate specific items, people based on clothing, or vehicles based on description. This technology complies with the city of Seattle's AI rules for use, requiring a "human in the loop" at the initiation and evaluation of the results. SPD will not use facial recognition technology. In addition, SPD would not use analytics available in some platforms that combine different data sources and use algorithms or AI to present trends.

Some RTCC vendors produce hardware that allows for private camera owners (such as private businesses) to share specific camera feeds with agencies. This option would be fully voluntary at the discretion of the camera owners. Private camera owners can also set up conditional sharing, meaning they can determine the parameters of what, how, and when their camera feeds are shared. Some vendors also provide a registry so that private camera owners can share the location of the camera, but not the video feeds, so agencies can easily

canvass for videos after an incident. The system can then allow SPD to send an email to all registered cameras in an area requesting relevant video. There is no obligation to share footage if a system is registered.

Some RTCC software vendors also include public-facing features such as notification software that allows an agency to push out real-time information to the public in the form of texts for those who opt-in. These functions are like Alert Seattle and Reverse 911 and could be used in large-impact situations such as traffic re-routing, chemical spills, or other life-safety disruptions.

There are also features that allow a rapid video response to calls for service. For example, a community member that calls 911 may be sent a link to their phone to opt-in to a video chat with a 911 operator or officer to provide face-to-face communication to help facilitate accurate officer response and/or medical aid instruction. The caller would need to opt-in to allow the use of their camera, microphone, and GPS. This service could be used in an active shooter situation to help officers assess the situation or other rapidly changing emergency environments.

Other potential features include tools that enable incident planning and real-time management across the department, including freehand sketching of maps, iconography, and differing views for different groups of users, and editing access across a variety of connected devices. Integrating graphical illustration tools with live video and team geolocation creates a flexible and holistic view of emergent incidents, streamlining response capabilities. This feature would help incident commanders utilize mapping capabilities to better manage large-scale events.

Another potential feature allows officers to listen to 911 calls directly, helping to bring small details within the words, tone, or background that can aid responders in achieving desired outcomes. This feature would utilize 911 call recording already in use at the Seattle 911 call center.

Finally, some RTCC software systems have services that allow members of the public to anonymously submit multi-media tips by texting pictures, text, or video to a publicized number. Tips are then stored in the system for examination and potentially used as evidence.

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

The mission of the SPD is to prevent crime, enforce the law, and support quality public safety by delivering respectful, equitable, professional, and dependable police services. SPD's priorities include the use of best practices that include officer safety guidelines and performance-based accountability to provide progressive and responsive police services to crime victims, witnesses, and all members of the community and to structure the organization to support the SPD mission and field a well-trained sworn and non-sworn workforce that uses technology, training, equipment, and research strategically and effectively.

The RTCC software helps provide responsive police services to victims, witnesses, and members of the community by providing responders with more accurate and robust

information that does not require significant staffing additions. Using technology that enables quicker, complex, and effective police response aligns with the SPD mission and will benefit the community as a whole.

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

At the time of writing, planning is still underway for exactly who would use the RTCC software. The vision is for SPD to staff a real-time crime center with a combination of sworn officers and civilian staff, eventually transitioning to a more civilian-staffed model. Due to the wide functionality of RTCC software, it is likely incident commanders with appropriate training will be the primary users of the software, supported by sworn and civilian staff. The Office of the Inspector General will have full access to the RTCC operation.

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 RTCC will have a set of access controls based on what is required for each user. Only authorized/trained SPD and OIG personnel will have direct access. Data and information obtained through the RTCC may only be accessed or extracted for legitimate law enforcement purposes, as governed by SPD Policy 12.050.

SPD is developing an omnibus surveillance technology policy to provide general guidance on several topics, including value and equity statements for technology use, an explanation of the surveillance ordinance requirements, internal processes for technology approval and acquisition, general tracking metrics for surveillance technologies, retention requirements and limitations, and general use requirements for surveillance technologies. Additionally, issues and guidance unique to specific surveillance technologies would be included for each technology. As such, the department will create a policy section for each surveillance technology, including those proposed here. The need for ALPR and CCTV technologies and the strategic deployment of the SPD policies is driven by gun violence and persistent felony crime at specific locations. SPD's use of these technologies will focus on these crimes.

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

The SPD does not currently have any policies related to RTCC. As the RTCC will be the platform for different technologies, such as CCTV, any video recordings that are captured will only be preserved as evidence if it is determined a crime has been committed.

SPD is developing an omnibus surveillance technology policy to provide general guidance on

several topics, including value and equity statements for technology use, an explanation of the surveillance ordinance requirements, internal processes for technology approval and acquisition, general tracking metrics for surveillance technologies, retention requirements and limitations, and general use requirements for surveillance technologies.

Additionally, issues and guidance unique to specific surveillance technologies would be included for each technology. As such, the department will create a policy section for each surveillance technology, including those proposed here. The need for ALPR and CCTV technologies and the strategic deployment of the SPD policies is driven by gun violence and persistent felony crime at specific locations. SPD's use of these technologies will focus on these crimes.

The use of CCTV will comply with SMC Chapter 14.12, Collection of Information for Law Enforcement Purposes. All existing SPD policies related to technology and Criminal Justice Information Systems will apply to the RTCC. (Policy 12.050). All use of the RTCC will be for legitimate law enforcement purposes only and personal or inappropriate use or dissemination of information can result in internal discipline, termination, and penalties under federal or state law.

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

Supervisors and commanding officers are responsible for ensuring compliance with SPD policies.

Access to the RTCC will only be made accessible to authorized SPD, OPA, and OIG personnel. Authorized personnel will receive SPD-developed training in the use of the RTCC and related policy, operation, and procedures prior to receiving system access.

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.

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.

The RTCC software integrates data from other SPD systems into a centralized location for real-time information and analysis. Data feeding into RTCC could come from dispatch, CCTVs, officer location, 911 calls, records management systems (RMS), ALPR, geographic information systems (GIS), and other information systems. Information from some of these systems may be stored in storage related to the RTCC software to provide a comprehensive record of an incident. Storage of information not used for investigations or law-enforcement uses would be for 30 days maximum.

SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a General Offense (GO) Report. Evidence is submitted to the Evidence Unit and associated with a specific GO Number and investigation.

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

The RTCC software is used to integrate data from various sources used by SPD into one place, a single window view. All data sources have their own pre-existing controls in place to minimize inadvertent or improper collection, as outlined in previous surveillance impact reports for the relevant technology.

The RTCC software itself will store some of the data from the integrated systems to provide a comprehensive picture of an incident. Data that is not part of a criminal investigation will be subject to a 30-day retention policy, after which it will be purged from the system.

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 desired deployment date is mid-2024. SPD's vision is to have a RTCC staffed by a combination of sworn and civilian staff that will monitor the RTCC software and provide information to patrol officers and detectives. Access may be given to detectives and patrol officers in certain situations and with appropriate training. The system will be used by incident commanders at the scene of major crimes and other events requiring police engagement.

The SPD Technology and Innovation Unit will be the initial owner of the system and will manage implementation.

4.4 How often will the technology be in operation?

The technology will be in continuous operation.

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

The installation of the RTCC software is permanent and will operate 24/7.

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?

There will be no new physical objects or sensors collecting data as part of the RTCC software package. It integrates existing data sources into one centralized platform. Some of the data sources feeding into the RTCC do have physical equipment that is visible to the public, such as CCTV cameras.

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

Only authorized SPD, OPA, and users can access the RTCC software platform. Access to the systems/technology is limited to authorized personnel via password-protected login credentials.

Data extracted from the system/technology and entered into investigative files is securely inputted 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.

All use of the RTCC will be for law enforcement purposes only. Personal or inappropriate use or dissemination of information can result in internal discipline, termination, and penalties under federal or state law.

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

Other law enforcement agencies have used similar RTCC platforms to share information during serious incidents that span jurisdictions. For example, an active shooter in the City of Atlanta was apprehended in a neighboring county that was using the same RTCC platform as the City of Atlanta.

Any direct usage by a different jurisdiction will be consistent with SPD policy.

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

RTCC software will be accessed and used for serious incidents happening in real-time to provide information to patrol resources. It will also be used to provide a comprehensive picture of numerous SPD systems to investigators.

Data held in the RTCC system may only be viewed or extracted for legitimate law enforcement purposes, as governed by SPD Policy 12.050.

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.)?

RTCC software data will be stored within secure City of Seattle facilities under the administration of the Seattle Information Technology Department. If cloud storage is utilized, it will follow city security guidelines and only be accessible to outside parties as part of system maintenance and support only when authorized.

Various measures will be in place to protect data from unauthorized access.

- Data Encryption
- Access control mechanisms (meeting CJIS requirements*)
- Strict user permission settings
- Industry standard network security measures (meeting CJIS requirements)

The system will maintain audit logs of user and system actions. These logs will be maintained within the system and be accessible to those with permission to view. Logs will be accessible to the Office of Inspector General upon request.

* Criminal Justice Information Services (CJIS) Division of the Federal Bureau of Investigation (FBI) sets requirements for organizations that access or use criminal justice information. These requirements are referred to as "CJIS requirements" and are developed and audited for compliance by the FBI.

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

Any incident or multimedia data extracted from the system will be stored in a method compliant with the FBI's CJIS requirements. The specific details are vendor dependent, but could include either cloud storage or on-premise storage. The storage configuration may vary from vendor to vendor, but SPD expects similar industry standards when it comes to cloud storage and access controls.

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

The retention period for data stored by RTCC software will be 30 days, data will be overwritten after that retention period expires. Data associated with criminal investigations will be saved as evidence in SPD's digital evidence locker consistent with retention guidelines for evidence.

Audits from the OIG or other official auditors, will be allowed as needed.

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

Per SIR section 5.2, RTCC data collected without evidentiary value will be automatically purged by the system after 30 days.

SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a General Offense Report. Evidence is submitted to the Evidence Unit and associated with a specific GO Number and investigation.

All information must be gathered and recorded in a manner that is consistent with SPD Policy 6.060, such that it does not reasonably infringe upon "individual rights, liberties, and freedoms secured by the Constitution of the United States and of the State of Washington, including, among others, the freedom of speech, press, association and assembly; liberty of conscience; the exercise of religion; and the right to petition government for redress of grievances; or violate an individual's right to privacy."

All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

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

Unit supervisors are responsible for ensuring compliance with data retention requirements within SPD.

Additionally, any appropriate auditor, including the OIG, can audit for compliance at any time.

6.0 Data Sharing and Accuracy

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

Data obtained from the technology 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 or compiled by the RTCC software 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 to execute research and confidentiality agreements as provided by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the devices.

6.2 Why is data sharing necessary?

Data sharing is necessary for SPD to fulfill its mission of contributing to crime reduction by assisting in collecting evidence related to criminal activity as part of investigations, and to comply with legal requirements.

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

Yes ☒ No ☐

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

Law enforcement agencies receiving criminal history information are subject to the requirements of CFR Title 28, 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?

Sharing agreements must meet the standards reflected in SPD Policy 12.055. Law enforcement agencies receiving criminal history information are subject to the requirements of CFR Title 28, Part 20. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

Following Council approval of the SIR, SPD must seek Council approval for any material change to the purpose or manner in which the RTCC software platform may be used.

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

Real-time crime center software data comes from various SPD systems and is blended into one single view/location. Accuracy of data flows over APIs are checked at the point of development and monitored by system administrator and system logging thereafter. The system administrator is responsible for monitoring API versioning and change management to proactively plan and avoid issues. In addition, as data is being received and analyzed in the RTCC, specially trained individuals are reviewing and assessing the data and making judgments about the quality, accuracy, suitability, and value of the information being collected.

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?

Both the content and means of collection of information that may be utilized by the RTCC is regulated by the Fourth Amendment of the United States Constitution, Article I, Sec. 7 of the Washington State Constitution, case law interpreting the same, Washington's Privacy Act, RCW 9.73, CFR Title 28, Part 23, and Seattle's Intelligence Ordinance, SMC Chapter 14.12.

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 SPD employees receive Security Awareness Training (Level 2), and all employees also receive City Privacy Training.

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.

SMC 14.12 and SPD Policy 6.060 directs 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. The purpose of policy 6.060 is "to ensure that the collection and review of such information serves a legitimate law enforcement purpose and does not unreasonably infringe upon individual rights, liberties, and freedoms secured by the Constitution of the United States and of the State of Washington, including, among others, the freedom of speech, press, association and assembly; liberty of conscience; the exercise of religion; and the right to petition government for redress of grievances; or violate an individual's right to privacy." SPD would only document sexual preferences or practices, political or religious activities if it is related to an unlawful act occurring, for example; as seen in a child pornography investigation.

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. The policy states that "employees shall not make decisions or take actions that are influenced by bias, prejudice, or discriminatory intent. Law enforcement and investigative decisions must be based upon observable behavior or specific intelligence," as well as outlining specifics related to this area.

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?

As stated above, RTCC software integrates dispatch, camera, officer location, 911 calls, records management system, and other information into one platform. With the nature of data obtained through the RTCC, there is some risk that private information may be obtained about members of the public without their knowledge. This risk and those privacy risks outlined in 7.3 above are mitigated by legal requirements and auditing processes that allow for authorized auditors, including the Office of Inspector General, to inspect use and deployment of the RTCC software. Additionally, the Office of Police Accountability can conduct investigations of possible violations of City and SPD privacy-related policies and laws.

8.0 Monitoring and Enforcement

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

Sharing of digital evidence outside the department is primarily done through SPD's digital evidence management system. Records of when data was shared and who it is shared with is

noted in the system audit logs. Digital evidence shared outside of the digital evidence management system (e.g., using media such as DVDs, thumb drives, etc.) is done though SPD's Digital Forensic Unit, which logs requests.

Per SPD Policy 12.080, the Crime Records Unit is responsible to receive and record all requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

Any requests for public disclosure are logged by SPD's Public Disclosure Unit. Any action taken, and data released subsequently, is then tracked through the request log. Responses to Public Disclosure Requests, including responsive records provided to a requestor, are retained by SPD for two years after the request is completed.

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

The Office of Inspector General conducts independent audits of SPD as instructed by the City Council and by City ordinance.

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
Q3 2024	Q4 2024	$300,000	$0	$100,000	General Fund

Notes:

The SPD's 2024 budget includes $1.8 million for the use of CCTV/ALPR technologies. Since RTCC software integrates these technologies into one single "pane of glass" for effective use, SPD will use a portion of these funds for acquisition of the technology. At the time of writing, the procurement process has not yet been started, so the costs above are estimates.

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
TBD	TBD	TBD	TBD	TBD

Notes:

At the time of writing, the planning process has not yet been completed.

1.3 Cost savings potential through use of the technology

The use of RTCC software may help mitigate SPD's shortage of sworn staffing by more effectively deploying patrol resources to incidents and follow-up investigations. However, use of the RTCC software and the other related technologies being assessed does not necessarily correlate to direct cost savings.

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

No funding beyond city General Fund dollars has been identified for this technology.

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
Atlanta		Currently in use
Detroit		Currently in use
Mesa, AZ		Currently in use
Orange County, CA		Currently in use
Washington DC		Deployed February 2024

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

3.0 White Papers or Other Documents

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

Title	Publication	Link

Bureau of Justice Assistance RTCC Information		https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/RealTimeCrimeCenterInformation.pdf

Racial Equity Toolkit ("RET") and engagement for public comment worksheet

Purpose

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

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

In addition to completing the RET template sections below, the 2024 Council Budget Action SPD-900-A requested that the Executive, the Office for Civil Rights (OCR) and the Inspector General for Public Safety (OIG) co-prepare a Racial Equity Toolkit (RET) analysis for these technologies, pursuant to the process that the Executive has already created to comply with the Surveillance Ordinance. Please see Appendix B: Office for Civil Rights RET Analysis.

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?

Gun violence, human trafficking, and other persistent felony crimes are concentrated at specific geographic places in the city. This concentrated crime is often anchored at these places and requires a holistic crime-prevention strategy.

The Crime Prevention Technology pilot, including the RTCC, is one integrated component to this overall strategy of addressing this issue. These technologies will be coupled with police patrols, continued investments in community-based initiatives, enhanced lighting, and enhanced cleaning.

The technology will be used for the following purposes:

- Closed-Circuit (CCTV) camera systems will assist investigators in collecting evidence related to serious and violent crimes, including homicides, assaults, and other offenses. The CCTV system can aid investigators in identifying suspects, clearing the innocent, and removing deadly weapons from the street, thereby reducing the risk of harm to the public.
- Real-Time Crime Center (RTCC) software helps provide situational awareness to increase officers' and the public's safety and reactively investigate incidents. Having real-time, accurate information in one place helps increase the reliability of the location of victims and suspects, enabling quicker aid and safer apprehension. Having better visual and spatial suspect information will help reduce unnecessary stops by officers, focusing their efforts on verified locations and accurate descriptions.

Potential impacts on civil liberties include but are not limited to:

- Privacy concerns associated with surveillance of people, vehicles, and license plates in public places.
- Misuse of collected video and information/mission creep.
- Lack of transparency with the public on what is being done with recordings.
- Loss of personal autonomy with surveillance of an area.

To mitigate these potential community concerns, SPD will:

- Post signs indicating that police surveillance and video recordings are occurring.
- Notification of the technology being used will be shared with the neighborhoods where it is deployed through community meetings and active canvassing with street fliers.
- Ensure technology is being used for crimes related to gun violence, human trafficking, and other persistent crimes in the surveillance area.
- SPD will create a public-facing dashboard that will update frequently and report on the uses of the technologies, including areas where cameras are recording, and the resulting number of police actions, such as arrests, court-authorized warrants, recovery of stolen vehicles, or other law enforcement actions.
- CCTV technology will only monitor public places, such as sidewalks, streets, and parks.
- Recorded material from CCTV cameras or the compilation of data at the RTCC, will only be kept for 30 days unless it is evidence of criminal behavior, in which case it will be transferred to SPD's secure digital evidence storage system. ALPR data will be maintained for 90 days and then deleted unless it contains evidence of criminal behavior.
- Provide access to CCTV, ALPR, and SPD's Real Time Crime Center (RTCC) user and device logs to the Office of Inspector General (OIG) for compliance audits.
- The Office of the Inspector General will have full access to the RTCC operation.
- The Office of Police Accountability may conduct investigations of violations of SPD policies and laws related to privacy.

Additionally, the technologies will only be implemented once the City's surveillance ordinance requirements are met, and the City Council authorizes the use.

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. SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior and other accountability measures. This pilot will be data-informed and guided. It will terminate if data suggests the technology is ineffective. Utilizing the abilities of the Performance Analytics and Research Unit, the Seattle Police Department has a plan to actively manage performance measures reflecting the "total cost of ownership of public safety," Equity, Accountability, and Quality ("EAQ"), which includes measures of disparate impact and over policing. In addition to a robust *Continuous Intervention Assessment* designed to inform, in real-time, the active development of a safer and more effective, Evidence-Based Policing (EBP) competency, the EAQ program assures *just*

right policing is achieved with undue collateral harm.

It's worth noting that many factors can contribute to disparate impacts in policing, most of which occur early in a person's life, long before there is engagement with the police. For example, systems and policies that perpetuate poverty, the failure to provide children with the strong and fair start they deserve in the crucial birth-to-five years, inadequate public education, and a lack of economic opportunity can all contribute to disparate outcomes. In addition, family dynamics and peer pressure can also create negative outcomes. We recognize these factors and strive to do our part to mitigate them, but we can't expect our police officers by themselves to cure these contributory factors. However, we do expect our officers to do their jobs respectfully and fairly as they interact with community members.

These technologies are location-specific, with a place-based focus, meaning they will record people in a public place where the technologies are being used. This mitigating factor reduces, to an extent, the possible disparate impact of potential police actions.

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

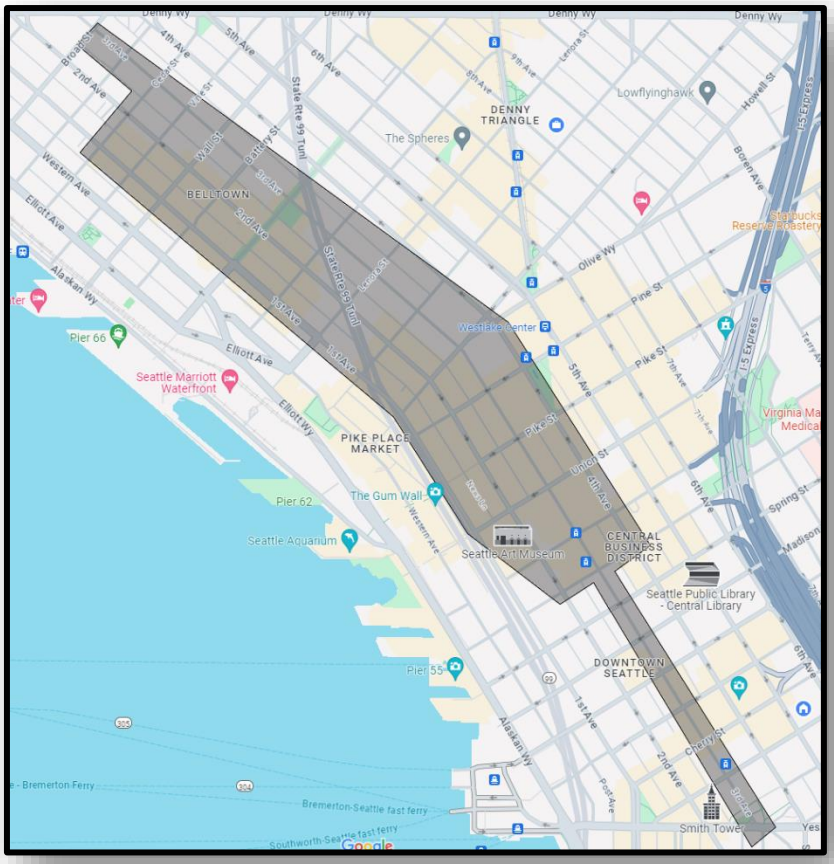
The following neighborhoods are being considered for deploying the CCTV technologies. Specific areas will be selected based on the data analysis indicating where gun violence, human trafficking, and persistent felony crimes are concentrated.

☐ all Seattle neighborhoods

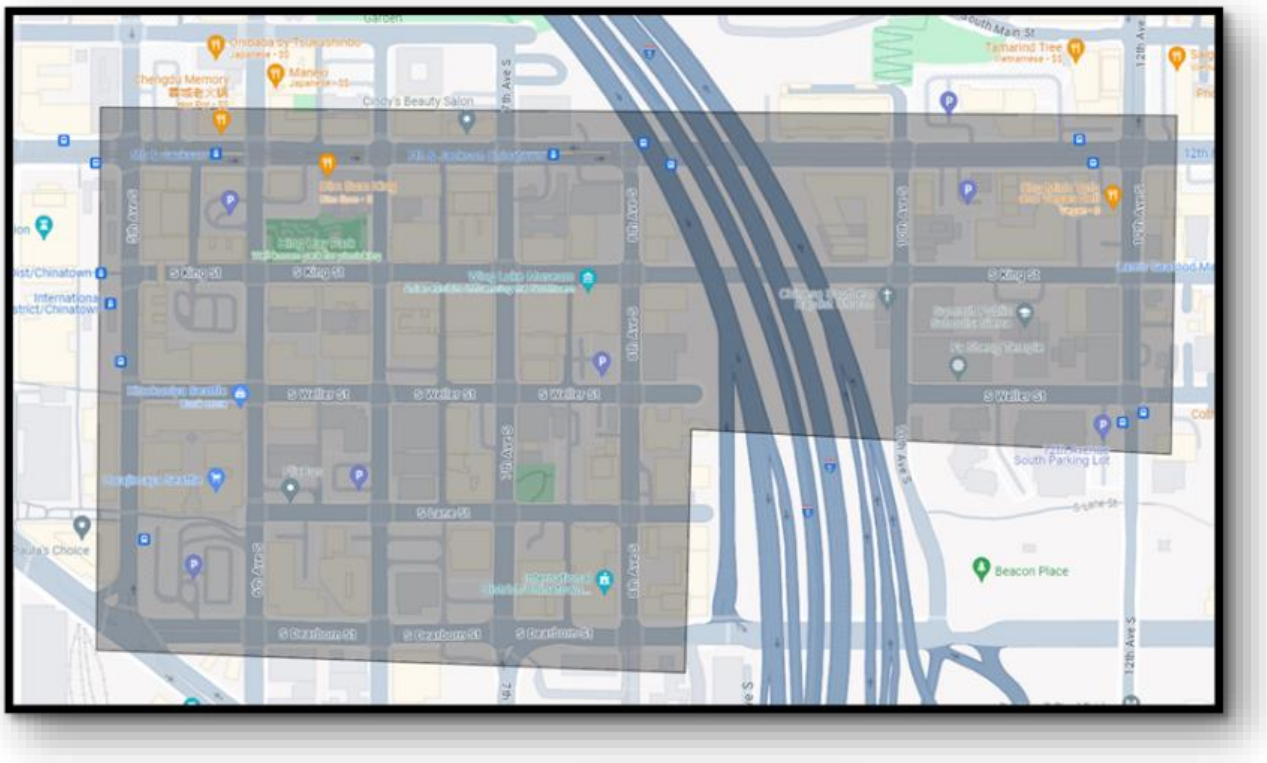
- ☒ **Aurora Ave N 85th to 145th**
- ☐ Ballard
- ☒ **Belltown**
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☒ **Chinatown/International District**
- ☐ Columbia City
- ☒ **Downtown Commercial Core**
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle) (Mutual Aid)
- ☐ Outside King County (Mutual Aid)

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

Downtown & Belltown Area *(Potential location)*



Chinatown-International District Area *(Potential)*



Aurora Avenue North Corridor
(Potential; Aurora Ave, 95th to 130th Streets)

1.4.1 What are the racial demographics of thos ea or impacted by these issues?

Race/Ethnicity	Aurora	Chinatown International District	Belltown	Downtown Commercial	Citywide
American Indian or Alaska Native	0.8%	0.7%	0.6%	1.1%	0.4%
Asian	14.0%	49.2%	30.4%	16.8%	16.9%
Black/African American	8.9%	8.6%	5.5%	11.1%	6.8%
Hispanic or Latino of Any Race	11.3%	7.6%	7.1%	8.3%	8.2%
Native Hawaiian or Pacific Islander	0.3%	0.2%	0.2%	0.3%	0.3%
Other	0.7%	0.7%	0.6%	0.7%	0.6%
Multiple Races	7.9%	5.8%	4.9%	5.6%	7.3%
White	56.2%	27.2%	50.8%	56.1%	59.5%

Source: U.S. Census Bureau Decennial Census; OPCD

Note: Geographical areas provided are 2020 Census Block Assignments of Urban Villages within the Downtown Urban Center, with the exception of Aurora. Aurora's boundaries are based on ½ mile buffer from Aurora between Meridian and Greenwood, and from 85th to 145th.

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?

CCTV will be deployed where crimes related to gun violence, human trafficking, and other persistent felony crimes are concentrated. SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as other accountability measures. This technology does not enhance the risks of racial or ethnicity-based bias.

These technologies are geographically focused on specific areas where gun violence, human trafficking, and other persistent felony crimes are concentrated. They are focused on individuals only if they are present in these areas.

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

Data from the technology may be shared outside SPD with 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.

Data may be made available to requesters under the Washington Public Records Act, Chapter 42.56 RCW ("PRA").

Data sharing has the potential to be a contributing factor to disparate impact on historically marginalized communities. To mitigate this possibility, SPD has established policies regarding disseminating data related to criminal prosecutions, Washington Public Records Act (Chapter 42.56 RCW), and authorized researchers. Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior.

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?

As with decisions around data sharing, data storage and data retention have similar potential for disparate impact on historically marginalized communities. CCTV will be deployed where crimes related to gun violence, human trafficking, and other persistent felony crimes are concentrated. Video from CCTVs will be stored for 30 days unless imagery is needed for investigations or to comply with legal requirements. Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, and other accountability measures.

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

The most important unintended possible negative consequence related to the implementation of CCTVs and the RTCC is the possibility that the civil rights of individuals may be compromised by unreasonable surveillance. To mitigate this risk, SPD is enacting a specific policy codifying the allowable circumstances under which SPD may utilize CCTVs and Real-Time Crime Center software. Access to user and device logs will be given to the OIG so they can audit the use of these technologies.

To prevent unintended outcomes, the City will develop and post signs in areas that are covered by the cameras' view to alert the public to their presence and use. Active canvassing in pilot locations and passing out street fliers will occur to further inform the public about the use of the technologies in the impacted neighborhoods. Additionally, the Office of the Inspector General will have access at any time to monitor and evaluate the use of these technologies. During the public outreach sessions described below, the City will listen to feedback from the public and provide responses during the technology review process.

The potential positive impact will be reduced serious crime concentrated in the locations where the technologies are deployed. If achieved, these reductions will create a safer environment for everyone who lives, works, plays, or visits these areas.

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.

A 4 Apple Learning Center, ACLU, Alliance for Pioneer Square, Amazon, Asian Counseling and Referral Services, Ballard BIA, Beacon Business Alliance, Belltown Community Council, Broadview/Bitter Lake CC, Build Lake City Together/Akin, Chief Seattle Club, Chinese Information Service Center, CID BIA, Crown Hill, Downtown Seattle Association, Dunn Lumber, Duwamish Valley Youth Corps, Epic Life Church, Ethiopian Community in Seattle, Ewing & Clark, For North Seattle, Friends of Little Saigon, Friends of Waterfront, Green Lake Community Center, Greenwood Community Center, Haller Lake Community Club, Home Depot Aurora, Korean Community Service Center, Licton Springs CC, Lowe's Aurora, Magnolia Chamber of Commerce, Matt Talbot Center, NAACP, North PCT Advisory Comm, Black Coffee NW, Phinney Neighborhood Association, Pike Place Market PDA, Pioneer Square Alliance, Jackson Place Community Council and Central Area Neighborhood District Council, PSQ Residence Council, Public Safety Council Chair, Queen Anne Block Watch Network, Queen Anne Community Council, Seattle Association, Seattle Chamber of Commerce, Seattle Chinatown-International District Preservation and Development Authority, Seattle Public Schools, Seniors in Action President, SoDo BIA, South Lake Union Chamber of Commerce, SPD African-American Council, Tecta America, U District BIA, Uptown Alliance, Urban Renaissance Group, Visit Seattle, VOCAL- WA, We R Seattle, WPAC, Yelser Terrace Community Council, and GSBA.

The Department of Neighborhoods, Human Services Department, and Office for Civil Rights were also asked to share with their community outreach list.

2.1 Scheduled public meeting(s).

Meeting notes, sign-in sheets, all comments received, and questions from the public included in Appendix C, D, E, F, and G.

Location	**Webex virtual meeting and in person option at the Bertha Knight Landes Room located on Floor 1 of City Hall (600 Fourth Avenue, Seattle, WA 98104)**
Time	February 12, 2024, 12:00 pm

Location	**Webex virtual meeting and in person option at a Community Center (details will be posted online shortly).**
Time	February 27, 2024, 6:00 pm

Additionally, the City convened 15 neighborhood-specific organizations meetings to discuss the technology and receive feedback and questions. See the list of organizations below:

- SPD's North, South, East, and West Precinct Advisory Councils
- NAACP
- Seattle Chamber of Commerce
- Greater Seattle Business Association (GSBA)
- Community Police Commission (CPC)
- African American Community Advisory Council
- East African Advisory Council
- Filipino Community of Seattle
- Emerald City Bible Fellowship Church
- Downtown public hearing
- Bitter Lake public hearing
- CID Community Safety Council (Including Friends of Little Saigon, CIDBIA, Seniors in Action etc.)
- For North Seattle
- ACLU
- Businesses and visitors along Aurora Ave North

3.0 Public Comment Analysis

This section will be completed after the public comment period has been completed on April 12, 2024.

3.1 Summary of Response Volume

Total responses to the public form (https://forms.office.com/g/yxJeiSh1JR): 754

Question	Responses
1) What concerns, if any, do you have about the use of this technology?	734
2) Do you have any additional concerns about the use of technology (in case you ran out of space in section one)	241
3) What value, if any, do you see in the use of this technology?	506
4) Do you have additional comments/questions re what value do you see in this technology?	149
5) What would you want City leadership to consider when making a decision about the use of this technology?	522

6) Do you have additional comments/considerations that leadership should take into account when making a decision about this technology?	185
7) Do you have any additional comments or questions?	145

8. OPTIONAL Demographic Question: Age Range

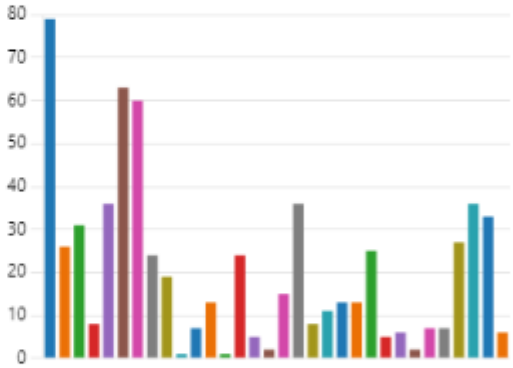
More Details

Prefer not to identify	68
Under 18	1
18 - 44	394
45 - 64	112
65+	63

9. OPTIONAL Demographic Question: Neighborhood

More Details

Prefer not to identify	79
Aurora Ave N 85th to 145th	26
Ballard	31
Belltown	8
Beacon Hill	36
Capitol Hill	63
Central District	60
Chinatown/International District	24
Columbia City	19
Delridge	1
Downtown Commercial Core	7
First Hill	13
Georgetown	1
Greenwood / Phinney	24
International District	5
Interbay	2
North	15
Northeast	36
Madison Park/ Madison Valley	8
Magnolia	11
Queen Anne	13
Rainier Beach	13
Ravenna / Laurelhurst	25
South Lake Union	5
Southeast	6
Southwest	2
South Park	7
Uptown	7
Wallingford / Fremont	27
West Seattle	36
King County	33
Outside King County	6



10. OPTIONAL Demographic Question: Gender

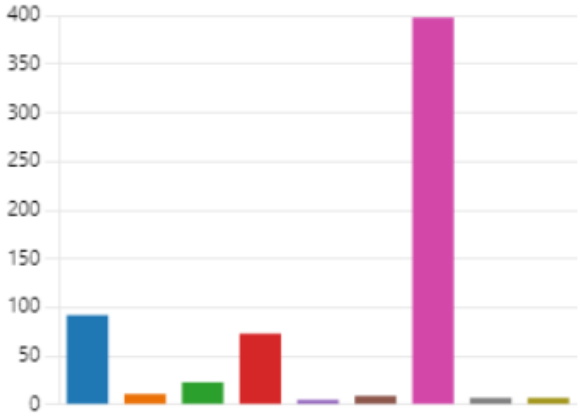
More Details

Prefer not to say	108
Woman	249
Man	172
Non-binary	61

11. OPTIONAL Demographic Question: Which race (s) / ethnicity (or ethnicities) do you identify as

More Details

Prefer not to identify	92
Black / African American	11
Hispanic / Latino	23
Asian / Asian American	73
Native Hawaiian or Pacific Island...	5
Indigenous	9
White or Caucasian	398
Another race/ethnicity	7
Other	7



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

Please see Appendix E.

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

Please see Appendix E.

3.4 Question Three: What would you want City leadership to consider when making a decision about the use of this technology?

Please see Appendix E.

3.5 Question Four: General response to the technology.

Please see Appendix E.

3.5 General Surveillance Comments

These are comments received that are not particular to any technology currently under review.

Please see Appendix E.

4.0 Response to Public Comments

This section will be completed after the public comment period has been completed on April 12, 2024.

4.1 How will you address the concerns that have been identified by the public?

Concerns that have been raised through public comment and engagement will be addressed in SPD policy. SPD is developing an omnibus surveillance technology policy to provide general guidance on several topics, including value and equity statements for technology use, an explanation of the surveillance ordinance requirements, internal processes for technology approval and acquisition, general tracking metrics for surveillance technologies, retention requirements and limitations, and general use requirements for surveillance technologies. Additionally, issues and guidance unique to specific surveillance technologies would be included for each technology. As such, the department will create a policy section for RTCC.

5.0 Equity Annual Reporting

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

The goals of this project are:

1. Reduction in gun violence, human trafficking, and other persistent felony crimes in specific geographic areas where the technologies are deployed.
2. Reduction in 911 calls in the pilot area.
3. To measure and minimize crime displacement outside of the pilot area.
4. Improved police response times, crime clearance rates, and community satisfaction measures.

We will also report the rate of arrests and prosecutions that occur because of the pilot and any negative unintended consequences, such as over or under policing.

The Seattle Police Department, utilizing the Data Analytics Team and working with the Office of the Inspector General, will monitor these objectives and the outcomes closely to watch for disparate impacts. If data analysis shows any disparate impacts, SPD will work with the the Office of the Inspector General to make the needed changes to address these impacts.

Further, the City will retain outside academic subject matter experts to develop and manage an evaluation plan related to the use of the technologies.

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

From: The Community Surveillance Working Group

To: Executive & Seattle City Council

Date: 07/26/2024

RE: Privacy and Civil Liberties Impact Assessment for CCTV and RTCC

Purpose

This section shall be completed after public engagement has concluded and the department has completed the racial equity toolkit section. The Privacy and Civil Liberties Impact 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 submission 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."

Executive Summary

Seattle IT provided the Working Group with the finalized Surveillance Impact Report (SIR) on June 4th, 2024, with an initial submission deadline of July 16th, 2024. Subsequently, the Working Group requested a two-week extension to July 30th, 2024. This document is the Working Group's Privacy and Civil Liberties Impact Assessment for both Closed Circuit Television (CCTV) and Real Time Crime Center (RTCC), given that they are two technologies that rely closely on each other in practice, as set forth in SMC 14.18.080(B)(1), which we provide for inclusion in the final SIR submitted to City Council.

The Working Group conducted a review of all provided materials within the SIR, including the SIR proposal from Seattle Police Department, letters from Seattle community organizations, and public comments. After reviewing the information, a majority of the working group is unsupportive of any pilot deployment of these two technologies as described in the SIRs. The amount and urgency of the concerns and outstanding questions both warrant pause on pilot deployment. Of the six members considering the CCTV and RTCC pilots, three are explicitly 'against', two are 'unstated, with broad concern', and one is 'for CCTV within stated pilot, and for RTCC'. This sentiment reflects the high degree of apprehension expressed by a vast majority of the public's comments. The City received a substantial number of public comments, both in-person and submitted electronically, regarding the potential misuse of these technologies. These comments were overwhelmingly negative and voiced a serious concern and lack of trust within the community as a whole of the Seattle Police Department's plan to expand the use of surveillance technology. These views were not unanimous, as there was a small number of commenters who were supportive of the pilots, primarily citing the impacts of gun crimes in their communities. Yet, considering our assessment as well as input from public comment and community organizations, the working group believes that going forward with these acquisitions may serve to further erode with a significant portion the public's trust in SPD and negatively affect community relations.

This document provides the Working Group's concerns, recommendations, and outstanding questions regarding the consideration of CCTV and RTCC technology usage by SPD. Our assessment focuses on the following major issues, for which we provide more detail in the body of the document:

1. **Possible infringements on reasonable expectation of protection from warrantless "unreasonable search" creating potential conflicts with The Fourth Amendment.**
2. **Possible impact on First Amendment Right that might deter public engagement (peaceful protest, assembly, etc.)**
3. **Risk of disparate impact of surveillance technologies on minority communities within Seattle.**
4. **Apparent lack of public input for definition of deployment areas, specifically regarding proximity to sensitive public resources including open meeting spaces and medical centers.**
5. **Lack of specifics as to the sourcing and capabilities of the proposed technologies in both CCTV and RTCC SIRs, reflecting broader privacy concerns.**
6. **Concern over possible slippery slope regarding the use of different types of artificial intelligence to monitor personally identifiable aspects of individuals.**
7. **Privacy, quality, and governance risks presented by the inclusion of third-party CCTV devices.**

8. **Lack of clarity around the sworn/civilian reviewers monitoring the video streams, and the data retention policies of that data.**
9. **The need for better definition of justification/success metrics and concrete timelines by which to measure them.**
10. **Lack of clarity on policy areas that the SIR relies upon for future "general guidance" such as the Omnibus Surveillance Policy.**
11. **Lack of clarity in oversight structure, specifically regarding the Office of the Inspector General and its ability to audit.**
12. **Lack of clearly defined scope in the form of specific crime definitions and geographic reach.**

We thank the Public Safety Committee Chair, Seattle CTO, and Seattle City Council for their time and consideration of this Civil Liberties Assessment as a crucial piece of the SIR process.

Sincerely,

René Peters (Position #1, Co-Chair) Kayleigh

McNiel (Position #2, Co-Chair) Wendy

Novotne (Position #3)

John Yun-Kuang Chen (Position #4)

Carolyn Riley-Payne (Position #5) Alex

Maestretti (Position #7)

Key Concerns

1. **Possible infringements on reasonable expectation of protection from warrantless "unreasonable search" creating potential conflicts with The Fourth Amendment.**

Per the Fourth Amendment, citizens have a right to be free from unreasonable, warrantless searches when they have a reasonable expectation of privacy. The Supreme Court of the US has held that citizens have a privacy interest in the whole of their movements, including those in public (See: U.S. v. Carpenter, 585 U.S. at 310, 138 S.Ct. 2206). We consider the question "How could CCTV impact these rights?"

If the integration of live-monitored CCTV surveillance feeds (including use with RTCC) would result in the tracking of individuals as they move throughout areas of the City, it could raise constitutional concerns in light of recent Fourth Amendment case law establishing that people have a reasonable expectation of privacy to their movements in public. See Leaders of a Beautiful Struggle v. Baltimore and U.S. v. Carpenter.

In Leaders of a Beautiful Struggle, the Fourth Circuit Court of Appeal, sitting en banc (all judges present), ruled that the Baltimore Police Department's (BPD) aerial surveillance program, which included the surveillance of Baltimore residents movements, violated the Fourth Amendment (Leaders of a Beautiful Struggle v. Baltimore Police Dep't, 2 F.4th 330, 341 [4th Cir. 2021]). BPD contracted with a private company to pilot a surveillance program aimed at combating high rates of homicide and violent crime. The pilot involved 3rd party planes equipped with powerful
wide-angle cameras flying over the entire city of Baltimore during 12 hours of daylight. The Fourth Circuit found that this persistent surveillance of outdoor movements invaded people's reasonable expectation of privacy, explaining that "allowing the police to wield this power unchecked is anathema to the values enshrined in our Fourth Amendment."

The Fourth Circuit based its decision on the U.S. Supreme Court's 2018 ruling in U.S. v. Carpenter, which held that it was unconstitutional for law enforcement to obtain a person's cell phone location data without a warrant because such information can be used to track the "whole of [a person's] physical movements," creating an "intimate window" into their life, including their "familial, political, professional, religious, and sexual associations."

While the technology at issue in both these cases is notably different than what SPD seeks to utilize here, the lack of clarity in the SIRs regarding the use of these proposed technologies raises concerns that such surveillance could reveal the intimate details of a person's life by tracking their movements throughout the City. As such, more review of this issue is warranted.

2. **Possible impact on First Amendment Right that might deter public engagement (peaceful protest, assembly, etc.)**

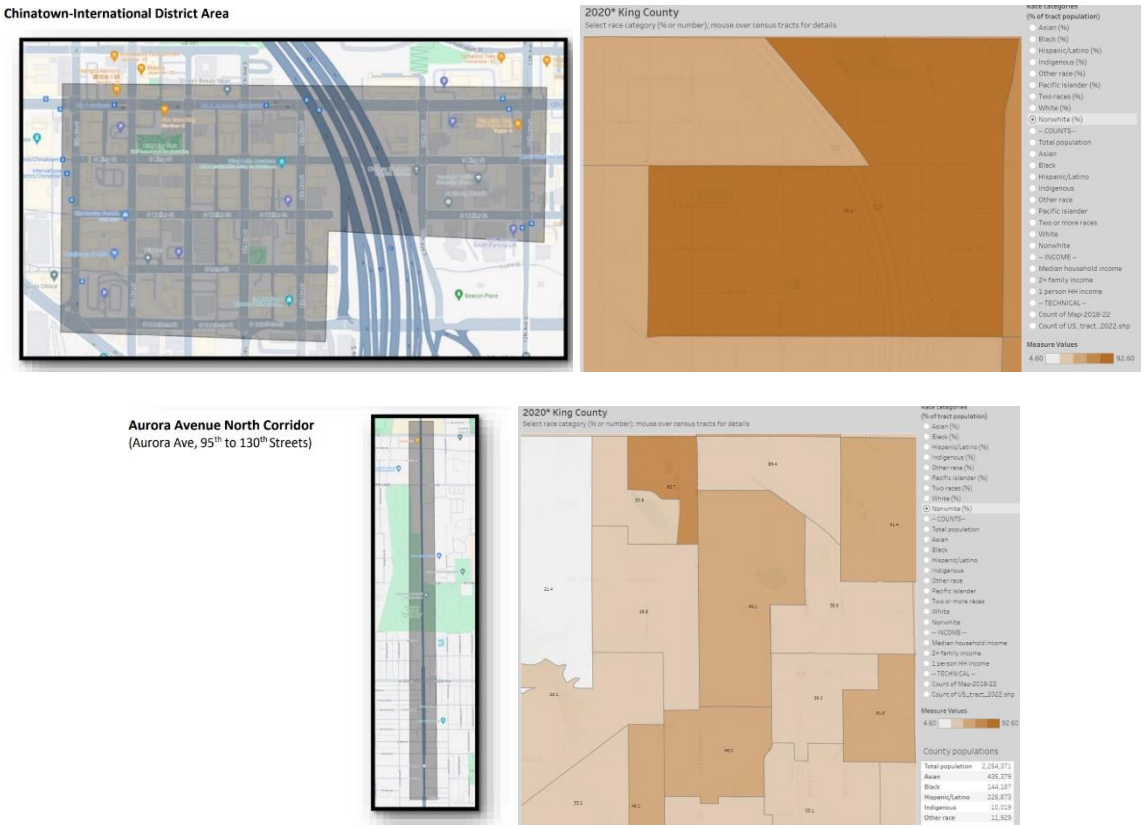
The working group believes there may be similar concerns with SPD's deployment if the true potential and use of this technology results in the tracking of individual's movements throughout the City. Furthermore, the use of CCTV surveillance, coupled with a RTCC's enhanced
license-plate readers, could be used to target protesters, deterring Seattle residents from exercising their First Amendment right to peacefully assemble and protest. Notably, the eastern

edge of the proposed "Downtown & Belltown Area" surveillance zone includes Westlake Park, which is frequently utilized as a public gathering space for protests, demonstrations, and other political and cultural events.

3. Risk of disparate impact of surveillance technologies on minority communities within Seattle.

The use of surveillance technologies inherently opens the door for outsized impact on immigrant, POC, and minority communities. These impacts can come to bear via inaccuracies in the technology itself (heightened statistics of incorrect recognition of subjects of color are well-documented), and simply by increasing the likelihood that citizens of color will be exposed to implicit biases during interactions with law enforcement or exposure to the criminal justice system.

With regard to the CCTV SIR, the placement of the proposed surveillance zones themselves may serve to put minority communities at higher risk. Per 2020 Census data organized by the University of Washington, the CCTV deployment areas have significant overlap with some of the highest-percentage minority population centers in King County. Virtually the entire Chinatown-International District zone comprises an area with a 77% non-white and 57% Asian population. The Downtown & Belltown zone overlaps areas with non-white populations as high as 58% and Black populations as high as 12%. The Aurora Avenue North Corridor zone overlaps areas of 49% and 63% non-white population, as well as some of the highest percentages of Hispanic/Latino population in the metro area (as much as 16%). This increases the chances that communities of color, immigrant community members, and other marginalized groups will be impacted by these technologies.



It is concerning that SPD does not substantially address this within its SIR, positing that "these technologies are location-specific, with a place-based focus, meaning they will record people who choose to be in a public place where the technologies are being used. This mitigating factor reduces, to an extent, the possible disparate impact of potential police actions." People living in these communities, especially those who are unhoused, do not have a choice as to whether they are in a public place while going about their daily lives. Furthermore, when considering the City Council-defined inclusion criteria in the Racial Equity Toolkit, which expressly aims to "highlight and mitigate any impacts on racial equity from the adoption and the use of the technology", SPD did not consider that the criteria "The technology disparately impacts disadvantaged groups" was met. By virtue of the coverage information above, as well as many of the other themes in this assessment, it is troubling that SPD appears to assert that there is no uneven impact with the proposed technology.

The working group expresses concern for collection of data on the "un-involved public" who are not a part of any in-progress or perpetrated criminal activity. It is mentioned in the SIR that "minors (children) are present in public spaces, SPD may record video with children present, however, because disclosure of images of any minor is presumed highly offensive, images of an identifiable minor are almost always exempt from public disclosure". Yet, SPD provides no information on how a public disclosure exemption would work. First is the question of how confirmation of a minor's presence within video data would be accomplished – without any stated age target, presumably measuring whether or not a member of the public is below the age of 18. It is already well documented that children of color are often perceived to be older than their true age, creating an area of concern with this prospect. In that same vein, there is plenty of research on how image-based AI recognition misidentifies minority subjects at higher rates.

4. **Apparent lack of public input for definition of deployment areas, and notification of technology presence, specifically regarding proximity to sensitive public resources including open meeting spaces and medical centers.**

Public engagement is a key gateway leading to this working group to render a proper Privacy & Civil Liberties Assessment. It is a broad concern that the evaluation and implementation of this technology requires more public input in crucial areas, including but not limited to:

- How areas of coverage are determined.
- Identifying sensitive community resources, such as public meeting areas and medical centers.
- Communication of surveillance technology presence.

In the SIR, SPD notes a number of different possible public areas that they seek to deploy the technology, including "places like sidewalks, streets, parks" and "other public areas". The verbiage around what constitutes an appropriate public space is vague, and furthermore, the definition of "public" is subjective and could differ between SPD and community members. The lack of a definitive list of acceptable spaces for deployment risks unstructured reach for SPD to make their own determinations. The creation of an exhaustive list of accepted location types,

that is reviewed collaboratively with communities, and clearly published, would be a measure that could increase public understanding and trust.

On the matter of coverage area determination, SPD notes in the SIR that "Specific areas will be selected based on the data analysis indicating where gun violence, human trafficking, and persistent felony crimes are concentrated." Yet, the methodology behind matching crime data to hyper-localized boundaries is very opaque. These data were not presented to the working group in any of the SIR documentation.

It is also apparent that there were missed opportunities to engage the public during the formulation of the surveillance areas. This presents an issue, as these areas defined by crime statistics include sensitive community resources, such as the aforementioned Westlake Park. Another example lies near the "Aurora Avenue North Corridor", where the surveillance area directly borders the Planned Parenthood Northgate Health Center. This puts citizens seeking critical health care services directly in the line of fire of surveillance, when there is a long and well-documented history of tracking, protests, and violence against these health centers. A quick search on the effective range of some models of PTZ cameras, as referenced in the SIR, shows that they are able to "identify license plates and people from ~140m away" and that there "is a sufficient level of detail to positively identify" a person (Model example: Uniview IPC94144SFW-X25-F40C). Thus, there is warranted-concern that a CCTV pilot deployed in this area could not only be used to identify vehicles but even individuals seeking healthcare services at Planned Parenthood Northgate Health Center.

With earlier communication and review of these proposed pilot zones with the public, there may have been opportunities to flag these sensitive overlaps, and for SPD to determine coverage areas that avoided them. As it stands, this serves as another potential disparate impact to a BIPOC and marginalized community.

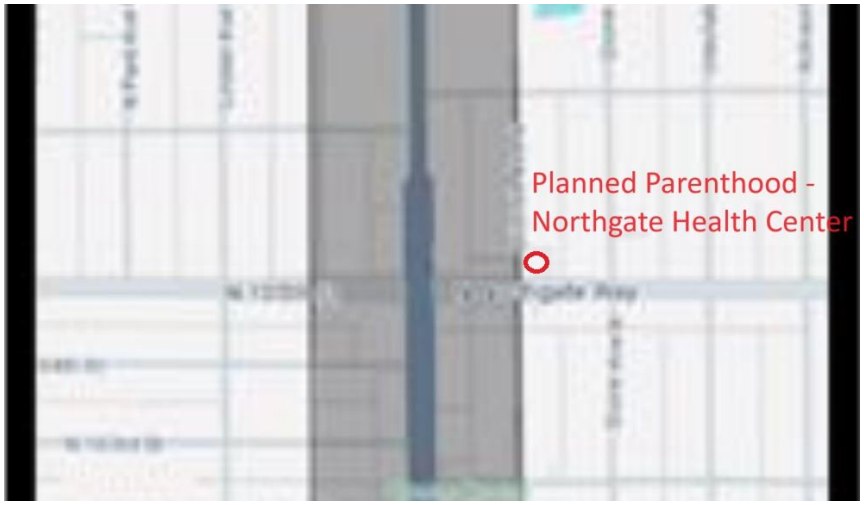
Another area of concern with this SIR is that there is not a detailed plan for reasonable notification of CCTV usage for the public. The basic requirement should be that there should be some type of signage, visual cue, or other easily-understood signal that 1) cameras are present, and 2) they are operational/being actively operated. The SIR states that "The cameras themselves will be visible to the public, and signs will be placed to alert the public to their presence and use". Yet, this gives way to a number of other considerations. In the case of a visual/posted sign or flier, what is the correct verbiage to accurately describe the scope of the camera usage? Signs and fliers posted in English will not be sufficient to notify non-English speakers that they are in a surveillance area. This is especially concerning given the fact that the

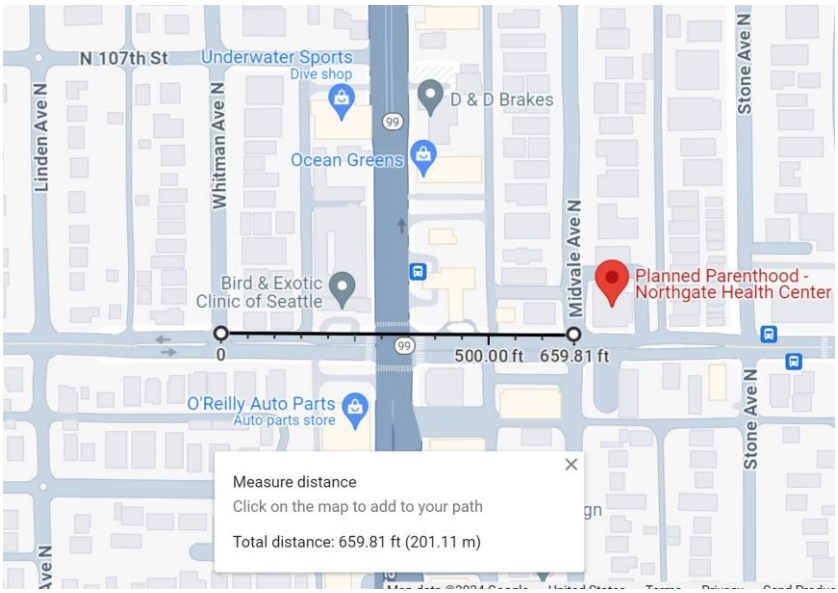
areas that have been chosen for consideration are home to a high concentration of many immigrant communities with a high amount of non-English speakers or citizens who are non-EFL. Signs may also have very low noticeability after daylight hours – understanding if the CCTV cameras themselves have lights to indicate their placement to passers by would be helpful, but the SIR doesn't contain information on any specific SKU or model. Neither signage nor lighting would be an effective notification for somebody who has a visual impairment, or is blind. As it stands, this too serves as another potential disparate risk to Seattle's BIPOC and differently-abled communities.

5. **Lack of specifics as to the sourcing and capabilities of the proposed technologies in both CCTV and RTCC SIRs, reflecting broader privacy concerns.**

The SIR describes that cameras "can range from simple fixed cameras to more sophisticated cameras with pan-tilt-zoom (PTZ) as well as other capabilities (infrared night vision, high definition imaging, etc.)", but it is difficult to render a full assessment from a technology standpoint when there is not specific information on the vendors, models, and specifications of the devices in question.

Providing information on the vendor(s) would allow the working group to understand more about their previous history of deployments, clients, partners, etc. Providing information about the specific models of cameras (product names, SKU #'s) would allow the working group to consider the full range of capabilities such as maximum viewing/zoom range, image fidelity (ability to discern individuals/objects at distance), and visibility (chassis, operation lights, etc). The SIR provides maps of the surveillance coverage areas, and while it is unstated, we assume that this represents the potential physical placement of the cameras and not the viewable range of the cameras. The width of the Aurora Avenue North Corridor (pictured below) measures roughly 650ft at the intersection of Aurora and 105th. We have already established above that some camera models have effective ranges of over 140m (about 450ft). The true coverage of the zones should reflect the possible placement of cameras, including the effective camera range (see picture of 105th and Aurora, camera ranges if placed on the edge of the shaded area represented by orange boxes). For this, the specifications of the cameras need to be well-understood. This underlines why the full technical specifications of all involved technologies would be very helpful context to have in-hand before considering a pilot rollout – the inability to gauge the actual footprint of the technology poses a public risk.


Planned Parenthood -
Northgate Health Center


N 107th St
Underwater Sports
Dive shop
D & D Brakes
Ocean Greens
Linden Ave N
Whitman Ave N
Midvale Ave N
Stone Ave N
Bird & Exotic
Clinic of Seattle
Planned Parenthood -
Northgate Health Center
0
500.00 ft
659.81 ft
O'Reilly Auto Parts
Auto parts store
Measure distance
Click on the map to add to your path
Total distance: 659.81 ft (201.11 m)


Planned Parenthood -
Northgate Health Center

Another reason why it's important to have vendor information in-hand prior to evaluating the SIRs is that, once installed, each vendor may have a different process of updating functionalities and software. SPD should have a published protocol on how to manage this. If a vendor rolls out new features/functions that need to be physically installed, or can be remotely installed via a software update, should that new functionality trigger a new SIR loop? There may be a risk that software updates could automatically roll in an unapproved functionality. This is another area that risks an uncontrolled expansion of surveillance reach.

Possible evidentiary issues are unclear due to lack of specifics surrounding the CCTV camera capabilities; if these cameras record sound as well as video, they may not be admissible under the Washington Privacy Act without a much clearer warning than the posted signed. See Lewis v. DOL (2006). In *Lewis*, the WA Supreme Court held that the WA Privacy Act RCW 9.73 requires that officers inform detainees that the officers are recording their conversation. Courts exclude police body cam and ICV videos when the audio and video recording admonishment is not clearly captured on the video. While *Lewis* was specific to in-car video recordings of interactions with law enforcement during traffic stops, the admonishment requirement could be applied to police-operated CCTV cameras that record sound. As such, if a court finds the posted signs are inefficient to notify individuals that their conversations are being recorded, these videos could be excluded.

The worry is that lack of specifics in these areas means that acceptance of the SIR as written may also constitute somewhat of a 'blank check' when it comes to SPD/the City purchasing devices with advanced surveillance capabilities. Information on vendors and models should be made publicly available with opportunity to provide input, for transparency.

6. Concern over possible slippery slope regarding the use of different types of artificial intelligence to monitor personally identifiable aspects of individuals.

The SIRs contain multiple elements of ambiguity with regards to exactly which AI tools ("Edge-Based Analytics capabilities") can be used on raw CCTV footage during and after recording. While the SIR mentions that "SPD will not use AI facial recognition tools", it also notes that other aspects of AI may be used such as: "object recognition (e.g., identifying vehicles or people by the clothing they are wearing or items they may be carrying)" as well as "in-application video analytics that use machine learned algorithms to analyze camera feeds and, using object recognition, locate specific items, people based on clothing, or vehicles based on description"

Clearly, there is a wide range of items that can be recognized, tagged, and logged with this technology. The ability to track personally identifiable aspects of individuals is an evident concern, but also concerning is that the verbiage of the SIR does not provide clarity on if there is a definitive list of specific targets of analysis, as well as assurance that other items won't be added in the future. In a February community meeting, SPD said that it "would not use any biometric identification tools", but without a publicly-available list of analysis types for accountability, there is concern that other types of AI analysis may be implemented without formal approval cycles, such as a tool that could hone in on a person's height/weight measurements, or gait patterns as they move through public spaces.

Additionally, due to Washington's public disclosure laws, bad actors could access information about

community members through Public Disclosure Requests (PDRs) for the CCTV video. This system could potentially be misused by abusers exposing victims of gender-based violence to further harm, harassment and stalking. Undocumented community members may be targeted by federal agencies seeking a work-around to Seattle's policy of being a "sanctuary city." Those seeking safe reproductive health care could be targeted by out-of-state agencies or actors seeking to harness CCTV footage as evidence against them in states which may soon criminalize reproductive health care.

7. Privacy, quality, and governance risks presented by the inclusion of third-party CCTV devices.

The working group flags a significant risk to civil liberties posed by third-party involvement in camera deployment. The inclusion of these devices risks opening a "Pandora's box" of uncontained expansion of CCTV coverage, and the SIR does not provide a sufficient risk mitigation plan for their implementation.

Similar to the problem of not understanding which vendors SPD would plan to purchase camera equipment from, there is even less control on what vendors third parties implement in their own respects. Many of these parties have had different models of cameras installed for short and long term operation at the time of this assessment. When evidence created by these cameras would go on to be used in criminal investigations, it is extremely important to establish a baseline or range for which cameras are acceptable. Differences in quality can be the difference between a correct identification and a mistaken identification – the difficulty that would come with enforcing a uniform standard across third-party cameras makes their integration problematic. There is no understanding of how SPD would logistically integrate a third-party camera into their system, and how they would make sure that the data transfers are done in a secure manner that can be maintained. SPD does not provide any information as to how many third party cameras that they would aim to integrate (whether it be a small amount to test if they can be integrated correctly, or a ceiling on how many they would integrate). There is no established way for accountability parties such as the OIG to interact with entities that provide access to their third-party cameras.

This risk is pronounced due to the fact that even with proposed SPD-owned CCTV cameras, the general policy for their use is incomplete, leaving no way to determine that the third-party feeds meet standards (quality inconsistency, data storage inconsistency, placement and notification inconsistency, etc). The working group thus broadly feels that inclusion of third party cameras is inappropriate, especially for a pilot stage rollout.

8. Lack of clarity around the sworn/civilian reviewers monitoring the video streams, and the data retention policies of that data.

With regard to the people reviewing the CCTV/RTCC data, there were a number of concerns surrounding privacy policies and access accountability. The SIR notes that "only authorized/trained SPD and OIG personnel will have direct access to the CCTV system" but there is a need for better understanding of what the qualifications to become authorized (if different than simply being an SPD officer or OIG member), as well as details about the training that these individuals undergo. Clarity on what types of training need to be completed, and at what frequency, would help to match areas of concern with proficiencies that the training aims to provide. The RTCC SIR notes that "The vision is for SPD to staff a real-time crime center with a

combination of sworn officers and civilian staff, eventually transitioning to a more civilian-staffed model". Thus, there is a need to understand any differences between training that sworn staff and civilian staff receive. What are the qualifications of civilian staff to gain access to information, and do they need to clear a higher bar to have access due to the fact that they do not have the ability to enforce the law? Will they need to complete background checks? It is important that standards such as SPD Policy 12.050 and Security Awareness Training (and Level 1, Level 2, etc.) be clearly explained and understood in the context of AI technology.

The methodology behind how individuals access CCTV and RTCC systems is also left relatively opaque within the SIRs. SPD Policy 12.050 appears to provide some guidance on user logs and query, but any pilot would need to be abundantly sure that access protocols such as proper authentication, time-logging for searches, types of searches, etc. are clearly collected and top line data shared with the public.

Data retention time is another area of concern. There are apparent mismatches between the retention time for data. Retention time is stated as of 30 days for "dispatch, CCTVs, officer location, 911 calls, records management systems (RMS), ALPR, geographic information systems (GIS), and other information systems" at one point in the RTCC SIR while another part of the same document states that "ALPR data will be maintained for 90 days". The working group also expressed concern around the 30 day retention time itself, and would prefer for there to be a shorter retention time to minimize exposure to possible bad actors or misuse. A shorter retention period would have a range of positive impacts for privacy - from reducing risk of inadvertent disclosure, to forcing a level of priority in capturing evidence only for the most serious infractions.

All in all, surveillance of this kind could enable police to track the movement of individuals as they go about their daily lives, exposing such intimate details as where they live, where they work, what stores they shop, what parks they take their children to, and who they engage with in the community. Once this data is collected, there is risk that it would be misused to target individuals who may not have been on law enforcement's radar otherwise. Clear, specific, publicly available standards are needed to limit the misapplication of the technology. These policies must be constantly reevaluated and improved as time goes on.

9. The need for better definition of justification/success metrics, concrete timelines by which to measure them, and public transparency about collected data.

The SIR lays out three main improvement themes: deterrence, response, and investigation.

- With regard to deterrence, the assertion that the presence of CCTV will deter violent and persistent felony crimes in the surveilled areas is dubious. There is no information to suggest a strong linkage between video footage used as evidence and metrics such as: correctly identified suspects, convictions, how often footage is accepted as evidence in trials. SIR-mentioned study results do not demonstrate effectiveness of cameras:
  - The Fayetteville 2023 study points to a moderate clearance increase

- The Dallas study concludes that implementation is not cost-effective for clearance rate increase (limited to thefts, not violent felonies)
- The 2019 New York study points to a significant-to-modest decrease in crime, but specifically for crime in residential areas and car parking properties. It also warns that cameras "should not be used as a standalone crime prevention measure"

Many, if not all, of the currently proposed areas currently have privately owned and city-owned cameras already. The SIR documentation lacks strong metrics and outcomes to show that either currently in-place cameras or proposed cameras have provided/will provide enough positive deterrence, response, and investigation improvements to justify their installation.

- With regard to response, the assertion is that CCTV will allow responders to more effectively identify perpetrators, secure the scene, and bring resources to bear (medical, etc). This assessment has already underlined concerns such as recognizing and quantifying the risk of misidentification (which has both a higher likelihood and an outsized impact in communities of color).
- With regard to investigation, the assertion is that detectives will be able to ID suspects, and prosecutors will be able to use CCTV as evidence to secure convictions. This is again a dubious assertion without data points such as: number of pieces of evidence retained, amount of video evidence used in prosecutions, rate of successful convictions or pleas compared to base rate.

Another layer of critical public visibility that the SIR does not explain in detail is publicly-visible data on usage and access. In the RTCC SIR, SPD notes that "SPD will create a public-facing dashboard that will update frequently and report on the uses of the technologies, including areas where cameras are recording, and the resulting number of police actions, such as arrests, court-authorized warrants, recovery of stolen vehicles, or other law enforcement actions" As part of the SIR process, it would have been useful if SPD had presented prototypes for what such a dashboard would look like, and provide information on exactly how members of the public would access them (what city website would this dashboard be accessible from?). Furthermore, in the spirit of public transparency, any CCTV stream should be publicly accessible. An example of such a setup exists on the WSDOT real-time cameras webpage, which shows camera views on a set refresh rate such as 2 or 5 minutes. As it stands in the submitted SIRs, the lack of deliberate and well-defined measures to improve data and collection visibility puts any Data Analytics Team/City Auditor in a poor position to report for things like the annual equity assessment, and would broadly undercut public trust.

Timeframe is another crucial aspect to any pilot, and it appears that the SIRs may not provide a clear mechanism for the pilot to end. The CCTV SIR states that "outside academic subject matter experts will be retained to design and manage an evaluation plan with an assessment at the end of one year and another at the end of two", but this in itself may not address any go/no-go mechanism behind the assessments. This Civil Liberties Assessment touches on the need for very clear metrics and understanding of how they will be measured. So too must there be clear actions at each checkpoint in the pilot deployment. Specifically, what are the actions that will

occur if not met, such as uninstall/decommissioning of the technology? Furthermore, who will be the "outside academic experts", what will their areas of expertise be, and how will the public be able to input on the formation of that review group? The working group flags the need to verify and ensure a clear endpoint for any pilot, such that initiating a pilot won't allow indefinite usage and/or expansion without a built-in control.

10. **Lack of clarity on policy areas that the SIR relies upon for future "general guidance" such as the Omnibus Surveillance Policy.**

Another concern is the lack of a sound policy that ensures compliance with the parameters of the pilot programs in question. Approval of the use of these technologies without first establishing a policy governing their use and operation poses substantial risk that they be misused to compromise individual rights and liberties of Seattle community members. While drafting such policies is likely time consuming, their absence only adds to the concern voiced by many in the community that these acquisition requests are being rushed through without proper diligence and community input.

Currently the SIR notes the following regarding governing policy:

"SPD is developing an omnibus surveillance technology policy to provide general guidance on several topics, including value and equity statements for technology use, an explanation of the surveillance ordinance requirements, internal processes for technology approval and acquisition, general tracking metrics for surveillance technologies, retention requirements and limitations, and general use requirements for surveillance technologies. Additionally, issues and guidance unique to specific surveillance technologies would be included for each technology. As such, the department will create a policy section for each surveillance technology, including those proposed here."

It is difficult for the working group to render an informed opinion on the true civil liberties impact of these technologies when the core governance is incomplete. Between the two SIRs, SPD refers to the to-be-written omnibus policy seven individual times for questions relating to 1) processes required prior to technology use/access, 2) legal standards that must be met before the project/technology is used, 3) addressing concerns from the public, and 4) potential unintended consequences and steps to take to ensure that these consequences won't occur.
Each of these questions is critical for understanding the scope of controls behind the pilots, and the protocols to measure and respond to their impacts to the community. Without an understanding of the timing of the omnibus policy rollout, the protections it puts in place, who is inputting, and how the community has a chance to input, the approval of these technologies without this crucial aspect completed would be premature.

11. **Lack of clarity in oversight structure, specifically regarding the Office of the Inspector General and its ability to audit.**

A well-established network of professional and community oversight entities is important to drive accountability and transparency with a technology deployment within said communities. The lack of a clear plan for an oversight network, or a plan that relies on internal reviews within SPD, are insufficient to foster public trust. The SIR gives responsibility to SPD unit supervisors, as well as "any appropriate auditor, including the Office of Inspector General can audit for compliance at any time".

Because the OIG appears to be the primary auditor for these pilots, the relationship between SPD and OIG needs to be very well understood in order to determine how robust of an accountability insurance there is. Although the OIG will have the ability to initiate an audit at any time, it is unclear exactly how the audit process works. An understanding of what the audit is composed of, such as questions, metrics, and scoring scale, would be helpful. Furthermore, there is an open question on what the OIG's "anytime access" means. Does it mean that they are able to remotely look at the same feeds and metrics that SPD sees, or that they have to physically appear at SPD offices to initiate an audit? If there is a delay between the announcement of intent to audit and the access to the information itself, there is a risk for malpractice by the information handlers. It is also unclear how often the OIG, on average, would initiate audits. The working group recommends that there be a mix of scheduled (such as monthly or quarterly) and unannounced audits to maximize accountability.

A useful function of the OIG, for example, might be to take over or oversee the creation of the aforementioned group of "outside academic subject matter experts" such that SPD (the subjects of the review in essence) are not solely responsible for sourcing their own reviewers. This would be a great measure for increasing public trust.

Within the context of "any appropriate auditor", the definition of appropriate may be subjective subject to SPD's judgment. There should be a clear outline of what makes an auditing organization able to initiate an audit. This way, any public interest groups, community organizations, or even national bodies for accountability, could know what information to provide SPD to help with accountability.

12. Lack of clearly defined scope in the form of: specific crime definitions and geographic reach.

Whether it is through uncontained inclusion of devices such as third party cameras or lack of clear pilot timelines, the inability to control the scope of the proposed pilots is a leading area of concern. This also applies to the definition of crimes used for justification of the technologies, and the amount of coverage that the surveillance technology would have in the city.

The working group has concerns about the definition of crimes presenting an opportunity to expand the justifications for technology use within the pilot. While crimes such as gun violence and human trafficking may be more apparent, the SIR also points to "other persistent crimes" which the working group sees as potentially broad in definition. Knowing what is included and excluded in this category, and if there is a definitive list of offenses, would aid evaluation of the proposal. Limiting the possibility of additional justifications to be added after the fact is important to maintain a clearly defined pilot, and to be able to produce transparent documentation for the public.

The working group also has concerns – especially given many of the other areas such as pilot governance, AI technology risks, and community input – that the amount of deployment locations would multiply the risk presented to citizens. Multiple working group members have

questioned the rollout of four CCTV locations (Aurora, Belltown, Chinatown, Downtown) given the lack of definition in key areas. Specifically, these questions center around why there is no proposed option to limit the scope of the pilot to one of these areas. A smaller rollout would limit negative impacts to the public while gaining tangible data and insights. Upon positive results (this necessitates an improved and fully developed review/assessment process as described above), the City would consider expansion and another round of proposals for said expansions. The high degree of concern in the areas above make the larger rollout proposed in the SIR a worrisome proposition.

Recommendations

1. **Risk of disparate impact of surveillance technologies on minority communities within Seattle.**
    - Produce a map that reflects neighborhood demographics (minority community percentage) and then overlay them with the coverage areas of the video cameras.
    - Revisit the Racial Equity Toolkit with acknowledgement of disparate impact on communities of color.

2. **Apparent lack of public input for definition of deployment areas, specifically regarding proximity to sensitive public resources including open meeting spaces and medical centers.**
    - Further expand and engage in ongoing outreach to affected communities before the implementation of the pilot program. Establish regular quarterly meetings with impacted communities to ensure transparency, foster trust, and reduce potential impact on.
    - Schedule periodic meetings (quarterly for instance) with each community area to sense difficulties, concerns, incidents, risk to sensitive community resources, related to the technology implementation.
    - Ensure that notice of surveillance is accessible to all. Ideally, signs should be in multiple languages common in the surveilled communities. Imagery on the signs should clearly indicate that video cameras are recording and these signs should be in well-lit areas or illuminated to ensure notice is available regardless of the time of day.
    - Develop a community-reviewed plan for notice of surveillance to differently-abled individuals and validate it with public interest groups with expertise in design for differently-abled individuals.

3. **Lack of specifics as to the sourcing and capabilities of the proposed technologies in both CCTV and RTCC SIRs, reflecting broader privacy concerns.**
    - Produce detailed information on the requirements put on CCTV cameras, vendor information, and full specifications (effective range, infrared, night vision, pan-tilt-zoom functionality, etc).

- Ensure that the following are made publicly available: How many cameras exist within surveillance zones, names of the manufacturers, vendors, model names, and model numbers of camera devices.
- Create publicly shared data on how many cameras devices SPD owns, how many people have access to the cameras, and collect data on how long it takes the SD to review data and dispose of the footage.
- Create a published protocol on how to manage hardware and software updates to any installed technology to limit uncontained expansion of surveillance capability. If a vendor rolls out new features/functions that need to be physically installed, or can be remotely installed via a software update, should that new functionality trigger a new SIR loop?
- Require further clarity on the specifics of a potential new RTCC before approving it: There has not been enough information provided by SPD regarding the specifications of this technology to determine whether it will provide any measurable benefits over the RTCC technology SPD currently employs.

4. **Concern over possible slippery slope regarding the use of different types of artificial intelligence to monitor personally identifiable aspects of individuals**
   - Do not engage in live-monitoring of CCTV footage unless an active emergency or event is taking place. This would limit the potential for individuals to be targeted with surveillance for low level property crimes. A policy directive could state that AFTER an event is reported to SPD, a detective or screening Sergeant may send a request to RTCC personnel to pull the CCTV footage for review in relation to the serious offense reported in the area. This would preserve the evidentiary purpose of this technology to investigate and solve serious violent crimes such as gun violence while limiting the potential impact on civil rights and liberties.
   - Consider a practice of exempting the public by default unless there is a crime occurrence within a timespan by eliminating personally identifiable data (faces) from data on a running basis and only unlocking via court order.
   - Require transparency and review for any automated analytic tools and ensure unapproved tools are not available.
   - Produce a published list of all models utilized as part of analysis of CCTV streams, as well as provided information on the datasets that were used to train that model.
   - Review and reapply learnings from GDPR (European standard for data protection)

5. **Privacy, quality, and governance risks presented by the inclusion of third-party CCTV devices.**
   - Do not allow private 3rd-party camera feeds to opt into the CCTV and RTCC system.

6. **Lack of clarity around the sworn/civilian reviewers monitoring the video streams, and the data retention policies of that data.**

- Do not engage in live-monitoring of CCTV footage – only access via a specific time-marked request after a crime is reported.
- SPD should submit design proposals for the dashboard format and they should be reviewed before deployment. They should be accessible, detailed, updated in real time, and easily found.
- Locations where police actions and data requests occur should be marked and searchable through time on a map interface.
- Reduce storage time and retention of CCTV recordings to 14 days to limit potential impact on civil liberties and possible data abuse. Formulate a review process for reducing the impact on victims and vulnerable community members.

7. **The need for better definition of justification/success metrics and concrete timelines by which to measure them.**
    - Come to more clear metrics on what the city would be tracking to answer the question "what does success look like?". This includes understanding the measurement units of each of these metrics and they should be agreed and determined BEFORE technologies are rolled out.
    - Institute a hard-stop date regarding pilot deployment. For example, limit any pilot program to one year: shortening the pilot program and requiring lengthy tracking of data related to its use will help in reducing the potential impact on civil rights and liberties while allowing the City to evaluate the effectiveness of this technology.
    - Provide a rubric for effectiveness assessments. This will include acceptable ranges or clearances for each metric. The plan will also have a protocol for creating a score by which to grade continuation of the pilot or cancellation of the pilot. A clear plan for pilot cancellation needs to be defined, including logistics for uninstallation, etc.
    - Ensure transparency in use: Track all law enforcement actions resulting from the use of these technologies and publicly publish results in a quarterly report.
    - Any CCTV stream should be publicly accessible. An example of such a setup exists on the WSDOT real-time cameras webpage, which shows camera views on a set refresh rate such as 2 or 5 minutes.

8. **Lack of clarity on policy areas that the SIR relies upon for future "general guidance" such as the Omnibus Surveillance Policy.**
    - Require SPD to formulate and publish clear policies outlining the use, operational management, and limitations of this technology BEFORE being allowed to employ it into the community (including the Omnibus policy). The publishing process needs to have community input.

9. **Lack of clarity in oversight structure, specifically regarding the Office of the Inspector General and its ability to audit.**

- Define a periodic audit by OIG, and ability to initiate 'unannounced' audits simultaneously.
- Mandate quarterly auditing through a Memorandum of Understanding (MOU) with OIG to ensure ongoing compliance with policies, City ordinances, and pilot program parameters.
- A useful function of the OIG, for example, might be to take over or oversee the creation of the aforementioned group of "outside academic subject matter experts" such that SPD (the subjects of the review in essence) are not solely responsible for sourcing their own reviewers. This would be a great measure for increasing public trust.
- There should be a clear outline of what makes an auditing organization able to initiate an audit. This way, any public interest groups, community organizations, or even national bodies for accountability, could know what information to provide SPD to help with accountability.

10. **Lack of clearly defined scope in the form of specific crime definitions and geographic reach.**
    - Produce documentation outlining specific definitions of the crimes, and corresponding reasons why each technology is well-suited for addressing that crime need to be outlined.
    - Limit CCTV use to only the serious violent offenses outlined in the SIR as the motivation for this pilot project.
    - Limit any pilot program to one location: limiting the pilot program to one community will reduce the potential impact on civil rights and liberties for Seattle community members. It will further ensure that the pilot program remains a test program aimed at a particular purpose. The decision on which location will be selected should be made based on data regarding violent crimes in the area and input from the affected community.
    - Create true coverage maps of the zones that are reflective of not only the possible placement of cameras, but also the effective camera ranges.

Questions

1. **Risk of disparate impact of surveillance technologies on minority communities within Seattle.**
    - Why isn't 'disproportionately impacts POC' checked in the RET given the clear contextual indication that these deployment areas for CCTV impact POC communities?
    - How will SPD respond to privacy concerns for victims and marginalized community members when PDRs for CCTV are requested by those with the intent to harass or harm them?

2. **Lack of specifics as to the sourcing and capabilities of the proposed technologies in both CCTV and RTCC SIRs, reflecting broader privacy concerns.**
    - With this, there should also be an understanding of the 'permanence' of the installations. With camera infrastructure and RTCC installation, these are costly and if they don't work, what will happen?

3. **Concern over possible slippery slope regarding the use of different types of artificial intelligence to monitor personally identifiable aspects of individuals.**
    - The CCTV SIR mentions at least 43 WA municipalities already use this or some form of CCTV. What are those municipalities and to what extent are they using CCTV?
    - Are there or will there ever be plans to use personally identifiable aspects of human likeness (body type, height, projected weight, etc) to identify people with AI in the video footage?
    - How would children's image be excluded from disclosure?
    - Is the data collected via the patrol car camera device connected in any way to the street cameras in targeted areas?

4. **Privacy, quality, and governance risks presented by the inclusion of third-party CCTV devices.**
    - Explain the process by which private owners of video security systems will be sharing streams from their cameras. Will these videos be "public" in nature? If these owners are business owners, will individuals receive notice of such recordings?

5. **Lack of clarity around the sworn/civilian reviewers monitoring the video streams, and the data retention policies of that data.**
    - What is the average holding time for state cases where video evidence is used?
    - How will a PDR or records request affect the retention time of CCTV video? if a request is received within the 30 day retention window, will that mean the video will be destroyed after it is released or will it continue to be retained?
    - Statement: "Video recordings will be kept on the cameras for 30 days, and not retained for a longer duration unless manually extracted by authorized personnel via the video management system software." – Is there no obligation for an authorized personnel to dispose of any manually extracted data if there is no crime observed after 30 days?
    - Statement: "Responses to Public Disclosure Requests, including responsive records provided to a requestor, are retained by SPD for two years after the request is completed." – Does this supersede normal deletion times?

6. **The need for better definition of justification/success metrics and concrete timelines by which to measure them.**
    - Does SPD or the city have an already in-place network of cameras deployed in these same surveillance areas? What have been the issues and positive results from accessing these cameras?
    - How many cases per year are created by the data gathered from on street camera devices in other targeted areas?
    - What parameters will be used to determine success? CCTV SIR indicates that SPD will evaluate and terminate the pilot if it is not successful and that assessments will be completed at the end of 1 year and at the end of 2 years. Who will be responsible for these evaluations?

- Outside academic subject matter experts will be retained to assist in evaluation: How will these subject matter experts be selected and what criteria will need to be met to establish them as experts?
- If the City Council does not approve the CCTV technology acquisition, how would the different possible versions of the proposed RTCC tech differ from the RTCC SPD currently uses?
    - Without acquisition of the CCTV program, what is the benefit of a new RTCC and would that decrease the projected cost of the new program?
- If CCTV is not approved, what is the impact on RTCC – is it rendered ineffective?
- What makes the potential 2024 rollout of RTCC pilot different than what already has been in place since 2015?
- "The SPD does not currently have any policies related to RTCC" – how is this possible if it's been installed since 2015?

7. **Lack of clarity in oversight structure, specifically regarding the Office of the Inspector General and its ability to audit.**
    - What is the realistic staffing required in order to maintain and run this system? Does it take officers off of the street?

8. **Lack of clearly defined scope in the form of specific crime definitions and geographic reach.**
    - How is a geographic location identified as a high-crime area? Specifically, what are the quantitative and qualitative benchmarks or thresholds for consideration?

City of Seattle

CTO Response to Working Group Assessment

Memo

Date: August 2, 2024

To: Seattle City Council

From: Rob Lloyd, Chief Technology Officer

Subject: CTO Response to the Privacy and Civil Liberties Impact Assessment for CCTV and RTCC by the Community Surveillance Working Group

---

Purpose

This document is prepared pursuant to the Surveillance Ordinance (SMC 14.18.020 G. and SMC 14.18.080) stating, "*Prior to submittal of a SIR to Council, the CTO may provide a written statement that addresses privacy rights, civil liberty or other concerns that are raised in the impact assessment created by the Working Group pursuant to Section 14.18.080.*" This memo outlines the Chief Technology Officer's (CTO's) response to the Community Surveillance Working Group assessment on the Surveillance Impact Report (SIR) for Closed-Circuit Television Camera Systems (CCTV) and Real-Time Crime Center (RTCC) software. The two new technologies proposed by the Seattle Police Department (SPD) are components of an overall *One Seattle* Safety Framework and strengthen the City's public safety response to aid victims, hold accountable those responsible for gun violence, alert real-time crime center staff to serious criminal events, see multiple streams of information overlaid on a map view, and convey situational awareness to officers responding in the field.

Background

The Information Technology Department (ITD) meets the objectives of the Privacy Principles and Surveillance Ordinance by providing 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 potential negative impacts of technology use and data collection on individuals. This requires 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. ITD, SPD, and the Mayor's Office have also worked collaboratively with the Working Group and the public to answer additional questions that arose during the public comment period and SIR review process. Of note, the public input process, program design, and responses for the proposed technologies involved 17 public meetings and feedback from both community members and activists.

Technology Purpose

The City of Seattle is exploring new technologies to help detect, deter, and interdict crime in discrete locations (e.g., hotspots) where gun violence, human trafficking, and violent crime are persistent. The Technology Assisted Crime Prevention Pilot Project is a new public safety program that will combine a

Closed-Circuit Television (CCTV) System with Real-Time Crime Center (RTCC) software together in one view.

The SPD CCTV camera systems are proposed to be installed at locations where gun violence, human trafficking, and persistent violent crime is concentrated. The cameras will face toward the street, sidewalk, and other public areas. Signs acknowledging use of the cameras will be posted in the immediate area of deployment, and street fliers will be distributed. Privately-owned security systems will be able to voluntarily share video of storefronts and areas where the public has access with SPD.

Real-Time Crime Center (RTCC) software provides a centralized location for real-time information and analysis. At its core, RTCC software integrates dispatch, camera, officer location, 911 calls, records management systems, and other information into one single view. The software is used to alert RTCC staff to a serious criminal event, see multiple streams of information overlaid on a map view, and convey information to officers responding in the field.

The pilot program will be deployed to three of the five major crime hotspots in Seattle — Aurora Avenue North, Chinatown-International District, and the Downtown Commercial Core, including parts of Belltown. Sensing and data-driven technologies must be matched with proper controls, training, and community engagement to ensure use preserves both public safety and equity.

Working Group Concerns

In their review, the Working Group highlighted the following issues:

1) Possible infringements on reasonable expectation of protection from warrantless “unreasonable search” creating potential conflicts with The Fourth Amendment;
2) Possible impact on First Amendment Right that might deter public engagement (peaceful protest, assembly, etc.);
3) Risk of disparate impact of surveillance technologies on minority communities within Seattle;
4) Apparent lack of public input for definition of deployment areas, specifically regarding proximity to sensitive public resources including open meeting spaces and medical centers;
5) Lack of specifics as to the sourcing and capabilities of the proposed technologies in both CCTV and RTCC SIRs, reflecting broader privacy concerns;
6) Concern over possible slippery slope regarding the use of different types of artificial intelligence to monitor personally identifiable aspects of individuals;
7) Privacy, quality, and governance risks presented by the inclusion of third-party CCTV devices;
8) Lack of clarity around the sworn/civilian reviewers monitoring the video streams, and the data retention policies of that data;
9) The need for better definition of justification/success metrics and concrete timelines by which to measure them;
10) Lack of clarity on policy areas that the SIR relies upon for future “general guidance” such as the Omnibus Surveillance Policy;
11) Lack of clarity in oversight structure, specifically regarding the Office of the Inspector General and its ability to audit; and
12) Lack of clearly defined scope in the form of specific crime definitions and geographic reach.

The Mayor’s Office, Police Department, and Information Technology Department understand the concerns raised by the Working Group. To address these, the pilot program will be implemented with

several protections addressing privacy concerns or unintended consequences. This includes limiting surveillance to public places in specific geographic areas where the identified crimes are concentrated, visible appropriate language signage, prohibiting the use of AI facial recognition, minimizing retention periods, broad neighborhood outreach before and during the pilot project, a rigorous and independent implementation and outcome evaluation led by the Office of Inspector General (OIG) and outside academic subject matter experts, and reporting to the public on the project's performance and outcomes.

The Privacy Impact Assessment and Racial Equity Toolkit section of the SIR document answers the issues about the collection, use, sharing, security, and access controls for the data part of the pilot program. The policy, training, and technology controls proposed by SPD adequately mitigate the potential privacy and civil liberties concerns raised by the Working Group provided ongoing monitoring is established. As a pilot program, it has clear set goals and evaluation measures under a *Continuous Impact Assessment* framework with outside academic subject matter experts. SPD's proposed public-facing dashboard must update frequently and report on the uses of the technologies to maintain the proposed level of transparency.

Response to Community Surveillance Working Group Assessment:

SPD and ITD look forward to working together with the City Council to achieve the three goals of (1) greater public safety, (2) protecting the privacy and civil rights of our residents, and (3) providing transparency to our public. Emerging technologies require new levels of community engagement and co-building safety solutions with neighborhood input, as well as working with companies to create necessary controls and transparency in the tools and data cities choose to use. In consultation with SPD, the following sections respond to the Working Group comments and recommendations with additional edits to the published SIR.

1) Possible infringements on reasonable expectation of protection from warrantless "unreasonable search" creating potential conflicts with The Fourth Amendment.
    - Section 1.2 of the CCTV Privacy Impact Assessment addresses this issue.
        - Section 1.2: SPD's proposed CCTV camera systems would capture video of identifiable individuals, some of whom may be unaware of the recording, despite signage. Without appropriate safeguards, this raises significant privacy concerns which has resulted in this review. Recognizing these concerns, SPD proposes the CCTV camera systems will be utilized in a limited fashion, in locations with risk trends, and only in public-facing locations. The cameras will face toward the street, sidewalk, and other public areas, and visible signs acknowledging use of the cameras will be posted.

2) Possible impact on First Amendment Right that might deter public engagement (peaceful protest, assembly, etc.)
    - Section 1.2 of the CCTV Privacy Impact Assessment addresses this issue.
        - Section 1.2: SPD's proposed CCTV camera systems would capture video of identifiable individuals, some of whom may be unaware of the recording, despite signage. Without appropriate safeguards, this raises significant privacy concerns which has resulted in this review. Recognizing these concerns, SPD proposes the CCTV camera systems will be utilized in a limited fashion, in locations with risk

trends, and only in public-facing locations. The cameras will face toward the street, sidewalk, and other public areas and visible signs acknowledging use of the cameras will be posted.

3) Risk of disparate impact of surveillance technologies on minority communities within Seattle.
    - Section 1.3 of the CCTV Racial Equity Toolkit addresses this issue.
        - Section 1.3: SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior and other accountability measures. This pilot will be data-informed and guided. It will terminate if data suggests the technology is ineffective. Utilizing the abilities of the Performance Analytics and Research Unit, the Seattle Police Department is assigned to actively manage performance measures reflecting the "total cost of ownership of public safety," Equity, Accountability, and Quality ("EAQ"), which includes measures of disparate impact and over policing. In addition to a robust Continuous Intervention Assessment designed to inform development of more effective Evidence-Based Policing (EBP), the technologies are location-specific, deployed based on concentrated Priority 1 criminal activity, rebalanced by analysts for equity, and narrow in view, meaning they will record people who choose to be in a public place where the technologies are being used and signed. These mitigating factors reduce, to the extent possible, disparate impact of potential police actions.

4) Apparent lack of public input for definition of deployment areas, specifically regarding proximity to sensitive public resources including open meeting spaces and medical centers.
    - Section 2.0 of the CCTV Racial Equity Toolkit addresses this issue.
        - Section 2.0: The City's public engagement and input process included two citywide public meetings, 15 neighborhood meetings, and feedback from organizations such as the NAACP, ACLU, and advisory groups from the pilot areas. In addition, the six Community Safety Forums held across the city from April to May also included opportunities for public comment on the technologies.
        - The pilot locations under consideration are at three of the five major hotspot locations in Seattle: Aurora Avenue North, Chinatown-International District, and the Downtown Commercial Core including parts of Belltown. These technologies are geographically focused on specific areas where gun violence, human trafficking, and other persistent felony crimes are concentrated.

5) Lack of specifics as to the sourcing and capabilities of the proposed technologies in both CCTV and RTCC SIRs, reflecting broader privacy concerns.
    - Section 2.3 of the CCTV Privacy Impact Assessment addresses this issue. Technical specifications with the technology solution occur after Council approval of the SIR and are finalized during the contract process with the potential vendor.
        - Section 2.3: Each CCTV system consists of the following, with some variance depending on the specific technology/vendor solution that is selected.

        - Cameras: these can range from simple fixed cameras to more sophisticated cameras with pan-tilt-zoom (PTZ) as well as other capabilities (infrared night vision, high-definition imaging, etc.).
    - The City will initiate the use of standard contract terms providing the following:
        - Prohibit collecting data that is not within the public view. This includes any data not readily visible from a public area or public property;
        - Prohibit monitoring individual or group activities legally allowed in the State of Washington and/or protected by the First Amendment to the United States Constitution;
        - Prohibit sharing with immigration authorities or use in the investigation of any matter related to immigration status of an individual;
        - Prohibit engaging in automated citations or other automated enforcement without manual review from SPD staff;
        - Prohibit selling any data generated by ALPR to any entity; and
        - Stating data ownership and right to use from camera operations and/or activity shall remain at all times the City's.

6) Concern over possible "slippery slope" regarding the use of different types of artificial intelligence to monitor personally identifiable aspects of individuals.
    - Section 1.2 and 2.3 of the RTCC Privacy Impact Assessment addresses this issue.
        - Section 1.2: SPD will not use AI facial recognition technologies.
        - Section 2.3: This technology complies with the city of Seattle's AI rules for use, requiring a "human in the loop" at the initiation and evaluation of the results. SPD will not use facial recognition technology. In addition, SPD would not use analytics available in some platforms that combine different data sources and use algorithms or AI to present trends.

7) Privacy, quality, and governance risks presented by the inclusion of third-party CCTV devices.
    - Section 1.1 and 3.1 of the CCTV Privacy Impact Assessment addresses this issue.
        - Section 1.1: Privately-owned security systems will be able to voluntarily share video of storefronts and areas where the public has access with SPD. This option would be fully voluntary at the discretion of the camera owners. Private camera owners can also set up conditional sharing, meaning they can determine the parameters of what, how, and when their camera feeds are shared. Some vendors also provide a registry so that private camera owners can share the location of the camera, but not the video feeds, so agencies can easily canvass for videos after an incident. The system can then allow SPD to send an email to all registered cameras in an area requesting relevant video. There is no obligation to share footage if a system is registered. SPD would also allow registrants to revoke permission at any time.
        - Section 3.1: The system will have a set of access controls based on what is required for each user. Only authorized and trained SPD and OIG personnel will have direct access to the CCTV system. Video may only be accessed or extracted for legitimate law enforcement purposes, as governed by SPD Policy 12.050. Staff shall also ensure that all records retention rules are properly followed.

8) Lack of clarity around the sworn/civilian reviewers monitoring the video streams, and the data retention policies of that data.
    - Section 3.1, 3.3, 4.1, 4.2, 5.2, and 5.3 of the CCTV Privacy Impact Assessment addresses this issue.
        - Section 3.1: The system will have a set of access controls based on what is required for each user. Only authorized/trained SPD and OIG personnel will have direct access to the CCTV system.
        - Section 3.3: CCTV camera systems will only be made accessible to authorized SPD, OPA, and OIG personnel. Authorized personnel will receive training in the CCTV video management system prior to authorization. All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.
        - Section 4.1: Until data is extracted from the CCTV system's local storage, the data is temporarily stored on the device. Video may only be extracted for legitimate law enforcement purposes (such as a dispatched call for service or investigations of crimes), as governed by SPD Policy 12.050. Video recordings will be kept on the cameras for 30 days, and not retained for a longer duration unless manually extracted by authorized personnel via the video management system software. Private, 3rd party video, if used, will be subject to the 30-day retention on SPD storage, unless used as evidence for a criminal investigation. SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a General Offense (GO) Report. Evidence is submitted to the Evidence Unit and associated with a specific GO Number and investigation.
        - Section 4.2: CCTV video recordings are automatically purged by the system after 30 days unless the footage holds evidentiary value related to criminal activity or assists in the pursuit of a criminal investigation. Additionally, the CCTV camera systems will maintain a complete audit log of activities (including but not limited to personnel access and video extraction logs) and would be subject to an audit by the Office of Inspector General at any time.
        - Section 5.2: Per the Washington Secretary of State's Law Enforcement Records Retention Schedule, the required records retention period for surveillance video that does not involve a specific incident is "Retain for 30 days after last recording or until determined that no security incident has occurred, whichever is sooner, then Destroy." Data associated with criminal investigations will be saved as evidence in SPD's digital evidence locker consistent with retention guidelines for evidence.
        - Section 5.3: As noted in section 5.2 above, CCTV data stored by the city will be automatically purged by the system after 30 days for any data that is not determined to be related to criminal activity/investigation. Data collected from a private security system will only be stored by the City for 30 days unless it contains evidence of criminal behavior.

9) The need for better definition of justification/success metrics and concrete timelines by which to measure them.
    - Section 4.4 of the CCTV Privacy Impact Assessment and Section 5.0 of CCTV and RTCC Racial Equity Toolkit addresses this issue.
        - Section 4.4: The technology will be in continuous operation for the duration of the pilot program. The possible initial pilot areas under consideration are Aurora Avenue North, Chinatown-International District, and the Downtown Commercial Core including parts of Belltown. The exact duration of the pilot will be evaluated under a Continuous Impact Assessment framework. Outside academic subject matter experts will be retained to design and manage an evaluation plan with an assessment at the end of one year and another at the end of year two.
        - Section 5.0: The goals of this project are:
          1. Reduction in gun violence, human trafficking, and other persistent felony crimes in the pilot area.
          2. Reduction in 911 calls in the pilot area.
          3. To minimize crime displacement outside of the pilot area.
          4. Improved police response times, crime clearance rates, and community satisfaction measures.

          The Seattle Police Department will report the rate of arrests and prosecutions that occur as a result of the pilot and any negative unintended consequences, such as over- or under-policing.

          The Seattle Police Department, utilizing the Data Analytics Team and working with the Office of the City Auditor, will monitor these objectives and the outcomes closely to watch for disparate impacts. If data analysis shows any disparate impacts, SPD will work with the Auditor and the Office of the Inspector General to make the needed changes to address these impacts. Further, the City will retain outside academic subject matter experts to develop and manage an evaluation plan related to the use of the technologies.

10) Lack of clarity on policy areas that the SIR relies upon for future “general guidance” such as the Omnibus Surveillance Policy.
    - Section 4.1 of the CCTV and RTCC Racial Equity Toolkit addresses this issue.
        - Concerns that have been raised through public comment and engagement will be addressed in SPD policy. SPD is developing an omnibus surveillance technology policy to provide general guidance on several topics, including value and equity statements for technology use, an explanation of the surveillance ordinance requirements, internal processes for technology approval and acquisition, general tracking metrics for surveillance technologies, retention requirements and limitations, standard contract terms for vendors, and general use requirements for surveillance technologies. Additionally, issues and guidance unique to specific surveillance technologies would be included for each technology. As such, the department will create a policy section for CCTV.

11) Lack of clarity in oversight structure, specifically regarding the Office of the Inspector General and its ability to audit.

- SMC Chapter 14.18.060 addresses this issue.
    - The Inspector General for Public Safety — in regard to SPD, the City Auditor, and other departments — shall conduct an annual review of the City's use of surveillance technology and the extent to which departments are in compliance with the requirements of this Chapter 14.18 and with the terms of approved SIRs.
- Furthermore, the Office of the Inspector General for Public Safety and the City Auditor will collaborate to retain academic subject matter experts to develop and manage an implementation and outcome evaluation of the pilot project. Seattle IT sees use of the proposed technologies as requiring termination if the project does not support progress toward the defined public safety outcomes. The evaluation results are due for reporting by the Police Department at the end of the first year, and a final report due to be published at the end of the second year.
- Section 4.2, 4.10, 5.4, and 8.2 of the CCTV Privacy Impact Assessment addresses this issue.
    - Section 4.2: Additionally, the CCTV camera systems will maintain a complete audit log of activities (including but not limited to personnel access and video extraction logs) and would be subject to an audit by the Office of Inspector General at any time.
    - Section 4.10: The system will maintain audit logs of user and system actions. These logs will be maintained within the system and be accessible to those with permission to view. Logs will be accessible to the Office of Inspector General upon request.
    - Section 5.4: Unit supervisors are responsible for ensuring compliance with data retention requirements within SPD. Additionally, any appropriate auditor, including the Office of Inspector General can audit for compliance at any time.
    - Section 8.2: OIG conducts independent audits of SPD as instructed by the City Council and by City ordinance.

12) Lack of clearly defined scope in the form of specific crime definitions and geographic reach.
    - Section 1.2 of the CCTV and RTCC Racial Equity Toolkit addresses this issue.

Working Group Recommendations:

In consultation with SPD, the following recommendations by the Working Group are included as part of the Technology Assisted Crime Prevention Pilot Project work plan, or as items to work with the City Council on potential amendments to the SIR. We have incorporated additional edits to the recommendations.

- Schedule periodic meetings (quarterly for instance) with each community area to note difficulties, concerns, incidents, and risks to sensitive community resources related to the implementation of surveillance technology. This shall be an ongoing practice for sensing technologies in neighborhoods.
- Ensure that notice of surveillance is accessible to all. Ideally, signs should be focused on imagery and follow sign conventions and clearly indicate that video cameras are recording

and these signs should be in well-lit areas or illuminated to ensure notice is available regardless of the time of day.

- Produce detailed information on the requirements put on CCTV cameras, vendor information, and full specifications (effective range, infrared, night vision, pan-tilt-zoom functionality, etc.).
- Ensure that the following are made publicly available: How many cameras exist within surveillance zones, names of the manufacturers, vendors, model names, duration of installation, and model numbers of camera devices.
- Require further clarity on the specifics of a potential new RTCC before approving it: Additional information should be provided by SPD regarding the specifications of this technology to determine whether it will provide any measurable benefits over the RTCC technology SPD currently deploys to some areas.
- Require transparency and review for any automated analytic tools and ensure unapproved tools are not available.
- Ensure transparency in use: Track law enforcement actions resulting from the use of these technologies and publicly publish results in a quarterly report.

Submitting Department Response

Description

Provide the high-level description of the technology, including whether software or hardware, who uses it and where/when.

Purpose

State the reasons for the use cases for this technology; how it helps meet the departmental mission; benefits to personnel and the public; under what ordinance or law it is used/mandated or required; risks to mission or public if this technology were not available.

Benefits to the Public

Provide technology benefit information, including those that affect departmental personnel, members of the public and the City in general.

Privacy and Civil Liberties Considerations

Provide an overview of the privacy and civil liberties concerns that have been raised over the use or potential mis-use of the technology; include real and perceived concerns.

Summary

Provide summary of reasons for technology use; benefits; and privacy considerations and how we are incorporating those concerns into our operational plans.

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 for 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.

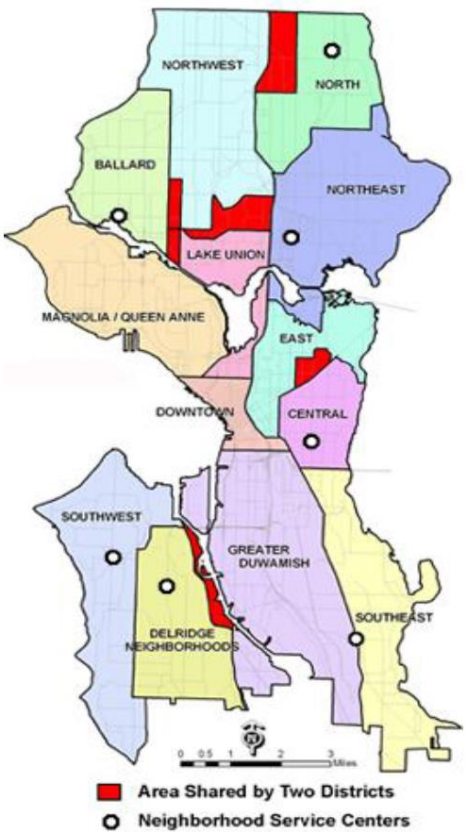
RET: "racial equity toolkit"

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: Office for Civil Rights RET Analysis

Appendix C: Public Hearing Notice(s)

Appendix D: Public Comment from the Public Hearings

Appendix E: Public Comment from the Online Form

Appendix F: Letters from Organizations

Appendix G: Public Comment from Other Sources