CITY OF SEATTLE

ORDINANCE 127298

COUNCIL BILL 121053

AN ORDINANCE relating to surveillance technology implementation; authorizing approval of uses and accepting the 2025 updated surveillance impact report and 2025 executive overview for the Seattle Police Department's use of Real-Time Crime Center software.

WHEREAS, on October 8, 2024, the City Council passed Ordinance 127111, adopting the original Surveillance Impact Report (SIR) for Real-Time Crime Center software (RTCC); and

WHEREAS, the purpose of the RTCC program provides a centralized location for real-time information and analysis—integrates dispatch, cameras, officer location, 911 calls, records management system, and other information into one single view. The software is used to alert real-time crime center staff to a serious criminal event, see multiple streams of information overlaid on a map view, and convey that information to officers who are responding in the field; and

WHEREAS, subsection 14.18.020.F of the Seattle Municipal Code (SMC), which section was enacted by Ordinance 125376 and last amended by Ordinance 125679, states that "[a]ny material update to an SIR, such as to change the purpose or manner in which a surveillance technology may be used, shall be by ordinance"; and

WHEREAS, the material update will provide the Seattle Police Department (SPD) the ability to view the Seattle Department of Transportation (SDOT) traffic monitoring cameras in the RTCC software; and

WHEREAS, the RTCC program went live in May 2025 and early examples of the RTCC program directly contributing to public safety outcomes include a drive-by shooting

where the suspect was taken into custody, footage from a stabbing incident in the Chinatown-International District to assist investigators, a female reporting an attempted robbery with the male suspect denying the allegations but the RTCC video footage showed the male grabbing the female's purse to disprove his story, and locating a suspect where the victim called 911 to report someone was following them with a knife;

NOW, THEREFORE,

BE IT ORDAINED BY THE CITY OF SEATTLE AS FOLLOWS:

Section 1. Pursuant to Ordinances 125376 and 125679, the City Council approves use of the Seattle Police Department's use of Real-Time Crime Center software and accepts the updated 2025 Surveillance Impact Report (SIR) for this technology, attached to this ordinance as Attachment 1, and the Executive Overview for the same technology, attached to this ordinance as Attachment 2.

Section 2. This ordinance shall take effect as provided by Seattle Municipal Code Sections 1.04.020 and 1.04.070.

Passed by the City Council the 9th day of September, 2025, and signed by me in open session in authentication of its passage this 9th day of September, 2025.

President _____ of the City Council

☑ Approved / ☐ returned unsigned / ☐ vetoed this 22nd day of September, 2025.

Bruce A. Harrell, Mayor

Filed by me this 22nd day of September, 2025.

Scheereen Dedman, City Clerk

(Seal)

Attachments:
Attachment 1 – 2025 Surveillance Impact Report: Real-Time Crime Center
Attachment 2 – 2025 Surveillance Impact Report Executive Overview: Real-Time Crime Center

City of Seattle

2025 Surveillance Impact Report

Real-Time Crime Center

Seattle Police Department

Surveillance Impact Report Versions:

- 2024 Surveillance Impact Report: Seattle Police Department Real-Time Crime Center Software adopted by Ordinance 127111 on 10/08/2024.
- 2025 Surveillance Impact Report: Seattle Police Department Real-Time Crime Center Software

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.

The Crime Prevention Technology program is designed to be a pilot project, with independent researchers conducting an outcome evaluation to be completed two years after implementation. Depending on the outcome of the evaluation, the pilot project may be either discontinued or continued.

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, cameras (such as CCTV and traffic monitoring cameras), 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, SDOT traffic 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 CCTV and SDOT traffic 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 judging 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), Seattle Department of Transportation (SDOT) traffic-monitoring cameras (as referenced in the “Closed Circuit Television ‘Traffic Cameras’ (Transportation)” SIR), 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 or SDOT traffic monitoring cameras 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 or SDOT traffic monitoring cameras) 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, SDOT traffic monitoring cameras, 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.

SDOT traffic monitoring cameras (as referenced in the "Closed Circuit Television 'Traffic Cameras' (Transportation)" SIR) will be utilized in the RTCC software for law enforcement purposes.

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
Q4 2024	Q2 2025	$300,000	$0	$100,000	General Fund

Notes:

Please consult the material update summary and fiscal note.

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:

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		https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/RealTimeCrimeCenterInformation.pdf

Information		

City of Seattle

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

Purpose

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

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

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?

The information presented in this RET is specific to the initial pilot areas of Aurora Ave. N, Chinatown/International District, and the 3rd Ave./Downtown Core.

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.

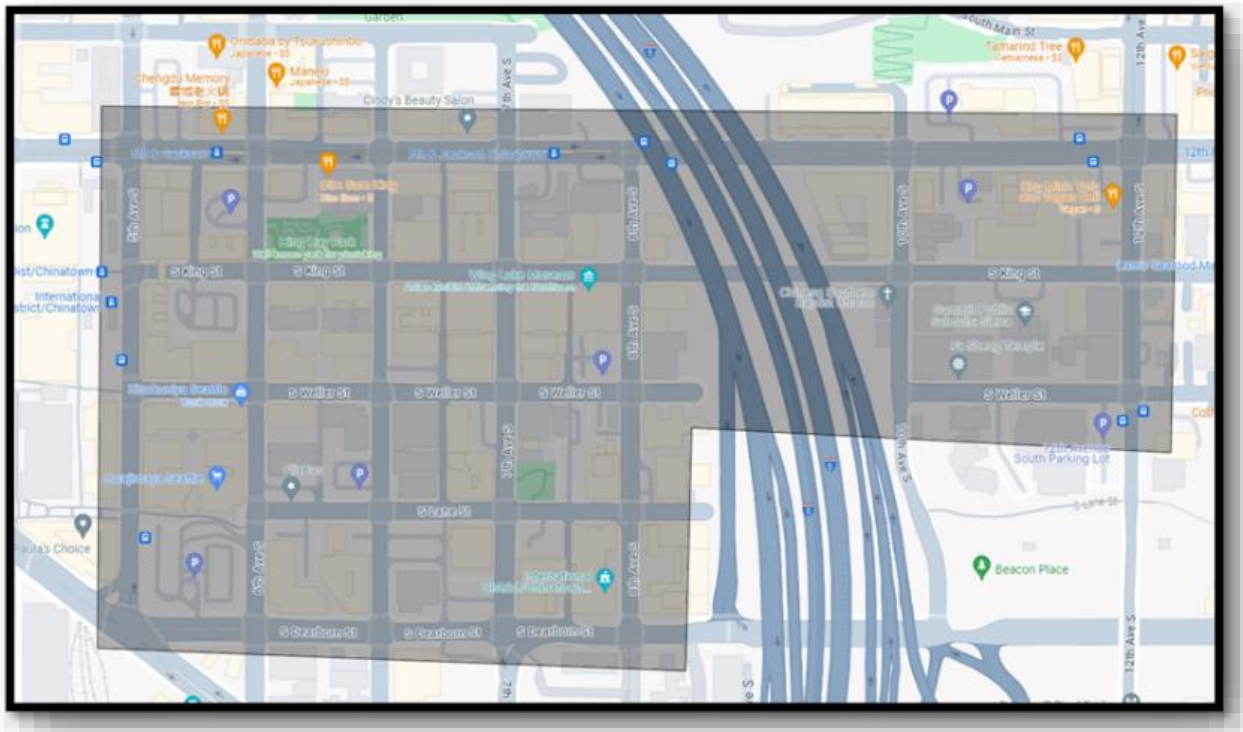
☐ all Seattle neighborhoods

- ☒ **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, 85th to 145th Streets)

1.4.1 What are the racial demographics of those living in this area 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

SMC 14.18 does not require material updates to go through the same process as the original SIR.

3.0 Public Comment Analysis

The public comment period was June 3, 2025 to June 23, 2025.

3.1 Summary of Response Volume

Please see Appendix B.

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

Please see Appendix B.

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

Please see Appendix B.

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 B.

3.5 Question Four: General response to the technology.

Please see Appendix B.

3.5 General Surveillance Comments

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

Please see Appendix B.

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

SMC 14.18 does not require material updates to go through the same process as the original SIR. Please consult Ordinance 127111 adopted by the City Council on 10/08/24 to view the original Privacy and Civil Liberties Assessment.

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.

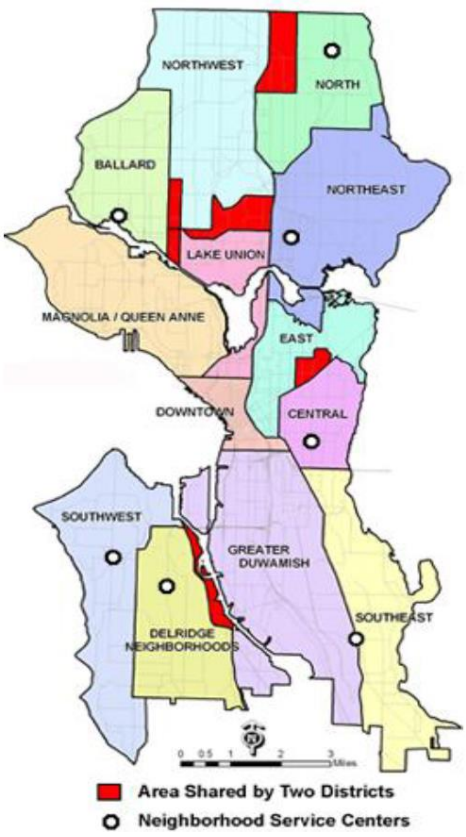
RET: "racial equity toolkit"

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: Public Comment Period (6/03/25 to 6/23/25)

CCTV 2025 Material Change, public comment received via Privacy Inbox

June 23rd, 2025

Dear Seattle City Leadership,

Here is my public comment on the SPD Real-Time Crime Center (RTCC) Surveillance Impact Report (SIR) currently going through the Material Update process.

I've provided my concerns and recommendations below in order of severity. You will find that the negatives far exceed any possible positives and as such **my overall recommendation is that the City of Seattle not deploy a RTCC and all the material updates to the system should be rescinded.**

Concerns & Recommendations:

1) Reactive, not preventative: SPD is misleading the public by calling this a "Technology Assisted Crime Prevention Pilot". This not a pilot and the SPD RTCC contains data from on-going and historical crime incidents, so by it's very nature will be reactive (911 calls, etc). SPD even says in item 1.1 of the RTCC SIR that the "purpose of RTCC software is to provide situational awareness to ... reactively investigate incidents." The RTCC is not a crime prevention tool and mislabeling it as such diverts consideration away from truly preventative measures, which are not technology driven - and that is true for both community-oriented measures (like after-school programs, rehabilitation, workforce training, etc) and police/policy-driven measures (such as gun lock boxes, gun buy-back programs, requiring reporting of lost/stolen guns, trigger locks, etc).
Recommendation: SPD must not deploy a RTCC (and certainly not implement any of the material updates proposed) - effort should instead be placed on actual crime prevention measures.

2) Meager efficacy: The low effectiveness does not outweigh the high monetary cost + significant privacy/civil liberties risks:

(a) The 2024 paper by Rachael Arietti (of City University of New York) titled "Do real-time crime centers improve case clearance? An examination of Chicago's strategic decision support centers" [https://doi.org/10.1016/j.jcrimjus.2023.102145], which SPD referenced in the RTCC SIR, shows that RTCCs deployed in Chicago had the largest effect (which was still modest) for property crime clearance. However, in item 5.1 of the RET inside the RTCC SIR, SPD says the number one goal of the project is "Reduction in gun violence, human trafficking, and other persistent felony crimes in the pilot area." This goal is out of alignment with what RTCCs are shown to achieve. Specifically, the paper said that RTCCs "appeared to have a relatively smaller impact on violent crime clearance (5% increase)" [Arietti page 6]

(b) Other studies have also shown minimal to no effect of RTCCs on violent crime. For example, the 2019 paper by Christopher Koper (of George Mason University) and et. al. titled "Evaluation of the Milwaukee Police Department's Crime Gun Intelligence Center" [https://crimegunintelcenters.org/wp-content/uploads/2019/10/MPD-CGIC-Evaluation-2019_Final-Report.pdf] found "In general, there were no upward trends in the percentage of incidents cleared during the post-[RTCC] period (2014-2017) for any of the offense types" [Koper pdf page 36].

(c) Overall, the results from studies assessing the use of technology on crime clearances has been mixed; whereas other (non-technological) aspects have been shown to have a greater impact on case clearances. For example, the 2021 paper by Heather Prince (of George Mason University) and et. al. titled "Effective police investigative practices: an evidence-assessment of the

research" [http://dx.doi.org/10.1108/PIJPSM-04-2021-0054] states "newer research findings suggest that investigations-specific organizational policies focused on strengthening the capacity and accountability of investigative work, applying targeted resources to investigations, and increasing investigative effort in developing witnesses, evidence and responding to crime scenes could improve an agency's ability to affect clearance rates" [Prince pdf page 15] So it would be a better use of SPD's time and taxpayer's money to pursue these non-technological improvements that have shown measurable improvements in crime clearances.

(d) SPD already has had a RTCC (iBase) since 2015. If RTCCs were effective at helping clear cases, then that should already be evident in SPD's existing data (such as, mean time to suspect identification before vs after 2015, mean length of time to case clearance before vs after 2015, etc). Since SPD didn't provide such data, the public can only assume that the data SPD does have doesn't look promising regarding the use of a RTCC. Additionally, in item 1.1 of the RTCC, SPD said that a RTCC "helps reduce unnecessary stops by officers, focusing their efforts on verified locations and accurate descriptions." So how many unnecessary stops did SPD conduct before vs after 2015? Moreover, how does the RTCC change the accuracy of suspect descriptions and how is that shown in SPD's data before vs after 2015?

Recommendation: SPD must not deploy a RTCC (and certainly not implement any of the material updates proposed) - there is no point to deploying an ineffective technology.

3) Expensive: This is a poor use of taxpayer money and even of the SPD budget itself. It's also highly likely to be a ballooning amount of money year-over-year, beyond what the SIR implies:

(a) Looking at four other US cities that have deployed RTCCs and for which their cost information is publicly accessible, the average cost is $7.16 per person (that is, per person based on the population data from each city's 2020 Census). With Seattle's 2020 population of 737,015, this would put the full-scale (post-pilot-phase) RTCC deployment by SPD in the ballpark of $5.3 million, not including the additional costs for the CCTV and ALPR expansions.

(b) Even the paper referenced by SPD in the SIR mentions the "substantial costs associated with RTCCs, with initial costs ranging between several hundred thousand dollars to $11 million ... This does not include the costs of ongoing maintenance, technology, and personnel" [Arietti page 1]. The paper later goes on to list the costs specific to Chicago's RTCC as "about $10.6 million, plus an additional $600,000 annually" [Arietti page 4].

(c) The Fiscal Impact section of the RTCC SIR is lacking any data regarding the expected year-over-year costs for powering the RTCC equipment, staffing the RTCC room, bandwidth & data storage costs, the on-going subscription to the vendor's software & support package, and projected maintenance costs. Given the budget deficit the City is facing, it is unwise for the City to spend likely well over $1.8 million dollars to surveil residents instead of providing social services and funding community-driven, proven solutions to reducing gun violence.

(d) This seems like a foot in the door for SPD to have an always ever increasing budget allocated to them to expand and deepen their surveillance. It will be a contract that is an investment in exceptionally costly, ineffective, reactive measures that are hard to remove and do nothing to actually help residents or reduce violence.

(e) SPD says that this will replace their existing RTCC (iBase). However, SPD also uses iBase for other functionality (link analysis, which was the only approved used of iBase under the Surveillance Ordinance). This means that there will continue to be on-going costs for both iBase and the RTCC (Fusus). This is yet another way that SPD's expenditures will continue to balloon.

Recommendation: SPD must not deploy a RTCC (and certainly not implement any of the material updates proposed) - there are better uses of limited City funds.

4) Racially-biased deployment: The Racial Equity Toolkit (RET) included inside the SIR hasn't been updated to reflect the additional locations added to be surveilled. The old RET is now rather inaccurate since it doesn't include a map of the SDOT traffic camera locations or the proposed additional SPD CCTV locations and item 1.4.2 still says "CCTV will be deployed where crimes related to gun violence, human trafficking, and other persistent felony crimes are concentrated" which is no longer true because SDOT traffic cameras are all over the city and their placement is not related to felony crimes. This is on top of the many issues with the original RET itself:

(a) The RET doesn't appear have been drafted in consult with the Office of Civil Rights, as required by City Council.
(b) RET item 1.4.1 in the SIR shows disparate impact in the locations chosen to be surveilled. Specifically, there is disproportionate impact on Native American residents in 4 out of 4 of the pilot locations, Black residents in 3 of the pilot locations, Asian & Latinx residents in 2 of the pilot locations, and Mixed folks in 1 of the pilot locations. Additionally, while the majority of Seattle residents are white, all of the pilot locations have an under-proportionate amount of white residents - thus meaning the pilot locations selected appear on paper to be racially motivated. I don't see how the impact won't be biased-based policing because if you are only looking for crime in non-white neighborhoods, then you're primarily going to find non-white suspects (and victims); whereas criminals in white neighborhoods (who are therefore likely white themselves) will fly under the radar of the police.
(c) RET item 1.4.2 in the SIRs states, "This technology does not enhance the risks of racial or ethnicity-based bias." SPD has not provided any explanation as to how deploying this technology in racially-biased locations won't generate racially-biased policing outcomes.
(d) This is made worse by SPD's response to the RET question asking how they will mitigate the risks for racial bias in the deployment and SPD answered that these technologies "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." So SPD is basically saying that residents can avoid SPD police biases (and invasion of their privacy) by not going outside in public - you need to stay home if you don't want to be surveilled - that it's up to residents to protect themselves against SPD biases.
(e) Only 1 of the 2 public engagement meetings on these surveillance technologies was held near a pilot location and the 1 location that was also happened to be the location with the highest amount of white residents out of the 4 pilot locations. Why can SPD find the time to talk to surveillance technology vendors and the City can find the money to surveil residents, but somehow doesn't have the time nor the money to even have host a community event in all of the pilot locations?

Recommendation: SPD must not deploy a RTCC (and certainly not implement any of the material updates proposed) - racist behavior (including with technology) has no place in Seattle.

5) Enabling circumvention of Seattle & WA state laws: Women, trans folks, and immigrant residents are placed in increased harm by SPD's proposed RTCC:

(a) For background, WA HB 1469 was passed in 2023 and created a Shield Law in WA state (now under RCW 7.115). Among other things, the WA Shield Law prohibits WA state, local agencies, & law enforcement and WA-based companies & other private entities from providing

information to, complying with subpoenas, or cooperating with an outside state related to bans or bounty hunting that state might have related to reproductive or gender-affirming healthcare.

(b) And WA SB 5497 was passed in 2019 and created the Keep Washington Working Act (now under multiple RCW sub-sections). Among other things, the Keep Washington Working Act restricts the extent to which local law enforcement agencies (such as SPD) may participate in enforcement of federal immigrant laws (such as by assisting ICE by collecting information about residents which may be undocumented).

(c) In item 2.3 of the RTCC SIR, SPD says that "Most RTCC vendors provide this service via cloud-based web applications..." and SPD has confirmed that the video recordings will be streamed and recorded in the cloud (not on-premise with the City of Seattle).

(d) Data stored off-premise (aka "in the cloud", "cloud-based", or "Software-as-a-Service", SaaS) is at risk of being subject to legal requests for that data directly from the platform provider by entities external to WA state. For example, a judge from Idaho could sign a subpoena/warrant that requests Axon Fusus (the proposed RTCC provider for SPD) to provide ALPR data for vehicles used by and/or CCTV recordings of people visiting Seattle who were suspected of having an abortion or assisting in providing trans healthcare. Or ICE could issue requests for ALPR and/or CCTV data specific to undocumented people that they believe might be in the Seattle area. Because Axon isn't a WA company, the data is not protected by the Shield Law; and because Fusus isn't a government law enforcement agency, the data is also not protected by the Keep WA Working Act.

(e) These risks to women, trans folks, and/or immigrants are so severe and tangible that as of April 2025, Nashville is no longer even considering deploying the very same tech that SPD has deployed (Axon Fusus): https://nashvillebanner.com/2025/04/28/metro-nashville-fusus-freddie-oconnell/

(f) The amendment that passed in Council that altered the contract language with Axon does not address these concerns either because state/federal laws will always be honored by a judge over simple contract language. Additionally, if the judge who signed the warrant also signed a gag order for those requests, then not only would SPD be unable to stop such information sharing but also Axon might be legally blocked from even disclosing that the request(s) exist to SPD (regardless of what the contract says).

(g) These concerns are especially relevant now given the current administration and because SPD has already mounted a camera within range of viewing people who visit the Planned Parenthood on 105th and the Home Depot on Aurora.

(h) SPD's existing RTCC (iBase) is on-premise, so it doesn't create these risks to residents.

Recommendation: SPD must not deploy a RTCC (and certainly not implement any of the material updates proposed) - SPD must not weaken state laws nor endanger women, trans folks, and immigrant residents. If City Council approves of this anyways, then at a minimum, require that the RTCC to be on-premise.

6) Illegal use of SDOT cameras: Adding SDOT's traffic monitoring cameras to the SPD RTCC would violate numerous sections of Ordinance 125936 (2019 SDOT CCTV & LPR SIRs).

(a) Item 3.0 on page 150 of Ordinance 125936 states "The CCTV system and data shall be used only for traffic management purposes, except for when the City's Emergency Operations Center is activated to respond to an emergency or to monitor a major city-wide event, in which case the system may be used by other city personnel (e.g. Police and Fire). The system shall not be used for civil or criminal enforcement purposes." So it is illegal for SDOT cameras to be routinely & constantly used by SPD without an event happening. Moreover, this implies that video footage

from the SDOT traffic monitoring cameras would not be admissible in court since it was illegally captured.

(b) At least four other items (3.1, 4.3, 4.7, & 6.1) of Ordinance 125936 only lists users who will have access to FLIR Cameleon ITS and does not list any City departments that would have on-going use of the SDOT traffic camera video feeds outside of Cameleon, so the public and City Council did not consider nor assess this when passing Ordinance 125936.

(c) Similar wording in items 3.3, 4.2, 5.1, & 7.2 of Ordinance 125936 state that "Video images will not be recorded, except for compelling traffic operational needs. If they are recorded, any such recordings will be destroyed immediately after use. Recordings shall not be stored or disseminated." So it is illegal for SPD to create and store recordings of the SDOT traffic camera feeds.

(d) Similar wording in items 3.3, 4.0, 4.2, & 7.2 of Ordinance 125936 also state that "Operators may not intentionally use the CCTV cameras to discern any personally identifiable information that would enable the operators to identify a member of the public, unless doing so is necessary to allow the operator to perform a traffic management function." So the SDOT traffic camera feeds would not be of any investigative or evidentiary use to SPD anyways since they are not allowed to contain any personally identifiable information.

(e) Items 4.0 & 4.1 on page 153 of Ordinance 125936 state that "The SDOT CCTV System will not be used to collect any data other than the following: • Live-streamed feed of current traffic conditions • Recorded video of traffic for engineering studies • Still images of traffic conditions used in training materials or included in social media." So both SPD's routine, continuous access to the SDOT traffic cameras and the creation of any recordings from them is illegal.

(f) Similar wording in items 4.2, 4.7, 5.0, 5.3, 6.2, & 7.2 of Ordinance 125936 again limit the recordings to only traffic engineering studies and specify that the data retention period for those recordings is 10 days. So not only would SPD's use of the SDOT traffic cameras violate their purpose of use when recordings are made, but SPD would also violate the law if they stored the recordings for 30 days, as they currently plan to do so.

(g) Items 6.0 & 6.1 on pages 159 - 160 of Ordinance 125936 states that users accessing the streams must be "notified that the system is intended to be used to monitor traffic and for no other purpose." So again, SPD's use of the SDOT traffic cameras would violate the SIR.

(h) Additionally, multiple items in Ordinance 125936 would be inaccurate if the SDOT traffic cameras were added to the SPD RTCC: items 7.3, 7.4, & 8.1; the RET, and the Community Surveillance Working Group's Privacy & Civil Liberties Impact Assessment.

Recommendation: SPD must not deploy a RTCC (and certainly not implement any of the material updates proposed) - SPD must not violate local laws, including the requirements laid out in any Surveillance Impact Report signed by the Mayor.

7) Surveillance expansion: RTCC SIR item 2.3 states that "Some RTCC vendors produce hardware that allows for private camera owners (such as private businesses) to share specific camera feeds with agencies." There are multiple concerns about this:

(a) CCTV recordings from nearby business are already being used and leveraged by SPD during investigations, so continuously, on-going access to live video feeds from private entities is unnecessary.

(b) SPD would have no control over technically ensuring that only camera feeds that are of publicly accessible areas are shared with SPD. For example, a business with multiple camera feeds may not consider that certain cameras the business has should not have their feeds shared with SPD since the viewing range includes non-public-facing locations. This could result in even further

invasion of privacy beyond which even a reasonable judge would have granted outside the confines of specific time duration as part of a targeted investigation - thus elevating the surveillance ability of SPD beyond the oversight of the judicial branch.

(c) SPD would have no control over when or where various private video feeds are added or removed from the system; nor would SPD have control over whether the video feeds have on-the-fly AI-generated overlays within the video stream content itself before the feed is made available to SPD - thus elevating the surveillance ability of SPD beyond both public scrutiny and the oversight supposedly enshrined via the Surveillance Ordinance (S.M.C. 14.18).

Recommendation: SPD must not deploy a RTCC (and certainly not implement any of the material updates proposed); but if City Council approves of this anyways, then at a minimum, privately-owned CCTV videos (both live and recorded) should require a warrant signed by a judge before they can be viewed, accessed, or saved by SPD.

8) Hidden/unknowable surveillance features: In item 1.2 of the RTCC SIR, SPD says, "some RTCC software uses non-generative AI, such as object detection, to analyze those surveillance technologies" and in item 2.3, SPD says that they "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." However, face recognition and predictive policing aren't the only concerns:

(a) Gait recognition, behavior analysis, and emotion analysis would also be concerning functionalities that the system might have. None of those tools should be used on the data.

(b) SPD hasn't confirmed that they will only use an RTCC that allows them to disable such features system-wide. This is important because without it, it relies on each individual using the RTCC not clicking the wrong buttons - meaning there is no technical guardrail; and past behavior from SPD has shown that individual employees are willing to violate both SPD Policy and the Surveillance Ordinance (i.e. OPA Case 2020OPA-0305 and OPA Case 2020OPA-0731).

(c) The vendor that SPD plans to use for the RTCC (Fusus) advertises that their system is "continuously evolving along with its database of profiles for search and analysis" and that Fusus is continuously updating the AI capabilities of the RTCC via weekly updates to the system. SPD has not disclosed to the public what are all the edge-based capabilities are they want to use. Not only that but SPD won't even know beforehand what are all the capabilities this system will have even after it's live and in-use (for possibly years). New features can and will be added to the RTCC both without SPD's awareness and without any public oversight or control - thus (again) elevating the surveillance ability of SPD beyond both public scrutiny and the oversight supposedly enshrined via the Surveillance Ordinance (S.M.C. 14.18).

(d) In item 6.5 of the RTCC SIR, SPD didn't mention any accuracy checks they were planning to perform of the AI capabilities of the RTCC. So it seems SPD expects both the City and the public to just trust whatever functionality the vendor provides - without any checks-and-balances on that.

(e) Moreover, even SPD themselves doesn't want automated assessment of their own videos, so why should residents be subjected to surveillance tools that even SPD doesn't like? https://www.seattletimes.com/seattle-news/law-justice/decision-to-halt-program-analyzing-seattle-police-bodycam-video-under-scrutiny/

Recommendation: SPD must not deploy a RTCC (and certainly not implement any of the material updates proposed); but if City Council approves of this anyways, then at a minimum, all edge-based analytics and/or AI capabilities in the RTCC must be disabled until SPD explicitly lists them individually in the SIR during an open public comment period and then receives approval to use them from City Council.

9) No limitations on use: Item 5.1 of the RET in the RTCC SIR says the number one goal for the project is "Reduction in gun violence, human trafficking, and other persistent felony crimes in the pilot area." However, nothing in the SIR limits the use of the RTCC to only "felony crimes". This is a bait-and-switch tactic whereby SPD is using the public's fear of the scariest sounding crimes to justify a surveillance technology that in practice will have unlimited use and very likely will instead commonly be used to harass those most often on-foot (poor folks, sex workers, homeless, tweens/minors, etc).
Recommendation: SPD must not deploy a RTCC (and certainly not implement any of the material updates proposed); but if City Council approves of this anyways, then at a minimum, specify that the only allowable use of the RTCC is for felony crimes.

10) Unidentified data sources: In item 4.1 of the RTCC SIR, SPD lists the data sources to the RTCC and closes with "and other information systems." This wording leaves open the door for future data integrations to the RTCC to be configured but never go through the Surveillance Ordinance process. For example, SPD could add social media data/analysis to the RTCC and that would not generate a new or updated SIR. No department should be above the scope of the Ordinance.
Recommendation: SPD must not deploy a RTCC (and certainly not implement any of the material updates proposed); but if City Council approves of this anyways, then at a minimum, strike "and other information systems" from item 4.1 of the SIR.

11) Excessive data retention: In item 4.2 of the RTCC SIR, SPD says that "Data that is not part of a criminal investigation will be subject to a 30-day retention policy..." This has multiple issues:

(a) 30 days is too long to keep data on innocent people just going about their day.
(b) Retaining the RTCC data (which includes ALPR and CCTV data) for such a long period of time enables stalkers to issue Public Records Act (PRA) requests (potentially repeatedly) for data to use against their victims.
(c) It also means that bounty hunters from states outside of WA can use the PRA request process to get access to RTCC data without needing to issue a warrant. This is yet another way this group of pilot technologies enables outside jurisdictions to get around our Shield Law, which is meant to protect people coming to WA state for reproductive or gender-affirming care.
(d) And it means that ICE can also use the PRA request process to get around Seattle's Sanctuary City policy, which was meant to protect our immigrant residents.
(e) Meanwhile, SPD will have to pay the storage costs for all that unneeded, excessive data.
(f) It should not take SPD 30 days to figure out if a crime occurred at a given location. The SPD CAD and RMS data should be sufficient to somewhat quickly determine if a crime occurred (like say 48 hours, which is the data retention period requested by the Community Surveillance Working Group and City Council for SPD ALPR data, which would be getting processed by the RTCC).

Recommendation: SPD must not deploy a RTCC (and certainly not implement any of the material updates proposed); but if City Council approves of this anyways, then at a minimum, limit data retention period to 48 hours for data not exported as evidence.

12) Duplication causing confusion in an emergency: Item 2.3 of the RTCC SIR, says "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..." Seattle already has an opt-in alert notification system (AlertSeattle - https://alert.seattle.gov/). Having two separate systems that perform overlapping functionality of

notifying residents in the case of an emergency is a bad idea because it could result in residents believing that they are subscribed for all emergency alerts when they are only subscribed to SPD's RTCC-based alerting system. If there is a non-SPD emergency, residents won't receive the alert because they are subscribed to the wrong system. There should be only one emergency alert system used by the City of Seattle and it should be whatever system the City's Office of Emergency Management officially designates as such. All city departments should feed their alert data to the OEM-designated system (as is already the case).
Recommendation: SPD must not deploy a RTCC (and certainly not implement any of the material updates proposed); but if City Council approves of this anyways, then at a minimum, the public alert notification feature of the RTCC must be disabled.

13) Security & Compliance:
- (a) Item 4.7 says, "Access to the systems/technology is limited to authorized personnel via password-protected login credentials." It would be better if access wasn't just password-based, but was also using MFA/2FA (or even 2SA would be something).
- (b) SPD has also not detailed whether a person must be on the SPD network in order to access the RTCC or if remote access will be permitted.
- (c) SPD hasn't confirmed whether the RTCC will have granular access control.
- (d) Nor whether the RTCC logs the username and timestamp when a camera's pan, tilt, or zoom are changed; or when an ALPR search is conducted. For example, if the system does NOT log this and there was a news report about misuse of the RTCC, then it might be impossible for the OIG/OPA to determine which employee was at fault.
- (e) Item 5.4 in the SIR says that, "Unit supervisors are responsible for ensuring compliance with data retention requirements within SPD"; but that doesn't make sense here. Wouldn't this mean that the unit supervisor for the homicide detectives and the supervisor for the gang unit (and so and so forth) would all each be responsible for ensuring data retention compliance of the RTCC? That responsibility should be more centralized so as to ensure consistency in application of compliance requirements for a potentially widely-used system like the RTCC.

Recommendation: SPD must not deploy a RTCC (and certainly not implement any of the material updates proposed); but if City Council approves of this anyways, then at a minimum, require the RTCC to support: detailed logging for all features, Multi-Factor Authentication (MFA), and granular access control of any cameras.

14) Training: Item 3.3 of the RTCC SIR says, "Authorized personnel will receive training in the RTCC management system prior to authorization." and item 7.2 says, "SPD Policy 12.050 mandates that all SPD employees receive Security Awareness Training (Level 2), and all employees also receive City Privacy Training." SPD does not mention creating any privacy or ethics training specific to the RTCC. There should be training that:
- (a) That RTCC features must never be used outside the scope of an active call or investigation; and that employees found to have used the RTCC outside that scope would be personally liable for their actions.
- (b) That ALPR data especially must be treated as sensitive information never to be used for personal purposes (such as stalking an ex/significant-other/neighbor/etc).
- (c) Advises that the cameras accessible via the RTCC must not have their pan/tilt/zoom altered to look inside private residences, to stalk/harass individuals, or to otherwise use the system for personal reasons)

(d) And that the cameras accessible via the RTCC must not have their camera's viewing angle moved away from an area of police response, while police are still present.
(e) Additionally, the RTCC SIR doesn't mention any policy that prohibits the user of the RTCC from taking screenshots, screen-recordings, or pictures/recordings using their cell phone or other mobile device. This especially impacts any victims, passerby, or anyone in the vicinity who are only partially clothed or fully naked, especially if unconscious.

Recommendation: SPD must not deploy a RTCC (and certainly not implement any of the material updates proposed); but if City Council approves of this anyways, then at a minimum, require the creation & utilization of privacy & ethics training specific to the RTCC, including covering examples of expressly forbidden use of the system.

Please seriously consider my public comment. Thank you.

Appendix B: Public Comment Period (6/03/25 to 6/23/25)

From: Roxy Robles
Sent: Tuesday, June 24, 2025 1:10 PM
To: LEG_CouncilMembers <council@seattle.gov>; Privacy <Privacy@seattle.gov>
Subject: NO TO EXPANDED SURVEILLANCE
Good afternoon,
I am writing as a resident concerned about increased surveillance in our city. These technologies were 'piloted' despite a huge amount of community dissent and after only three weeks of use. Three weeks is not nearly enough to pilot test a new technology and to gather information about its efficacy.
Not only does this raise concerns about the overuse and surveillance of already over-policed communities, this raises concerns about the council's ability to follow its own principle of 'good governance', with a consistent application of ethics, race and social justice principles, and data-driven results. I stand firmly against the additional use of surveillance technologies in our city a SPD is already unreliable, selectively responsive, and unbelievably brutal and racist.
SPD is constantly escalating situations, particularly with regard to people exercising their first amendment right to peaceful protest, and despite Shon Barnes' lip service to 'crime prevention' I have yet to see any marked change under his leadership. *We cannot continue to fund untested technologies for a brutal, racist, and unreliable police force!!!*
Roxy Robles *they/she*

From: Brooke Christiansen
Sent: Monday, June 23, 2025 8:45 PM
To: Privacy <Privacy@seattle.gov>
Subject: SIR Material Update Public Comment
Hello, I'm a constituent out of Cap Hill (zip code 98122) and my comment is a follow:
Instead of investing in surveillance tech, let's invest in solving the root causes of crime in this city: high rent (unregulated landlords); limited access to shelter, mental health support, addiction support, job support for (formerly) unhoused folks, etc.; our tax money going to policing and sweeps that may make our neighborhoods temporarily look cleaner but don't solve people's problems; etc.
Best,
Brooke

From: R. John Setzer
Sent: Friday, June 20, 2025 12:00 PM
To: Privacy <Privacy@seattle.gov>
Subject: SIR Material update public comment
With all due respect,
We don't need more surveillance in Seattle. This isn't a police state, and SPD cannot be trusted with that power.

Sent: Sunday, June 22, 2025 9:19 AM
To: Privacy <Privacy@seattle.gov>
Subject: SIR Material Update public comment
Hello,
I am a constituent and a resident of north Seattle who thoroughly opposes expanding of citywide CCTV footage pilot program in the RTCC. More surveillance will NOT keep us safe. We need real programs and

funding for local community advocacy groups and schools instead of cameras to watch our comings and goings. Prioritize proaction instead of reaction!
N.Emery
She/her

From: Jared Howe
Sent: Sunday, June 22, 2025 12:54 PM
To: Privacy <Privacy@seattle.gov>
Subject: SIR Material Update public comment
Dear Seattle City Council,
I'm writing to express my strong opposition to the proposed expansion of CCTV surveillance in Seattle. This plan has moved forward without adequate public notification or transparency from City leadership, SPD, or local media—and the community deserves to be heard.
Research consistently shows that CCTV does not reduce violent crime or improve clearance rates. The SPD's own cited study—a 40-year meta-analysis—found *no significant impact on violent crime*. Additional studies from the UK, Dallas, and elsewhere echo these findings, emphasizing the cost-ineffectiveness and lack of investigatory value.
Beyond its ineffectiveness, CCTV undermines civil liberties, particularly for marginalized communities. Surveillance has a documented history of abuse—from targeting protests and abortion seekers to racial profiling and stalking. Expanding camera networks only increases the risk of misuse, especially as they tie into facial recognition and other AI-driven surveillance tools.
Seattle already has community-centered initiatives that work. Programs like the Regional Peacekeepers Collective and the Rainier Beach Restorative Resolutions project have reduced violence significantly—and offer far better ROI than surveillance tech.
I urge you to oppose the expansion of CCTV and instead invest in evidence-based, community-led safety solutions. Our city's future depends on trust, transparency, and truly equitable public safety.
Sincerely,
Jared Howe
Seattle, WA
District 2

From: Noel Rivard <nrivard67@gmail.com>
Sent: Sunday, June 22, 2025 10:44 AM
To: Privacy <Privacy@seattle.gov>
Subject: No to RTCC and CCTV!!!!
Cameras don't deter people or stop harm from happening, they are just for punishment. Call it what it is or get it out of my neighborhood.
The city's consideration of an off-premise real-time crime center software database is terrifying to me. Especially with the hell our federal administration is putting us through! Our state laws protect us to some degree, but the moving of our data to a third party removes those protections and threatens horrors unseen. PLEASE be diligent and push back in this.
Stop installing the tools for them to surveil and punish!! Get more creative. Do better for our city. Punishment doesn't stop harm from occurring. Get to the root problem. What other pathways could actually prevent this behavior?
I urge you to reconsider for our sake and yours because you live here too. The people their illegally detaining and deporting right now are also your neighbors. History proves, that what we allow to happen

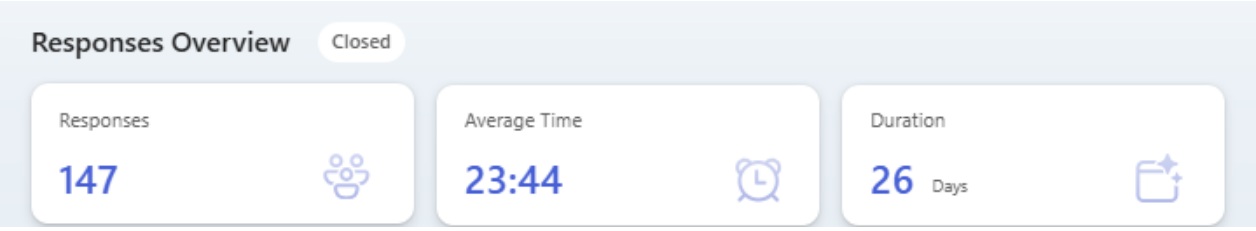
to them, will eventually happen to us.
Noel Rivard (they/them)

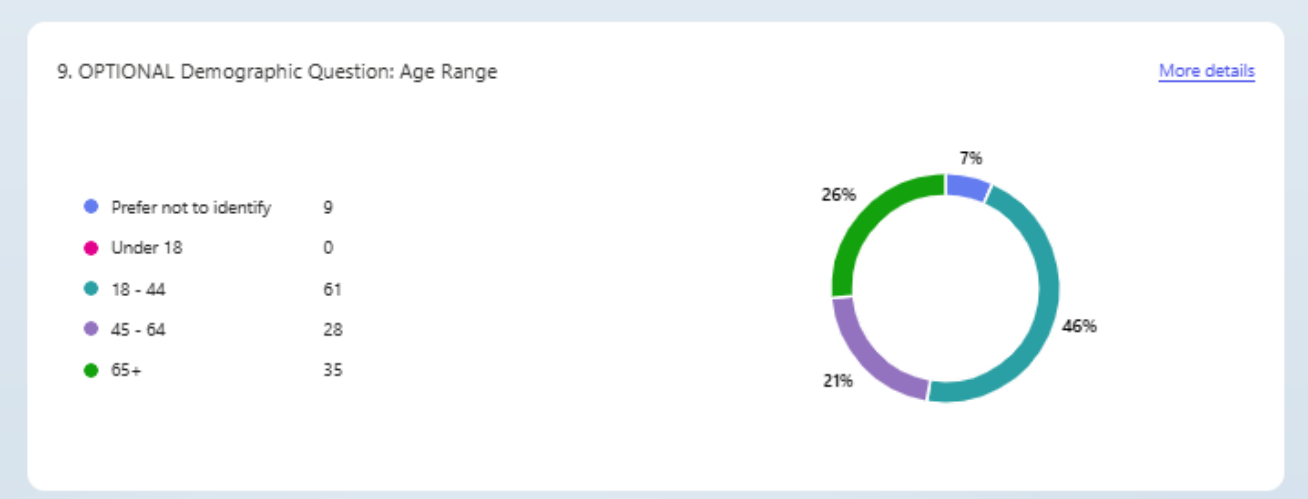
From: Siobhan Hopp
Sent: Friday, June 20, 2025 8:45 AM
To: Privacy <Privacy@seattle.gov>
Subject: SIR material updates public comment
NO expansion of surveillance! DO NOT give more data to SPD. SPD is violent, racially profiles, protects capital over people, and aids and abets ICE in kidnapping members of my community. They should be being given LESS power and LESS access, not more. I say NO to SDOT giving SPD access to more cameras!

From: Joelle Pretty
Sent: Wednesday, June 18, 2025 6:35 PM
To: Privacy <Privacy@seattle.gov>; LEG_CouncilMembers <council@seattle.gov>
Subject: SIR Material Update public comment
CCTV will NOT reduce violent crime or aid in police investigations
CCTV poses a threat to civil liberties
Police control CCTV camera, the cameras see what the police want them to see
RTCC is a threat to women, immigrants, those utilizing their first amendment rights to free speech. It also creates a system ripe for abuse and potential to violate ALL residents' First and Fourth Amendment Rights
I am opposed to these systems, to the Mayor and City Council expanding surveillance, and any officials in Seattle, King County, and Washington State (frankly, in the country) to cooperating with ICE.
KNOCK IT OFF
Sincerely,
Joelle Pretty, Seattle

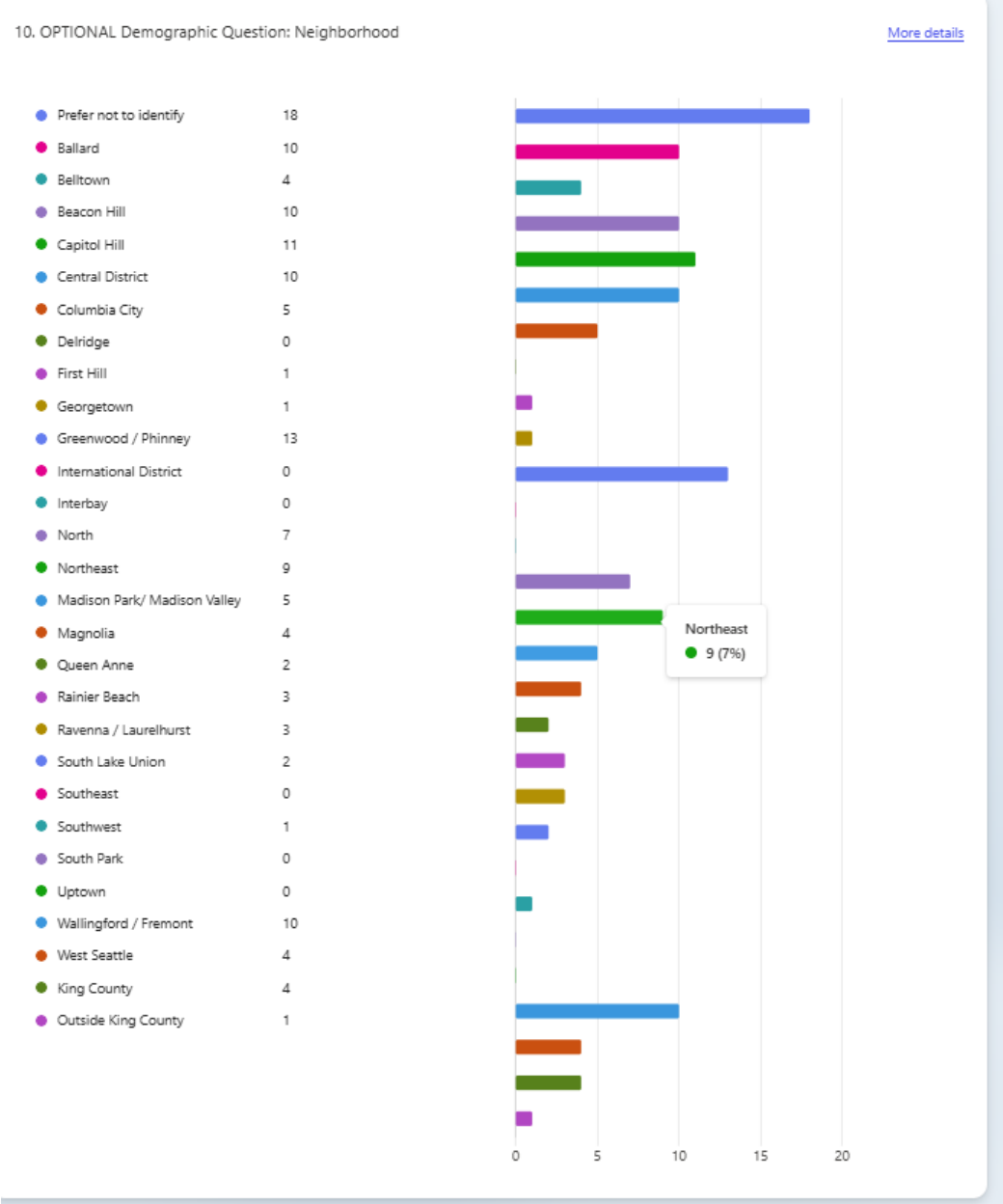
Appendix B: Public Comment Period (6/03/25 to 6/23/25)

Responses received via form:





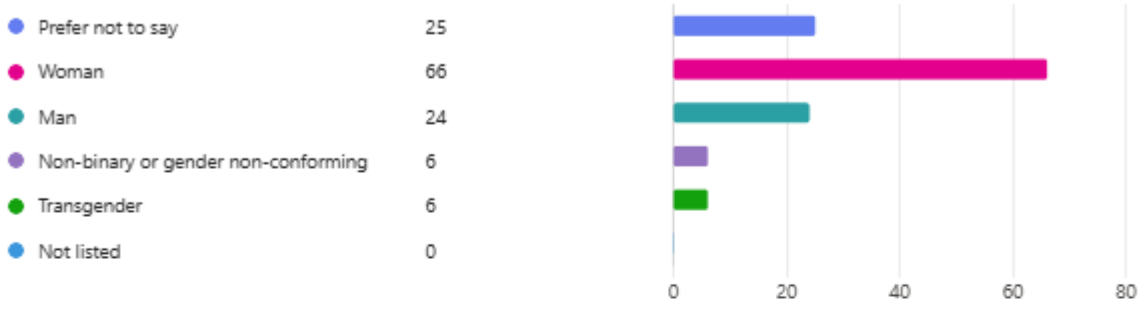
Appendix B: Public Comment Period (6/03/25 to 6/23/25)



Appendix B: Public Comment Period (6/03/25 to 6/23/25)

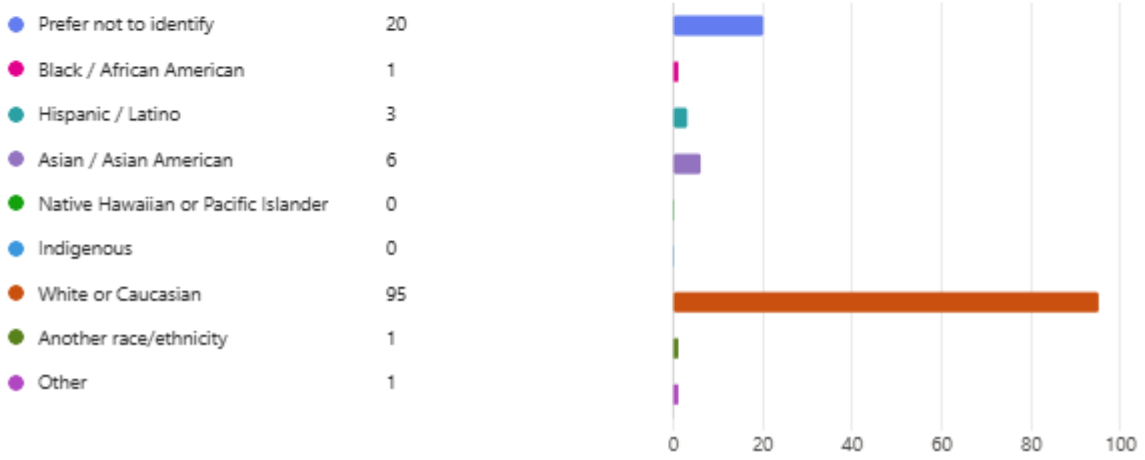
11. OPTIONAL Demographic Question: Gender

More details



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

More details



Id	What concerns, if any, do you have about the use of this technology?	Do you have any additional concerns about the use of technology (in case you ran out of space in section one)	What value, if any, do you see in the use of this technology?	Do you have additional comments/questions re what value do you see in this technology?	What would you want City leadership to consider when making a decision about the use of this technology?	Do you have additional comments/considerations that leadership should take into account when making a decision about this technology?	Do you have any additional comments or questions?
1	I oppose the use of this		Bone		Do not expand the		

	technology as it increases the negative outcomes for LGBT+, BIPOC and immigrant communities and increases harmful surveillance in our city at a time when at all government levels surveillance is being used to harm many communities			use of the these cameras and discontinue using them
2	Surveillance tools only serve to help commit violence against marginalized groups. In the past few weeks Seattle has seen SPD collude with ICE, Tukwila PD collude with ICE, and these agents & officers have violated the constitution and abducted citizens.			Consider how this surveillance technology is being used to target and hurt marginalized communities.
3	Cloud hosting puts data at risk of breaches, threatening to expose people who	RTCC can act as a license plate reader, and cloud based data storage would allow ICE to	None - it gives away our right to privacy and will be abused	Widespread access to spy on our community is not necessary and does not keep us safe.

	travel to WA for abortions or people escaping domestic violence	surveil and harm immigrant communities			Engage the community and find what people need. Address root causes. Consider how those in power will use this data to harm innocent people.	
4	Moving the on-premise RTCC database to an off-premise, cloud-hosted database exponentially risks people's personal information and their safety by exposing the RTCC information to access by any entity that can remotely access (whether authorized or not) the cloud-based database. Cloud-based software and databases are much more vulnerable to hacking than on-premise systems that have inherent	A remote RTCC database poses severe harms to vulnerable populations: Many anti-abortion states, including neighboring Idaho, have passed bounty hunter laws. This creates a market and demand to hunt down this data for people believed to have gone to Seattle to get reproductive healthcare. Homeless people, who have no option for privacy, are likely to become targets of mass surveillance.	none			city's legal liability when (not if) people's personal information is breached.

	physical barriers to access.	Customs and Border Control (CBC) and ICE can access the data directly, thereby circumventing Washington State Law. ICE has a history of accessing data directly from private surveillance companies that market their products to police, in order to circumvent state/local laws.		
5	We know that this technology disproportionately impacts homeless people, Black people, immigrants, and other communities that already have enough to deal with. Also, I don't trust these surveillance technologies. What are they really used for? What is done with the data they gather?	None		I want to urge City leadership to use an equity lens when considering making such a decision. Who is most impacted and why? Whose rights are being violated, whether intentionally or unintentionally? What else could these funds/resources be used for, instead of

					surveilling people?		
6	A cloud-based RTCC would weaken state laws and endanger women, trans folks, and immigrant residents. This technology should not be based in the cloud or with a private third party.		No value. We have it already and do not need it managed by a private third party out side of Washington state control.		Do not use this technology it will be used to punish those seeking Healthcare in Washington.		
7	Lack of safeguards for the data being collected, invasion of privacy, and likelihood that these tools will be used to target already marginalized communities. This technology will not make us any safer.		None.				
8	SPD already has a real time crime center. SPD's existing RTCC (iBase) is on-premise, so it doesn't create the risk of data being	Threat of harm to all people exercising First Amendment Rights of free speech, public protest and assembly Seattle has a	No. Creates a system ripe for abuse and potential to violate all residents' First and Fourth Amendment Rights Cloud-based	Surveillance technology will NOT aid law enforcement in solving crime. The 2024 paper that SPD cites states that	There are MANY effective tools the city could use to decrease community violence Violence interruption programs	We're devolving into a state of authoritarianism. Do you want to be part of the problem or solution?	SPD is assisting ICE SPD confirmed to Guy Oron that they have been providing "mutual aid" to

obtained from third parties or legal requests from those outside Washington state. There is no reason for SPD to obtain a cloud-based RTCC which would weaken state laws and endanger women, trans folks, and immigrant residents.

Threat of harm to abortion and gender-affirming healthcare Many anti-abortion states, including neighboring Idaho, have passed bounty hunter laws. This creates a market and demand to hunt down this data for people believed to have gone to Seattle to get reproductive healthcare. If SPD switches over to a cloud-hosted

long history of participatory democracy dating at least as far back as the 1919 general strike. Seattle has seen mass protests for labor rights, abortion rights, anti-war protests, and protests around issues of international trade policies, and most recently mass demonstrations advocating for a ceasefire in Gaza. Unfortunately, police violence against protesters is not unprecedented. After SPD's betrayal of the public trust in the summer of 2020, the city recently paid a $10M settlement. Violence against protestors in 2020 is one of the principal

software can be hacked. This happened in 2021 when hackers gained access to Verkada - giving them access to 150,000 cameras inside schools, hospitals, gyms, police stations, prisons, offices and women's health clinics RTCC software creates conditions that are ripe for police abuse, as it provides little, if any, oversight for how police use it, little documentation or auditable logs, and few transparency mechanisms. RTCC software like Fusus recruits a vast assortment of privately owned cameras that allow the company to

RTCC "appeared to have a relatively smaller impact on violent crime clearance (5% increase)," other studies of RTCC show no effect on violent crime clearance rates.
In a 40 year systematic review with meta-analysis of the efficacy of CCTV the authors concluded there were "no significant effects observed for violent crime" and "a body of research on the investigatory benefits of CCTV has yet to develop." Only 1% to 0.2% of ALPR captured license plates are either on a hot list or associated with any crime.RTCC software is expensive RTCC

work. Neighborhoods that have adopted a Cure Violence Model or Group Violence Intervention Models have seen homicides and assaults decrease 30-50%. The city could scale effective community-led solutions such as the Regional Peacekeepers Collective coordinated by the Regional Office of Gun Violence Prevention and the Rainier Beach Action Coalition and their Restorative Resolutions project, which has already reduced violence in the Rainier Beach neighborhood by 33%. Richmond, CA has chosen to invest in

ICE/Department of Homeland Security. SPD says its assistance dispersing community members so ICE can kidnap people doesn't violate the Keep Washington Working Act which bars local police from collaborating with ICE. Some of this "mutual aid" occurred while Interim Police Chief Shon Barnes was making the headline grabbing claim that he expects to go to jail because he won't cooperate with the Trump Administration.

SPD and Mayor Harrell refuse to respond to questions from Hard Pressed about how

RTCC database, we enable the criminalizatio n of those seeking reproductive care.
The rate of out-of-state abortions, those coming from other states to seek abortion in Washington, increased by 36% in 2023 and included 20 different states including neighboring Idaho and states as far away as Texas and Alabama.
Anti-abortion groups have a history of using license plate data.
RTCC software allows data to be shared across law enforcement agencies.
Third party agencies in anti-abortion states could use this data to criminally prosecute those seeking abortion in Washington state.

reasons that Seattle remains under the consent decree that it has been under for excessive use of force since 2012.
SPD has used existing surveillance systems to spy on peaceful protestors.
During the 2020 protests for racial justice, SPD used live video streaming to record peaceful protestors, and shared it with U.S. Marshalls, Washington State Department of Corrections, and to a private citizen volunteering at Seattle's emergency operations center (EOC).
SPD has continued to use existing surveillance to spy on protestors including

bypass laws and restrictions that normally limit police, including viewing camera footage without a warrant or ongoing consent from the owner.
The risk is not hypothetical as seen by other law enforcement agencies: In Pasco County, Florida, which operates an RTCC, the sheriff's office's predictive policing system encouraged officers to continuously monitor and harass residents for minor code violations such as missing mailbox numbers and overgrown grass.
SPD has a track record of officers abusing their access to

software are subscription products meaning the city will have to pay for it every single year.
RTCC software, and other companies selling subscriptions , operate on the land-and-expand strategy where it starts off small with a city to get its proverbial foot in the door and then increases the amount the city is buying from them every year. In other words, a for profit company will be pushing Seattle to spend even more money on its products every year.
The city cannot afford this ineffective and expensive technology - especially in light of the fact that

violence interruption and other community-led safety initiatives and they have seen a drop in the number of homicides.
This is in contrast to neighboring cities like Oakland and San Francisco that have increased their police budgets and have not seen a decline in violent crime.
Both violent crime and property crime can be reduced by community investments.
Investments restoring vacant land and community non-profits that tackle violence and build community lead to reductions in both violent crime and property crimes.
Many communities across the

many times ICE has asked for data sharing.
The only thing preventing ICE from accessing all of SPD's surveillance data (including 30 days of video and 90 days of license plate scans) is SPD's dubious claim that it will follow the Keep Washington Working Act & Washington Shield Law (read on for more info on how meaningless these assurances are) and won't cooperate with ICE.

Recently an Idaho mother and son were charged with kidnapping for allegedly taking a minor across state lines to access abortion care in Oregon. The state of Texas has already attempted to get data from Seattle Children's Hospital for any Texas residents receiving gender-affirming care. As soon as SPD switches over to a cloud-hosted RTCC database, red states will start issuing subpoenas to access data directly from Fusus.
Threat of harm to women, sexual assault and stalking survivors, and vulnerable marginalized community residents RTCC software including one on Sept. 23, 2023, that called for justice for the death of Jaahnavi Kandula, who died Jan. 23, 2023, as a result of being hit by SPD officer Kevin Dave while driving his officer vehicle as she walked through a marked crosswalk.
RTCC software is a vast network of cameras which can include doorbell cameras, drones, robots, fixed surveillance cameras, helicopters, hidden cameras, police body cameras, and cameras in schools and churches, among other settings.
RTCC opens up the opportunity for those exercising dissent to be tracked and surveillance technology. In 2021 SPD Officer Swartz used police data to stalk his ex-girlfriend; in 2020, an officer accessed confidential information about a domestic violence investigation and shared it with someone involved; and just last year, an officer performed an unauthorized search for personal reasons to reveal a citizen's firearm ownership.
The privatization of policing represented by relying on private consumers to expand the camera network undermines democratic values, effectively excluding Seattle residents from being Seattle is anticipating a $250 million shortfall in 2025
Looking at four other US cities that have deployed RTCCs, the average cost is $7.16 per person. With Seattle's 2020 population of 737,015, this would put the full-scale (post-pilot-phase) RTCC deployment by SPD in the ballpark of $5.3 million, not including the additional costs for the CCTV and ALPR expansion.
Even the paper referenced by SPD in the SIR mentions the "substantial costs associated with RTCCs, with initial costs ranging between several hundred thousand dollars to $11 million".
country are making investments in preventative community-centered approaches and are seeing a reduction in crime and violence in the community.
Violent crime can be reduced by investments in mental health treatment, providing substance-abuse-treatment facilities, and access to affordable housing.
Poverty and income inequality are associated with violence, especially assault and homicide.
Inequality predicts homicides better than any other variable.
Evidence supports that this is a causal link.
And direct income

companies like Fusus rely on private consumers to expand the camera network which gather enough data to reveal sensitive personal information, including where someone lives, works, and their religious affiliation. Individuals, homeowner associations, or businesses that opt into RTCC may be able to access the data directly from the vendor. Hostile individuals could access data to stalk or harass individuals. The threat to vulnerable communities is NOT hypothetical, as seen by the actions of other law enforcement agencies: NYP officers used mass surveillance	targeted, and risks the threat of police retaliation. Surveillance is about the power to watch and intervene in a variety of situations, whether criminal or not, and surveillance technology has the potential to have a chilling effect on free speech rights. In 2021 LAPD requested bulk camera data targeting Black Lives Matter protesters. In New York City there is evidence that NYPD has used surveillance technology to surveille Black Lives Matter protesters. Creates a system ripe for abuse and potential to violate all residents' First and Fourth	able to provide input and oversight on the growing Seattle surveillance apparatus. RTCC software like Fusus continually adds new image recognition algorithms and integrations with third-party applications via the software's AI capabilities. This continuous introduction of new and unvetted surveillance tools would be in violation of Seattle's Surveillance Ordinance.	support has been found to reduce firearm violence. Opening libraries and expanding library hours both reduce violence and property crimes.

technology to record and monitor everyone parked in front of a mosque, and Burmingham police also used this technology, in conjunction with other tools, to track Muslim residents.	Amendment Rights
Homeless residents, who have no option for privacy, are likely to become targets of mass surveillance.	Cloud-based software can be hacked. This happened in 2021 when hackers gained access to Verkada - giving them access to 150,000 cameras inside schools, hospitals, gyms, police stations, prisons, offices and women's health clinics
California is using AI to identify and target its homeless residents.	RTCC software creates conditions that are ripe for police abuse, as it provides little, if any, oversight for how police use it, little documentation or auditable logs, and few transparency mechanisms.
Threat of harm to immigrants	RTCC software like Fusus recruits a vast assortment of privately owned
ICE has a history of terrorizing immigrant communities.	
Jurisdictions that do not use local resources to enforce federal immigration laws have lower rates of crime,	

poverty, and unemployment than those that chose to collaborate. It was with this knowledge that the Keep Washington Working Act was passed to prevent data sharing between immigration and local law enforcement. RTCC software like Fusus can turn any camera into an automated license plate readers (ALPRs). By moving to a cloud-based platform, Customs and Border Control (CBC) and ICE can access automated license plate reader data directly; circumventing Washington State Law. ICE has a practice of accessing data directly from private ALPR surveillance companies	cameras that allow the company to bypass laws and restrictions that normally limit police, including viewing camera footage without a warrant or ongoing consent from the owner. The risk is not hypothetical as seen by other law enforcement agencies: In Pasco County, Florida, which operates an RTCC, the sheriff's office's predictive policing system encouraged officers to continuously monitor and harass residents for minor code violations such as missing mailbox numbers and overgrown grass.

	that market their products to police, in order to circumvent any local sanctuary laws. The department gets a lot of use out of this data, as seen by them running thousands of searches of ALPR databases in a single month as early as 2019. ICE's utilization of this data shows the degree of risk it poses to vulnerable communities. Police surveillance systems have been used by ICE and to target people seeking abortion healthcare even in sanctuary states The Burner and Notes from the Emerald City have details						
9	RTCC software is	There are MANY	no	Creates a system ripe	Threat of harm to all	Threat of harm to	Threat of harm to

expensive RTCC software are subscription products meaning the city will have to pay for it every single year. RTCC software, and other companies selling subscriptions, operate on the land-and-expand strategy where it starts off small with a city to get its proverbial foot in the door and then increases the amount the city is buying from them every year. In other words, a for profit company will be pushing Seattle to spend even more money on its products every year. The city cannot afford this ineffective and expensive technology - especially in	effective tools the city could use to decrease community violence Violence interruption programs work. Neighborhoods that have adopted a Cure Violence Model or Group Violence Intervention Models have seen homicides and assaults decrease 30-50%. The city could scale effective community-led solutions such as the Regional Peacekeepers Collective coordinated by the Regional Office of Gun Violence Prevention and the Rainier Beach Action Coalition and their Restorative Resolutions project, which has already reduced	Surveillance technology will NOT aid law enforcement in solving crime. The 2024 paper that SPD cites states that RTCC "appeared to have a relatively smaller impact on violent crime clearance (5% increase)," other studies of RTCC show no effect on violent crime clearance rates. In a 40 year systematic review with meta-analysis of the efficacy of CCTV the authors concluded there were “no significant effects observed for violent crime” and “a body of research on the investigatory benefits of CCTV has yet to develop.” Only 1% to	for abuse and potential to violate all residents’ First and Fourth Amendment Rights Cloud-based software can be hacked. This happened in 2021 when hackers gained access to Verkada - giving them access to 150,000 cameras inside schools, hospitals, gyms, police stations, prisons, offices and women’s health clinics RTCC software creates conditions that are ripe for police abuse, as it provides little, if any, oversight for how police use it, little documentation or auditable logs, and few transparency mechanisms. RTCC	people exercising First Amendment Rights of free speech, public protest and assembly Seattle has a long history of participatory democracy dating at least as far back as the 1919 general strike. Seattle has seen mass protests for labor rights, abortion rights, anti-war protests, and protests around issues of international trade policies, and most recently mass demonstrations advocating for a ceasefire in Gaza. Unfortunately, police violence against protesters is not unprecedented. After SPD’s betrayal of the public trust in the summer of	immigrants ICE has a history of terrorizing immigrant communities. Jurisdictions that do not use local resources to enforce federal immigration laws have lower rates of crime, poverty, and unemployment than those that chose to collaborate. It was with this knowledge that the Keep Washington Working Act was passed to prevent data sharing between immigration and local law enforcement. RTCC software like Fusus can turn any camera into an automated license plate readers (ALPRs). By moving to a cloud-based platform, Customs and Border Control (CBC) and ICE can	women, sexual assault and stalking survivors, and vulnerable marginalized community residents RTCC software companies like Fusus rely on private consumers to expand the camera network which gather enough data to reveal sensitive personal information, including where someone lives, works, and their religious affiliation. Individuals, homeowner associations, or businesses that opt into RTCC may be able to access the data directly from the vendor. Hostile individuals could access data to stalk or harass individuals. The threat to vulnerable

light of the fact that Seattle is anticipating a $250 million shortfall in 2025 Looking at four other US cities that have deployed RTCCs, the average cost is $7.16 per person. With Seattle's 2020 population of 737,015, this would put the full-scale (post-pilot-phase) RTCC deployment by SPD in the ballpark of $5.3 million, not including the additional costs for the CCTV and ALPR expansion. Even the paper referenced by SPD in the SIR mentions the "substantial costs associated with RTCCs, with initial costs ranging between several hundred thousand	violence in the Rainier Beach neighborhood by 33%. Richmond, CA has chosen to invest in violence interruption and other community-led safety initiatives and they have seen a drop in the number of homicides. This is in contrast to neighboring cities like Oakland and San Francisco that have increased their police budgets and have not seen a decline in violent crime. Both violent crime and property crime can be reduced by community investments. Investments restoring vacant land and community non-profits that tackle violence and build community	0.2% of ALPR captured license plates are either on a hot list or associated with any crime.	software like Fusus recruits a vast assortment of privately owned cameras that allow the company to bypass laws and restrictions that normally limit police, including viewing camera footage without a warrant or ongoing consent from the owner. The risk is not hypothetical as seen by other law enforcement agencies: In Pasco County, Florida, which operates an RTCC, the sheriff's office's predictive policing system encouraged officers to continuously monitor and harass residents for minor code violations such as missing	2020, the city recently paid a $10M settlement. Violence against protestors in 2020 is one of the principal reasons that Seattle remains under the consent decree that it has been under for excessive use of force since 2012. SPD has used existing surveillance systems to spy on peaceful protestors. During the 2020 protests for racial justice, SPD used live video streaming to record peaceful protestors, and shared it with U.S. Marshalls, Washington State Department of Corrections, and to a private citizen volunteering at Seattle's emergency	access automated license plate reader data directly; circumventing Washington State Law. ICE has a practice of accessing data directly from private ALPR surveillance companies that market their products to police, in order to circumvent any local sanctuary laws. The department gets a lot of use out of this data, as seen by them running thousands of searches of ALPR databases in a single month as early as 2019. ICE's utilization of this data shows the degree of risk it poses to vulnerable communities.	communities is NOT hypothetical, as seen by the actions of other law enforcement agencies: NYP officers used mass surveillance technology to record and monitor everyone parked in front of a mosque, and Burmingham police also used this technology, in conjunction with other tools, to track Muslim residents. Homeless residents, who have no option for privacy, are likely to become targets of mass surveillance. California is using AI to identify and target its homeless residents.

dollars to $11 million".	lead to reductions in both violent crime and property crimes. Many communities across the country are making investments in preventative community-centered approaches and are seeing a reduction in crime and violence in the community. Violent crime can be reduced by investments in mental health treatment, providing substance-abuse-treatment facilities, and access to affordable housing. Poverty and income inequality are associated with violence, especially assault and homicide. Inequality predicts homicides	mailbox numbers and overgrown grass. SPD has a track record of officers abusing their access to surveillance technology. In 2021 SPD Officer Swartz used police data to stalk his ex-girlfriend; in 2020, an officer accessed confidential information about a domestic violence investigation and shared it with someone involved; and just last year, an officer performed an unauthorized search for personal reasons to reveal a citizen's firearm ownership. The privatization of policing represented by relying on private consumers to expand the camera	operations center (EOC). SPD has continued to use existing surveillance to spy on protestors including including one on Sept. 23, 2023, that called for justice for the death of Jaahnavi Kandula, who died Jan. 23, 2023, as a result of being hit by SPD officer Kevin Dave while driving his officer vehicle as she walked through a marked crosswalk. RTCC software is a vast network of cameras which can include doorbell cameras, drones, robots, fixed surveillance cameras, helicopters, hidden cameras, police body cameras, and cameras in schools and churches,

	better than any other variable. Evidence supports that this is a causal link. And direct income support has been found to reduce firearm violence. Opening libraries and expanding library hours both reduce violence and property crimes.	network undermines democratic values, effectively excluding Seattle residents from being able to provide input and oversight on the growing Seattle surveillance apparatus. RTCC software like Fusus continually adds new image recognition algorithms and integrations with third-party applications via the software's AI capabilities. This continuous introduction of new and unvetted surveillance tools would be in violation of Seattle's Surveillance Ordinance.	among other settings. RTCC opens up the opportunity for those exercising dissent to be tracked and targeted, and risks the threat of police retaliation. Surveillance is about the power to watch and intervene in a variety of situations, whether criminal or not, and surveillance technology has the potential to have a chilling effect on free speech rights. In 2021 LAPD requested bulk camera data targeting Black Lives Matter protesters. In New York City there is evidence that NYPD has used surveillance technology to surveille Black Lives

			Matter protesters.		
10	spend money on socials safety nets instead of surveillance	zero	stop trying to put us under constant surveillance and fix the homeless and housing crisis with social safety nets, higher ages and taxing the rich		Yeah, you;re ruining the city because you won't tax the rich and help the homeless
11	Establishing a penopticon to monitor citizens is the height of autocratic dystopia. It will has already been used to target LGBTQIA+, minorities, and those seeking abortions.	None.	Eliminate it in its entirety. Redistribute the police budget to transit and climate resilience.	The First and Fourth Amendments.	Here's your chance to be on the right side of history, or be just more autocrats.
12	I worry that the data gathered by these cameras will end up sold to and/or held by private corporations, further invading our privacy as private individuals. With a move to cloud-based RTCC, these violations are	None, SPD already have onsite RTCC.	Do you trust any of the private corporations who may have an interest in this data to use it responsibly? What is the benefit to residents to move to cloud as opposed to the existing system?		

basically assured. Moving RTCC offsite opens up data security risks and would enable other states to circumvent our Shield Law and Keep WA Working Act, which exist to protect people seeking reproductive healthcare and immigrant workers. SPD already have an RTCC, and have already used it to abuse Seattle residents (stalking former partners, inappropriately sharing information regarding a domestic violence investigation with an involved party, monitoring peaceful protestors after the protest is over, etc).

13	This proposal is a risk to Washingtonian's privacy and freedoms to go about their lives, as there is a strong potential that this technology will make it easier for bad actors to misuse civilians' information for unequal policing and political persecution.			
14	Racial profiling, surveillance state, increasingly untrustworthy federal government (which SPD sometimes cooperates with). SPD should have to earn the trust of the people, and they have not done so.	None		
15	RTCC poses a massive risk for everyone. The more data stored in a location the more of a tempting	Absolutely none. This technology is an abuse of power with a universal adapter and should be	The issues on RTCC are very well documented and all came up last year when the Seattle community,	If the city cares about protecting the people of Seattle, it should remove RTCC.

target it is. This is both as a target for ICE & other law enforcement agencies to access (which they have) and for hackers to target. RTCC companies have been caught using data obtained from hacks & security breaches in their algorithms. https://www.404media.co/license-plate-reader-company-flock-is-building-a-massive-people-lookup-tool-leak-shows/ ICE has access RTCC databases from across the country including Washington State & supposed "sanctuary" states. https://www.404media.co/ice-taps-into-nationwide-	removed from Seattle.	Office of Civil Rights, and Community Surveillance Working Group all recommended against RTCC. Why is the city considering expanding this technology now when it is being used by ICE to disappear people and its abuses are so documented? Where is the money for this expansion coming from? Relatedly, how is there money for this while the city is doing austerity and cutting services? Why was SPD allowed to submit the original SIR for RTCC without estimating an annual cost only to be allowed to say it needed millions of dollars per

ai-enabled-camera-network-data-shows/ Law enforcement in states with abortion bans have utilized RTCC to search nationwide databases of surveillance data. Including surveillance data from abortion sanctuary states to look for people that have had abortions. https://www.404media.co/a-texas-cop-searched-license-plate-cameras-nationwide-for-a-woman-who-got-an-abortion/ No law, contract, agreement, or court decision can stop ICE from accessing RTCC databases because the current federal administratio n does not		year for RTCC as soon as the technology was approved?

	care about or follow the law or court decisions That's even before considering all of the cases of individual officers abusing RTCC to spy on and blackmail people.				
16	It is a breach of privacy for the general public and will put vulnerable communities at risk.	There is no reason for SPD to obtain a cloud-based RTCC It would weaken state laws and endanger women, trans folks, and immigrant residents.	None	It's effect on vulnerable communities.	
17	RTCCs dramatically expand the city's surveillance capabilities, collecting real-time data about people's locations, habits, and associations. This infrastructure reinforces racial profiling, targets already over-		Any claims of value are minimal and overstated. While RTCCs are sometimes credited with minor improvements in clearing cases, such as a 5% increase in Chicago, there is no meaningful evidence that they reduce gun violence	City leadership should consider how much public money is being funneled into a system that has little proven impact on safety. As outlined by the ACLU and Stop Surveillance City, these funds—over $2 million—	Before making any decisions, the City should hold public hearings and require independent studies on the impact of surveillance on civil rights. Communities most impacted by policing must have a voice in this process. Seattle has a

	policed communities, and puts undocumented people and those seeking reproductive or gender-affirming care at risk. According to Stop Surveillance City, Seattle police have a documented history of abusing surveillance tools, including spying on protestors and activists. There's no reason to believe a Real-Time Crime Center would be any different, especially with no independent oversight or accountability.		or make communities safer. Stop LAPD Spying and other watchdog groups have shown these systems mainly serve to intensify police presence, not solve crime. They create a high-tech illusion of safety while failing to address the root causes of harm.	would be far better spent on proven community-based solutions like housing, youth programs, mental health care, and violence interruption. RTCCs are not a public safety necessity—they are a political and technological overreach.	choice: continue down a path of expanding surveillance and criminalization, or invest in real public safety rooted in care, equity, and community. We urge you to reject the RTCC proposal.
18	This will be used to further surveil and criminalize our most vulnerable neighbors! This is a huge invasion of	Waste of money! In a cost of living crisis in an increasingly unaffordable city, in a housing and groceries crisis, where safety nets are being cut,		That it is a waste of money and a huge violation of residents' privacy.	

	privacy for everyone!	this is the absolute last thing any regular person needs!		
19	SPD already has a real time crime center. SPD's existing RTCC (iBase) is on-premise, so it doesn't create the risk of data being obtained from third parties or legal requests from those outside Washington state. There is no reason for SPD to obtain a cloud-based RTCC which would weaken state laws and endanger women, trans folks, and immigrant residents. Moving the on-premise RTCC database to an off premise, cloud-hosted database managed by a third-party, private company would enable	None that would outweigh its harms.		This technology is expensive and studies show it has either no, or negligible, impact on solving crime. I want City dollars to be spent on solutions that have been PROVEN to be effective at reducing crime — such as community-led violence interruption programs — not systems like this which have not. See this document (https://docs.google.com/document/d/14EhNiDMb7M8Z7TafyZsbxGOfdelDOGzRYxZNd3biwIE/edit) for specific examples of the many effective tools the city should use instead, which are

other states to circumvent WA state's Shield Law and Keep WA Working Act, which are meant to protect both people seeking reproductive healthcare and immigrant workers. My concerns include the examples of harm caused by this type of technology listed here: https://docs.google.com/document/d/14EhNiDMb7M8Z7TafyZsbxGOfdelDOGzRYxZNd3biwIE/edit This technology is expensive and studies show it has either no, or negligible, impact on solving crime. I want City dollars to be spent on solutions that have been PROVEN to be effective at reducing		actually shown to decrease violence.

	crime — such as community-led violence interruption programs — not systems like this which have not.				
20	I strongly oppose moving our onsite real-time crime center (RTCC) to the cloud. It will be less protected there and more vulnerable to requests for data from other states — states that have strong, negative views of women's right to abortion, of trans people, and of immigrants.			I want my city to use viable, proven solutions like violence interruption programs, mental health services, and investments in libraries and green spaces, etc., to make our city safer and better. Not surveillance, and not by moving RTCC in a way that will put people in danger.	
21	I am against the use of this technology.	I am against the expansion.	None		
22	That SPD will use this to target, harass, and profile marginalized community members		Absolutely no value	SPD has a long history of using their tools and resources against the community to the point of being under federal	Stop wasting our resources and tax dollars on SPD and fund what the community actually needs!

				oversight for many years- they do not need more tools and resources!	
23	RTCCs dramatically expand the city's surveillance capabilities, collecting real-time data about people's locations, habits, and associations. This infrastructure reinforces racial profiling, targets already over-policed communities, and puts undocumented people and those seeking reproductive or gender-affirming care at risk. According to Stop Surveillance City, Seattle police have a documented history of abusing surveillance tools, including spying on protestors	Any claims of value are minimal and overstated. While RTCCs are sometimes credited with minor improvements in clearing cases, such as a 5% increase in Chicago, there is no meaningful evidence that they reduce gun violence or make communities safer. Stop LAPD Spying and other watchdog groups have shown these systems mainly serve to intensify police presence, not solve crime. They create a high-tech illusion of safety while failing to address the root causes of harm.	City leadership should consider how much public money is being funneled into a system that has little proven impact on safety. As outlined by the ACLU and Stop Surveillance City, these funds—over $2 million—would be far better spent on proven community-based solutions like housing, youth programs, mental health care, and violence interruption. RTCCs are not a public safety necessity—they are a political and technological overreach.	Before making any decisions, the City should hold public hearings and require independent studies on the impact of surveillance on civil rights. Communities most impacted by policing must have a voice in this process. Seattle has a choice: continue down a path of expanding surveillance and criminalization, or invest in real public safety rooted in care, equity, and community. We urge you to reject the RTCC proposal.

	and activists. There's no reason to believe a Real-Time Crime Center would be any different, especially with no independent oversight or accountabilit y.						
24	My concern is that this technology will violate Seattlite's right to privacy, and make Seattlites anxious and paranoid about being watched all the time.	N/A	None, it would be a complete waste of our already thin budget.	N/A	Privacy is a RIGHT.	N/A	N/A
25	Surveillance is a powerful tool of social repression and state violence against its populace	It's use to support ICE and their enforced dissappearan ces of peoples.	None. It will only be used to harm people.	We keep us safe, not endless surveillance	The immense harm it will cause to already marginalized and abused portions of our population. NO POLICE STATE		Could we use this to track the City Council members movements?
26	I do not want more police surveillance.		None. SPD is big enough and has enough resources.		Expanding other programs to benefit residents material situation.		

Appendix B: Public Comment Period (6/03/25 to 6/23/25)

27	This is an invasion of privacy and implements strategies utilized by fascist governments.	None	This technology does not represent the values of Seattle, and it is NOT what the people want. Please do not allow this abuse of power in our city.
28	It's frightening, if could be hacked and used against people and it won't reduce crime.	None, we do not need increased surveillance.	How it's going to affect everyone, the cost vs. benefit and how little it's going to make a difference in crime.
29	Surveillance is used primarily to harm people of color and other marginalized groups. Police in this city are already bad enough at protecting the people, providing our data and privacy is only going to lead to more unnecessary violence. Allowing even more citywide surveillance is a huge injustice to		City leadership must place restrictions on this technology, cops already patrol in these areas more frequently. This frequent patrolling is what causes divides, inequalities, and contributes to higher crime rates. The addition to real time high definition cameras protects no one and can only be used

	the city. Desired expansion into even more marginalized spaces will not help cops catch bad guys, it will help cops racially profile, brutalize, and discriminate against our own people.			to retroactively bring some sort of justice. Any funds towards this project could easily be used towards other programs that truly keep communities safe such as hard reduction, community centers, and funding for education.	
30	I oppose the expansion of surveillance	none	expensive and ineffective	FOCUS ON INVESTING IN OUR HEALTH AND EDUCATION, NOT POLICING	
31	This technology will make it less safe for marginalized people in Seattle. Transgender and queer people are already targeted by police, as seen in police brutality recently at Cal Anderson Park on May 24. Efforts to criminalize being	There is no value.		Consider the danger of the federal government or military coming to Seattle to take our data and use it for their own means. And consider the people who don't want to have their identity constantly found on a police	Rather than investing in this technology and the constant sweeps on homeless encampments, we should spend more money giving them affordable housing. South Lake Union and other areas must create affordable housing for

	transgender are being made in many other states (and at a federal level). Allowing more security cameras to track and store information about us is extraordinary dangerous. Moreover, this detracts from us being a sanctuary city for migrants. We need to protect our friends and family no matter what. Migrants provide an essential role in our economy, and without them we will face higher costs, longer wait times at our favorite restaurants, and we will lose what makes Seattle special.			security screen.	those who need it.
32	ICE and Border patrol are using cloud-based surveillance tools to	There is no evidence whatsoever that RTCC lives up to the vendor	I do not see any value in this technology.	There is no evidence whatsoever that that RTCC has any public	

conduct warrant-less searches and violate sanctuary city laws. Vendor contracts are insufficient to protect the data. This has been reported on by 404 media. https://www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data-shows/ Furthermore the Trump administration has informed ICE employees that they are at liberty to conduct warrant-less searches https://www.thehandbasket.co/p/ice-warrantless-arrests-castanon-nava Any expansion of this technology is a weapon in the hands of the Trump administration and puts our immigrant communities at risk.	claims. The 2024 paper that SPD cites states that RTCC "appeared to have a relatively smaller impact on violent crime clearance (5% increase)," other studies of RTCC show no effect on violent crime clearance rates. This technology is costly and a waste of city dollars at a time when the cities deficit and federal cuts threaten vulnerable communities. This technology and any expansion of it and especially ending its definition of a "pilot" without any evaluation of the program and only 3 weeks after its implementation in unconscionable.		benefit. In fact, I have spoken to Brian Maxey, who stated that the benefits of RTCC were "anecdotal and hypothetical" Cloud-bases surveillance tools are a weapon in the hands of the Trump administration and will be used to violate our sanctuary laws. We will hold our city leaders accountable for the decision to pursue RTCC and to ignore public input which has been largely dis favorable of the technology.

33	This adds to SPD's enormous surveillance network. This allows data to go to the cloud where it can be hacked. This allows SPD to cooperate with ICE, CBP, etc.	None	Why would we want to expand SPD's already enormous surveillance network? Why would we want to do anything that could lead to data sharing with ICE, CBP, etc.?
34	It can be used to target women, immigrants, and LGBTQ+ individuals. SPD already has plenty of surveilance technology. The cost of this program could be better spent on hiring.	None	Consider the privacy rights of the population at large. This is police state stuff!
35	Surveillance is a powerful tool of social oppression. This will only increase violence. It will only lead to more discriminatio n and division. Adding more surveillance technology will only increase crime and increase violence	No value. This is dangerous.	Think of where else the funding for this could go. Preventive care for the people!

	towards innocent people		
36	Many. Please do not expand.		Please direct funds towards affordable housing and human services.
37	This technology is a threat to our first and fourth amendment rights. It will be harmful to women, sexual assault and stalking survivors, and vulnerable marginalized community residents because the third party RTCC software is not protected and can be used negatively on law-abiding community members by out of state individuals or prosecuting agents. It will allow circumnavigation of WA state's Shield Law and Keep WA Working Act, which	I see no value in this technology. Studies show that it is actually not effective in reducing violent crime. But there are many cases where it has been used by law enforcement to harass people and divulge private information about people fleeing domestic violence and other state violence which is wrong.	I'd urge them to consider where that money could be spent elsewhere to actually improve the lives of those underserved or most vulnerable. Why not scale the effective community-led solutions such as the Regional Peacekeepers Collective coordinated by the Regional Office of Gun Violence Prevention and the Rainier Beach Action Coalition and their Restorative Resolutions project, which has already reduced violence in the Rainier

	WA residents voted on and needs to be upheld. It is also expensive and would needlessly add to our already $250 million shortfall of the 2025 budget. Studies also show that it is actually not affective in reducing violent crime. Please, do not vote to outsource this surveillance to a third part.			Beach neighborhood by 33%? Both violent crime and property crime can be reduced by community investments. Investments restoring vacant land and community non-profits that tackle violence and build community lead to reductions in both violent crime and property crimes.	
38	More surveillance is not more safety, and adding even more cameras is not the answer to reducing crime or other issues. More cameras on the streets will be used for purposes other than safety and this should not be done under any	None, it will not aid in keeping Seattle safe.	I see no value in this, and I understand this to be purely a move to further surveil and monitor the residents of Seattle.	How this technology will truly be implemented over safety measures. This technology is easily manipulated and used to profile people.	More cameras is not the answer.

	circumstances.						
39	The use of these cameras so widely has been policy acceptable specifically because it was not used by police. I am deeply concerned about the privacy implications of this data was used freely by the police. Not to mention the Trump administration.		None.		How this change violates the trust of Seattle's citizens. How this helps further the authoritarian goals of the Trump administration.		
40	I am concerned about the potential for cloud-based systems to enable data to be accessed by other parties and thus circumvent Washington's protections such as the Shield Law and Keep Washington Working laws.	I am concerned about any third part private company having access to law enforcement data. I prefer the the RTCC be kept on premise rather than off premise.	I do not see value in expanding this technologoy to be for cloud-based systems.	Please, please do take the perspectives of your constituents into account. We do not know how things will move federally and with AI in the future, we need to move cautiously to uphold our core constitutional values.	See the above comments. This is a risky step, without clear benefit, that opens Washingtonian's up to greater surveillance by federal and third party companies. We can't fully know how data captured now will be used in the future. I fully support the SPD in accessing information	Please see above comments.	Remember that we need to make decisions now with a forethought to our future generations. No decision will be perfect but we need to consider privacy and freedom with the awareness that these rights are not ensured to be respected moving forward.

			to solve crimes. I do not support maintaining this information on the cloud by a third party private company, without greater data protections. Thank you so much for hearing me.	
41	Increasing surveillance will increase racial profiling, and make it easier for the police and state agencies to track and target vulnerable individuals & groups, putting them in more danger. The technology is used to criminalize & harm my immigrant neighbors, neighbors who live unsheltered, neighbors who use drugs, neighbors who work in the sex trade, and my		Consider how the use and expansion and sharing of this technology puts your already vulnerable constituents in more danger, and contributes to ever widening state repression and control of the people.	

	neighbors of color.					
42	I am concerned about how it might be used outside of the state and beyond our state laws, bounty hunter laws from Idaho, for example. Other examples could be federal over reach. Not into this tech. Not down. No, please.	I do not approve of this level of invasive surveillance in general.	No value that I approve of.	Who this is actually going to effect, who is this immediately going to impact, and who is it actual helping. How could this be abused, by who, and what would the consequences of that be? Are there better uses for these funds and personnel?	Don't do it.	Please, don't do it.
43	Yes, I do have massive concerns about this technology in just the fact that it's yet another part of mass governmental surveillance that's been slowly expanding over the past few decades. The program already has already been likely used for helping track cross-state abortions. And as more			Consider whether it's worth conducting mass-surveillance on your constituents in exchange for extremely minor benefits, if any. Consider whether it's worth contributing to the erosion of both people's right to privacy, as well as assisting in interstate hunts for		

	and more states take away people's rights as we've seen over the past few years, it'll only be used for such purposes even further. Do not spy on citizens. Do not spy on your constituents. SPD is more than capable of doing its job without engaging in mass-surveillance.		people trying to exercise their bodily autonomy. And don't lie to yourselves about how this will be "limited" or "only for certain criminal activities" because these kinds of things will and have always, always, ALWAYS expanded and have ALWAYS been co-opted. Please do not do this.	
44	Expanding civilian transportation technology to police makes us less safe, not more safe. The police do not need more data. In addition there is a history of police departments collaborating with federal authorities, such as ICE. Integrating traffic data with the police decreases	This is an irrelevant question without also considering the direct and potential harm this would cause. When those are first evaluated the risk is so high, that no value in implementing this camera integration project could offset.		Remember that the current federal government wants to deport immigrants black and brown residents, stop abortion healthcare, and ban gender healthcare. Every step you take to expand the surveillance infrastructure is building more tools that they will

	the barrier to federal authorities' access, which increases the danger to our most vulnerable citizens.				use when they have the chance, regardless of your intent.	
45	I am concerned that this expansion will endanger those traveling to our state seeking reproductive Healthcare and transgender healthcare.	We have RTCC technology and do not need to involve a 3rd party.	I understand the value of the current system to law enforcement. The cons outweigh the pros when we send it to the cloud and enable a nationwide spying capability.	See #1		
46	This is clear over-reach and abuse of surveillance technology against citizens; moreover it weakens our state's protections		Quite valuable to authoritarian style government			It should be bone-chilling that we have normalized such intrusiveness
47	It would put our privacy at risk for being free to travel between states for lifesaving healthcare needs.		I don't think it's safe to outsource like this.	That it could override Washington's laws for privacy protection!	THE PEOPLE DON'T WANT IT.	
48	Exposing information to ICE that		None			

	they should not have		
49	RTCC and CCTV do not provide any benefit to mitigate all of the harm they cause. They neither reduce violence nor increase clearance (arrest rates) for violent crime. A 40 year systematic review with meta-analysis of the efficacy of CCTV – concludes "no significant effects observed for violent crime or disorder". Despite RTCC's high price tag ("initial costs ranging between several hundred thousand dollars and $11 million"), studies of RTCC show no effect on violent crime clearance rates. These technologies will foster the	None	RTCC and CCTV do not provide any benefit to mitigate all of the harm they cause. They neither reduce violence nor increase clearance (arrest rates) for violent crime. A 40 year systematic review with meta-analysis of the efficacy of CCTV – concludes "no significant effects observed for violent crime or disorder". Despite RTCC's high price tag ("initial costs ranging between several hundred thousand dollars and $11 million"), studies of RTCC show no effect on violent crime clearance rates.

very spirit of distrust and disunity that you claim to hope they will end. that response should be increased investment in equitable and evidence-based strategies for gun violence prevention while also offering meaningful support to victims and survivors. Violence can be reduced by investments in violence interruption programs, mental health treatment, substance-abuse-treatment facilities, affordable housing, emergency financial assistance, and libraries. Poverty and income inequality are associated with violence, especially assault and homicide. Evidence

supports that this is a causal link, inequality predicts homicides better than any other variable. Surveillance contributes to disinvestment in communities. Seattle is required to have a balanced budget, every dollar spent on surveillance is a dollar that cannot be invested in any of the evidence-based strategies for violence prevention listed above or otherwise invested in our communities as mental health supports, programs for kids, parks/public spaces, affordable housing, jobs/job skill training, and food access. Police have a lengthy

history of mis-using and abusing surveillance to blackmail people, target people based on their religion, spy on people, and cover up violence by police. SPD has a history of abusing the surveillance tools it already has, including to spy on protestors, stalk former romantic partners, and leak information about domestic violence victims. Additionally, SPD has a history of providing inaccurate information in Surveillance Impact Reports (SIRs) for the technologies it wants. SPD has done this with CCTV & RTCC at least once already. On February 12, 2024, SPD Captain

James Britt told the public that SPD would absolutely not actively monitor CCTV feeds in the RTCC. Nick Zajchowski from SPD contradicted this in the June 26, 2024 meeting of the Community Surveillance Working Group saying that SPD would be actively monitoring the camera feeds at least part of the time. Cloud-based surveillance tools destroy Seattle's ability to act as a sanctuary city and render Washington State's Shield Law and the Keep Washington Working Act meaningless. Surveillance creates a map of people's lives that Immigration and Customs

	Enforcement (ICE) and law enforcement & private individuals in other states, including ones with bans on abortion and/or transgender healthcare, can access through the for-profit companies storing it. The CCTV pilot specifies the Aurora corridor and includes the Planned Parenthood located on Aurora Avenue and 105th. The rate of people coming from other states to seek abortion in Washington increased by 36% in 2023.		
50	So many! It makes our city less safe. It takes away our privacy protections.	None.	Outsourcing means we would lose our Seattle/WA privacy laws which we cannot do!
51	Having sensitive information essentially		We are in scary times. Your public words of

owned and outsourced to an unregulated, private 3rd party system is a huge concern and puts many vulnerable populations at risk of exploitation - people from other states coming to WA for gender affirming care or abortions, for one thing ... it also puts immigrants at risk and violates (in an indirect way) the reassurance that has been provided that the police are not collecting data and sharing it with ICE, etc; if a 3rd party has access to this information and shares it with ICE or others, and we are complicit in supplying the information to a third party system, then we are complicit in the whole system.	reassurance about protecting the safety of the most vulnerable among us mean very little if your actions directly or indirectly put those same folks at great risk. WA is a beacon of hope in the country right now. I have friends from all over who have talked about moving here, visiting here, etc. Those same people will absolutely NOT come, even to visit, if they know their information is being collected and shared with private, unregulated 3rd party systems. They are not safe where they stand. And I feel like I (as a queer person) am standing on sand every day, even in this

					“progressive” state because of decisions like these. Please protect us.
52	Seriously? The GOP/Trump administration has ICE and Homeland Security officers acting like the Secret Police, and Seattle City Council proposes to make surveillance data available to those entities (and others)?	This change will enable other states to circumvent WA state’s Shield Law and Keep WA Working Act, which are meant to protect both people seeking reproductive healthcare and immigrant workers. SPD already has a real time crime center. SPD's existing RTCC (iBase) is on-premise, so it doesn't create the risk of data being obtained from third parties or legal requests from those outside Washington state. There is no reason for SPD to obtain a cloud-based RTCC which would weaken state	None whatsoever.		Whether the City leadership really wants to make violations of Constitutional rights even easier--and whether the majority of the city's electorate supports this use of our tax dollars (especially given the city's budget woes).

		laws and endanger women, trans folks, and immigrant residents.			
53	Many anti-abortion states, including neighboring Idaho, have passed bounty hunter laws. This creates a market and demand to hunt down this data for people believed to have gone to Seattle to get reproductive healthcare. If SPD switches over to a cloud-hosted RTCC database, we enable the criminalization of those seeking reproductive care.		none		The need to protect our vulnerable citizens from additional, unnecessary surveillance.
54	My concerns are vast but it boils down to a concern for the safety and well being of women receiving access to safe abortions. Beyond that	I wouldn't want this available to law enforcement even in a climate that WASN'T objectively out of control, as	I do not see the value of this if a safer society is the goal. And I imagine that a safer society is a non-controversial idea.	Giving a powerful tool like this to assist the illegal deportation of immigrants is not good for this city, or this country.	Consider the extremism that is becoming more palatable by the sheer mass of petitions, requests and threats from this

	we know this data will be available to border patrol, ICE etc and I don't think in this climate anyone can argue that this will make anyone safer. This will negatively affect quality of life for many people.	this current one is.			Presidential administratio n and those in support of it; consider it daily and stay sane.		
55	This further endangers women, trans folks, and immigrant residents.		None		Reveals sensitive personal info including where someone lives, works, and their religious affiliation.		
56	Unnecessary surveillance by a government that is already targeting vulnerable people, as well as people who are standing up for our democracy.		none that outweighs the costs and risks		Do not risk harming vulnerable peoples.		
57	In the current political environment there is danger that this information will be used by agencies	None	I can see no value in sharing this information. If there is a legitimate need then the information can be	None who is going to use	Who is going to use this information and for what purpose.	None	Do not approve this sharing of information.

	that not law abiding.	requested in a lawful manner in a supena.		
58	Please, PLEASE, help protect our innocent residents and citizens! Please please do NOT help ICE!	Sure, great, but NOT to aid illegal and wrong actions on behalf of bad people!	Please do not use this technology to hurt innocent people. Please!	I thought I read on Substack that our police chief was going to protect our people. ?
59	I don't want it to track people to the degree it will be able to. It's an invasion of privacy. I do not want to put my tax dollars towards this.			
60	I'm concerned about federal access to this information. If it's not in the cloud no one can ask Seattle, Seattle PD, or a cloud provider for it.	No value for individuals; tremendous value for ICE.	Don't use it. The fact of the existence of the data makes it exceedingly vulnerable to the feds. Even if access is granted "accidentally" or if the courts require that the data is handed over.	
61	You can be used to Target defenseless individuals.	None	Do the disadvantages outweigh the advantages?	

62	This database is available to ICE and will be used to fuel its brutal, careless, and illegal campaign against immigrants regardless of their status and anyone who challenges their illegal actions that ignore the rule of law, the Constitution, and the authority of the Congress.				The reason given in question 1 is sufficient to reject use of this technology. ICE has become a threat to every American.	
63	police power overreach		recycling it into something to enable peace	just don't do it	handshakes are more powerful than digital eyes	
64	RTCC software is a cloud-based software platform designed for real-time crime centers to integrate multiple surveillance technologies such as cameras, automated license plate readers (ALPRs), CCTV, among other police surveillance	This technology can be abused and accessed by third parties when stored in the cloud and poses a threat of harm and misuse to all people exercising First Amendment Rights of free speech, public protest and assembly. It	None	This powerful technology should not be passed without an opportunity for serious consideration and public comment. We are seeing a dangerous rise in authoritarianism at the federal level and having a cloud-based RTCC runs the risk of having	They need to consult with privacy advocates, including the ACLU and Electronic Frontier Foundation, to fully understand the threat	Once you go down this road, you cannot easily turn back, so you should be incredibly careful and thoughtful.

tools. RTCC software like Fusus can turn any camera into an automated license plate readers (ALPRs) which gather enough data to reveal sensitive personal information, including where someone lives, works, and their religious affiliation. The City Council's attempt to move the on-premise RTCC database to an off premise, cloud-hosted database managed by a third-party, private company. This change will enable other states to circumvent WA state's Shield Law and Keep WA Working Act, which are meant to protect both people	is also expensive, unnecessary, and has little likelihood of making Seattle any safer.	Seattle contribute to spying on private citizens who are exercising their legal rights.

	seeking reproductive healthcare and immigrant workers. SPD already has a real time crime center. SPD's existing RTCC (iBase) is on-premise, so it doesn't create the risk of data being obtained from third parties or legal requests from those outside Washington state. There is no reason for SPD to obtain a cloud-based RTCC which would weaken state laws and endanger women, trans folks, and immigrant residents			
65	I have so many concerns. (1) Creation of a RTCC will create a system that will become a MAGNET for abuse as well as the potential to	SPD already has a real time crime center. SPD's existing RTCC (iBase) is on-premise, so it doesn't create the risk of data being obtained	None. I see only potential for abuse and harm	Do you want to create a police and surveillance state in our area? Do you want this to be your legacy? Are your values that much aligned with

violate the 1st & 4th amendment rights of all residents. (2) Surveillance technology does not aid law enforcement in solving crimes (despite all the tv shows and movies...) (3) This technology represents a very real threat of harm to immigrants - if footage is obtained by ICE, CBP, etc (4) This technology poses a threat of harm to all people exercising First Amendment Rights of free speech, public protest and assembly – especially because its use puts our city solidly into the "surveillance state" and SPD (with its history of required federal	from third parties or legal requests from those outside Washington state. There is no reason for SPD to obtain a cloud-based RTCC which would weaken state laws and endanger women, trans folks, and immigrant residents. AND this technology is expensive.		our autocrat Dictator wanna be President??

	oversight due to bad behavior) has a history of using surveillance systems to spy on peaceful protesters. . (5) Threat of harm to women, sexual assault and stalking survivors, and vulnerable marginalized community residents - historic use of the technology to track religious and sexual minorities, to stalk women/sexual abuse survivors, immigrants, etc (6) Threat of harm by being used to track and intimidate by residents seeking abortion and gender-affirming healthcare		
66	the use of this cloud based platform could allow ICE and border control to	None	Do whatever is in your power to stop the use of a cloud based program that could be

	access information for at risk immigrants.		used by ICE and therefore put at risk immigrants in unnecessary harms way.	
67	We know that these tools, which were put in place by King County Housing Authority, have generated surveillance data ICE has searched in order to look for people. Not criminals—just immigrants in most cases that had no criminal record, but who could have their status revoked so they could be detained and deported. This is not in the spirit of separating state and local resources from federal ICE enforcement. Don't expand the use of these tools.	In terms of sending surveillance data to national, private databases, there are no benefits and many dangerous uses to which this data could be put.	Consider the uses this data is being put to that have nothing to do with local law enforcement.	Instead of expanding the use of these systems, their use needs to be curtailed. As a resident I and others will be watching this issue closely; this is where we need to put "welcoming" promises into action.

68	Invasion of privacy and data sharing risks to indifivual freedoms	It gives the government too much power	None		Do not expand the abiity of the government to spy on the population		
69	It is used by law enforcement all over the country. It can be used to track women who have had an abortion, to track immigrants and to track LBGTQ people.		None that outlays the threat to our citizens.		Taking care of all our citizens.		
70	These technologies can easily be used to target those the trump administratio n is (trans youth, BIPOC, immigrants)		It's not helpful, please stop spending money on surveillance		Do not approve the use of this technology please.		
71	RTCC software is a cloud-based software platform designed for real-time crime centers to integrate multiple surveillance technologies such as cameras, automated license plate	See above	See above	See above	See above	See above	See above

readers (ALPRs), CCTV, among other police surveillance tools. RTCC software like Fusus can turn any camera into an automated license plate readers (ALPRs) which gather enough data to reveal sensitive personal information, including where someone lives, works, and their religious affiliation.

The City Council is attempting to move the on-premise RTCC database to an off premise, cloud-hosted database managed by a third-party, private company. This change will enable other states to circumvent WA state's Shield Law and Keep WA

	Working Act, which are meant to protect both people seeking reproductive healthcare and immigrant workers. SPD already has a real time crime center. SPD's existing RTCC (iBase) is on-premise, so it doesn't create the risk of data being obtained from third parties or legal requests from those outside Washington state. There is no reason for SPD to obtain a cloud-based RTCC which would weaken state laws and endanger women, trans folks, and immigrant residents. Threat of harm to abortion and gender-affirming		

healthcare: Many anti-abortion states, including neighboring Idaho, have passed bounty hunter laws. This creates a market and demand to hunt down this data for people believed to have gone to Seattle to get reproductive healthcare. If SPD switches over to a cloud-hosted RTCC database, we enable the criminalizatio n of those seeking reproductive care.

The rate of out-of-state abortions, those coming from other states to seek abortion in Washington, increased by 36% in 2023 and included 20 different states including neighboring Idaho and states as far

away as Texas and Alabama.

Anti-abortion groups have a history of using license plate data. RTCC software allows data to be shared across law enforcement agencies. Third party agencies in anti-abortion states could use this data to criminally prosecute those seeking abortion in Washington state.

Recently an Idaho mother and son were charged with kidnapping for allegedly taking a minor across state lines to access abortion care in Oregon. The state of Texas has already attempted to get data from Seattle Children's Hospital for any Texas residents receiving

	gender-affirming care. As soon as SPD switches over to a cloud-hosted RTCC database, red states will start issuing subpoenas to access data directly from Fusus. Threat of harm to women, sexual assault and stalking survivors, and vulnerable marginalized community residents RTCC software enabled a Texas cop to search surveillance data from across the county, including Washington State, other states with abortion "sanctuary" laws, and non-police entities including the King County Housing Authority, for someone that had an	

abortion RTCC software makes it impossible to keep surveillance data from ICE. Local police departments are very cozy with ICE and RTCC makes it easier for them to casually share surveillance data. And, RTCC means ICE is able to search nationwide databases of surveillance data including data from police departments in Washington State, other states with “sanctuary” laws, and non-police entities including the King County Housing Authority. RTCC software was used by police to spy on “immigration protests”

	RTCC software companies like Fusus rely on private consumers to expand the camera network which gather enough data to reveal sensitive personal inform					
72	Threat of harm to abortion and gender-affirming healthcare Many anti-abortion states, including neighboring Idaho, have passed bounty hunter laws. This creates a market and demand to hunt down this data for people believed to have gone to Seattle to get reproductive healthcare. If SPD switches over to a cloud-hosted RTCC database, we enable the criminalizatio n of those seeking	Threat of harm to all people exercising First Amendment Rights of free speech, public protest and assembly Seattle has a long history of participatory democracy dating at least as far back as the 1919 general strike. Seattle has seen mass protests for labor rights, abortion rights, anti-war protests, and protests around issues of international trade policies, and most recently mass demonstratio	None	Most people want to live their lives in peace and have no idea about the harms of this type of data collection. I doubt that many people will give input because they aren't experts in this type of technology and naively believe that it will make them safer.	A functioning democracy needs the population to feel more empowered, not less. This type of technology takes power away from individual citizens and gives it to who knows who-- the highest bidder?	

reproductive care. The rate of out-of-state abortions, those coming from other states to seek abortion in Washington, increased by 36% in 2023 and included 20 different states including neighboring Idaho and states as far away as Texas and Alabama. Anti-abortion groups have a history of using license plate data. RTCC software allows data to be shared across law enforcement agencies. Third party agencies in anti-abortion states could use this data to criminally prosecute those seeking abortion in Washington state. Recently an Idaho mother and son were charged with kidnapping for allegedly	ns advocating for a ceasefire in Gaza. Unfortunately, police violence against protesters is not unprecedented. After SPD's betrayal of the public trust in the summer of 2020, the city recently paid a $10M settlement. Violence against protestors in 2020 is one of the principal reasons that Seattle remains under the consent decree that it has been under for excessive use of force since 2012. SPD has used existing surveillance systems to spy on peaceful protestors. During the 2020 protests for racial justice, SPD used live video

taking a minor across state lines to access abortion care in Oregon. The state of Texas has already attempted to get data from Seattle Children's Hospital for any Texas residents receiving gender-affirming care. As soon as SPD switches over to a cloud-hosted RTCC database, red states will start issuing subpoenas to access data directly from Fusus. Threat of harm to women, sexual assault and stalking survivors, and vulnerable marginalized community residents RTCC software enabled a Texas cop to search surveillance data from across the	streaming to record peaceful protestors, and shared it with U.S. Marshalls, Washington State Department of Corrections, and to a private citizen volunteering at Seattle's emergency operations center (EOC). SPD has continued to use existing surveillance to spy on protestors including including one on Sept. 23, 2023, that called for justice for the death of Jaahnavi Kandula, who died Jan. 23, 2023, as a result of being hit by SPD officer Kevin Dave while driving his officer vehicle as she walked through a marked crosswalk. RTCC software is a vast network

county, including Washington State, other states with abortion “sanctuary” laws, and non-police entities including the King County Housing Authority, for someone that had an abortion RTCC software makes it impossible to keep surveillance data from ICE. Local police departments are very cozy with ICE and RTCC makes it easier for them to casually share surveillance data. And, RTCC means ICE is able to search nationwide databases of surveillance data including data from police departments in Washington State, other	of cameras which can include doorbell cameras, drones, robots, fixed surveillance cameras, helicopters, hidden cameras, police body cameras, and cameras in schools and churches, among other settings. RTCC opens up the opportunity for those exercising dissent to be tracked and targeted, and risks the threat of police retaliation. Surveillance is about the power to watch and intervene in a variety of situations, whether criminal or not, and surveillance technology has the potential to have a chilling effect on free speech rights. In 2021

states with "sanctuary" laws, and non-police entities including the King County Housing Authority. RTCC software was used by police to spy on "immigration protests" RTCC software companies like Fusus rely on private consumers to expand the camera network which gather enough data to reveal sensitive personal information, including where someone lives, works, and their religious affiliation. Individuals, homeowner associations, or businesses that opt into RTCC may be able to access the data directly from the vendor. Hostile	LAPD requested bulk camera data targeting Black Lives Matter protesters. In New York City there is evidence that NYPD has used surveillance technology to surveille Black Lives Matter protesters. Creates a system ripe for abuse and potential to violate all residents' First and Fourth Amendment Rights Cloud-based software can be hacked. This happened in 2021 when hackers gained access to Verkada - giving them access to 150,000 cameras inside schools, hospitals, gyms, police stations, prisons, offices and

individuals could access data to stalk or harass individuals. The threat to vulnerable communities is NOT hypothetical, as seen by the actions of other law enforcement agencies: NYP officers used mass surveillance technology to record and monitor everyone parked in front of a mosque, and Burmingham police also used this technology, in conjunction with other tools, to track Muslim residents. Homeless residents, who have no option for privacy, are likely to become targets of mass surveillance. California is using AI to identify and target its homeless residents.	women's health clinics RTCC software creates conditions that are ripe for police abuse, as it provides little, if any, oversight for how police use it, little documentation or auditable logs, and few transparency mechanisms. RTCC software like Fusus recruits a vast assortment of privately owned cameras that allow the company to bypass laws and restrictions that normally limit police, including viewing camera footage without a warrant or ongoing consent from the owner. The risk is not hypothetical as seen by other law enforcement agencies: In

Threat of harm to immigrants ICE has a history of terrorizing immigrant communities. Jurisdictions that do not use local resources to enforce federal immigration laws have lower rates of crime, poverty, and unemployme nt than those that chose to collaborate. It was with this knowledge that the Keep Washington Working Act was passed to prevent data sharing between immigration and local law enforcement. RTCC software like Fusus can turn any camera into an automated license plate readers (ALPRs). By moving to a cloud-based platform, Customs and Border	Pasco County, Florida, which operates an RTCC, the sheriff's office's predictive policing system encouraged officers to continuously monitor and harass residents for minor code violations such as missing mailbox numbers and overgrown grass. SPD has a track record of officers abusing their access to surveillance technology. In 2021 SPD Officer Swartz used police data to stalk his ex-girlfriend; in 2020, an officer accessed confidential information about a domestic violence investigation and shared it with someone

	Control (CBC) and ICE can access automated license plate reader data directly; circumventing Washington State Law. ICE has a practice of accessing data directly from private ALPR surveillance companies that market their products to police, in order to circumvent any local sanctuary laws.	involved; and just last year, an officer performed an unauthorized search for personal reasons to reveal a citizen's firearm ownership. The privatization of policing represented by relying on private consumers to expand the camera network undermines democratic values, effectively excluding Seattle residents from being able to provide input and oversight on the growing Seattle surveillance.		
73	This takes away our liberty and privacy for living normal legal lives. The government does not have the right to use any kind of cameras to watch our		Because it has gotten out of hand and gone too far it needs to be stopped altogether. Government can not be trusted to use it legally. It is	Personal rights and liberties.

	people. That is destroying the rights we were given in the constitution.		abusive. So no.				
74	The City Council is attempting to move the on-premise RTCC database to an off premise, cloud-hosted database managed by a third-party, private company. This change will enable other states to circumvent WA state's Shield Law and Keep WA Working Act, which are meant to protect both people seeking reproductive healthcare and immigrant workers. SPD already has a real time crime center. SPD's existing RTCC (iBase) is on-premise, so it doesn't create the risk of data being	Threat of harm to abortion and gender-affirming healthcare Many anti-abortion states, including neighboring Idaho, have passed bounty hunter laws. This creates a market and demand to hunt down this data for people believed to have gone to Seattle to get reproductive healthcare. If SPD switches over to a cloud-hosted RTCC database, we enable the criminalizatio n of those seeking reproductive care. The rate of out-of-state abortions, those coming from other states to seek abortion in		Threat of harm to immigrants ICE has a history of terrorizing immigrant communities. Jurisdictions that do not use local resources to enforce federal immigration laws have lower rates of crime, poverty, and unemployme nt than those that chose to collaborate. It was with this knowledge that the Keep Washington Working Act was passed to prevent data sharing between immigration and local law enforcement. RTCC software like Fusus can turn any camera into an automated license plate readers (ALPRs).	Creates a system ripe for abuse and potential to violate all residents' First and Fourth Amendment Rights Cloud-based software can be hacked. This happened in 2021 when hackers gained access to Verkada - giving them access to 150,000 cameras inside schools, hospitals, gyms, police stations, prisons, offices and women's health clinics RTCC software creates conditions that are ripe for police abuse, as it provides little, if any, oversight for	There are MANY effective tools the city could use to decrease community violence Violence interruption programs work. Neighborhoo ds that have adopted a Cure Violence Model or Group Violence Intervention Models have seen homicides and assaults decrease 30-50%. The city could scale effective community-led solutions such as the Regional Peacekeeper s Collective coordinated by the Regional Office of Gun Violence Prevention and the Rainier Beach Action

obtained from third parties or legal requests from those outside Washington state. There is no reason for SPD to obtain a cloud-based RTCC which would weaken state laws and endanger women, trans folks, and immigrant residents.	Washington, increased by 36% in 2023 and included 20 different states including neighboring Idaho and states as far away as Texas and Alabama. Anti-abortion groups have a history of using license plate data. RTCC software allows data to be shared across law enforcement agencies. Third party agencies in anti-abortion states could use this data to criminally prosecute those seeking abortion in Washington state. Recently an Idaho mother and son were charged with kidnapping for allegedly taking a minor across state lines to access abortion care in Oregon. The state of Texas has already	By moving to a cloud-based platform, Customs and Border Control (CBC) and ICE can access automated license plate reader data directly; circumventing Washington State Law. ICE has a practice of accessing data directly from private ALPR surveillance companies that market their products to police, in order to circumvent any local sanctuary laws. The department gets a lot of use out of this data, as seen by them running thousands of searches of ALPR databases in a single month as early as 2019. ICE's utilization of this data shows the	how police use it, little documentation or auditable logs, and few transparency mechanisms. RTCC software like Fusus recruits a vast assortment of privately owned cameras that allow the company to bypass laws and restrictions that normally limit police, including viewing camera footage without a warrant or ongoing consent from the owner. The risk is not hypothetical as seen by other law enforcement agencies: In Pasco County, Florida, which operates an RTCC, the sheriff's office's predictive policing system encouraged	Coalition and their Restorative Resolutions project, which has already reduced violence in the Rainier Beach neighborhood by 33%.	

attempted to get data from Seattle Children's Hospital for any Texas residents receiving gender-affirming care. As soon as SPD switches over to a cloud-hosted RTCC database, red states will start issuing subpoenas to access data directly from Fusus.	degree of risk it poses to vulnerable communities.	officers to continuously monitor and harass residents for minor code violations such as missing mailbox numbers and overgrown grass.
Threat of harm to women, sexual assault and stalking survivors, and vulnerable marginalized community residents	Threat of harm to all people exercising First Amendment Rights of free speech, public protest and assembly	SPD has a track record of officers abusing their access to surveillance technology. In 2021 SPD Officer Swartz used police data to stalk his ex-girlfriend; in 2020, an officer accessed confidential information about a domestic violence investigation and shared it with someone involved; and just last year, an officer performed an unauthorized search for personal reasons to reveal a citizen's firearm ownership.
RTCC software enabled a Texas cop to search surveillance data from across the county, including Washington State, other states with abortion "sanctuary" laws, and non-police	Seattle has a long history of participatory democracy dating at least as far back as the 1919 general strike. Seattle has seen mass protests for labor rights, abortion rights, anti-war protests, and protests around issues of international trade policies, and most recently mass demonstratio ns advocating for a ceasefire in Gaza. Unfortunately , police violence against protesters is not unprecedent	

entities including the King County Housing Authority, for someone that had an abortion

RTCC software makes it impossible to keep surveillance data from ICE. Local police departments are very cozy with ICE and RTCC makes it easier for them to casually share surveillance data. And, RTCC means ICE is able to search nationwide databases of surveillance data including data from police departments in Washington State, other states with "sanctuary" laws, and non-police entities including the King County Housing Authority.

ed. After SPD's betrayal of the public trust in the summer of 2020, the city recently paid a $10M settlement. Violence against protestors in 2020 is one of the principal reasons that Seattle remains under the consent decree that it has been under for excessive use of force since 2012.

SPD has used existing surveillance systems to spy on peaceful protestors. During the 2020 protests for racial justice, SPD used live video streaming to record peaceful protestors, and shared it with U.S. Marshalls, Washington State Department of

The privatization of policing represented by relying on private consumers to expand the camera network undermines democratic values, effectively excluding Seattle residents from being able to provide input and oversight on the growing Seattle surveillance apparatus.

RTCC software like Fusus continually adds new image recognition algorithms and integrations with third-party applications via the software's AI capabilities. This continuous introduction of new and unvetted surveillance tools would be in violation

RTCC software was used by police to spy on "immigration protests" RTCC software companies like Fusus rely on private consumers to expand the camera network which gather enough data to reveal sensitive personal information, including where someone lives, works, and their religious affiliation. Individuals, homeowner associations, or businesses that opt into RTCC may be able to access the data directly from the vendor. Hostile individuals could access data to stalk or harass individuals. The threat to vulnerable communities is NOT

Corrections, and to a private citizen volunteering at Seattle's emergency operations center (EOC). SPD has continued to use existing surveillance to spy on protestors including including one on Sept. 23, 2023, that called for justice for the death of Jaahnavi Kandula, who died Jan. 23, 2023, as a result of being hit by SPD officer Kevin Dave while driving his officer vehicle as she walked through a marked crosswalk. RTCC software is a vast network of cameras which can include doorbell cameras, drones, robots, fixed surveillance cameras, helicopters, hidden

of Seattle's Surveillance Ordinance. Surveillance technology will NOT aid law enforcement in solving crime. The 2024 paper that SPD cites states that RTCC "appeared to have a relatively smaller impact on violent crime clearance (5% increase)," other studies of RTCC show no effect on violent crime clearance rates. In a 40 year systematic review with meta-analysis of the efficacy of CCTV the authors concluded there were "no significant effects observed for violent crime" and "a body of research on the investigatory benefits of

hypothetical, as seen by the actions of other law enforcement agencies: NYP officers used mass surveillance technology to record and monitor everyone parked in front of a mosque, and Burmingham police also used this technology, in conjunction with other tools, to track Muslim residents. Homeless residents, who have no option for privacy, are likely to become targets of mass surveillance. California is using AI to identify and target its homeless residents.	cameras, police body cameras, and cameras in schools and churches, among other settings. RTCC opens up the opportunity for those exercising dissent to be tracked and targeted, and risks the threat of police retaliation. Surveillance is about the power to watch and intervene in a variety of situations, whether criminal or not, and surveillance technology has the potential to have a chilling effect on free speech rights. In 2021 LAPD requested bulk camera data targeting Black Lives Matter protesters. In New York City there is evidence that NYPD has	CCTV has yet to develop." Only 1% to 0.2% of ALPR captured license plates are either on a hot list or associated with any crime. RTCC software is expensive RTCC software are subscription products meaning the city will have to pay for it every single year. RTCC software, and other companies selling subscriptions , operate on the land-and-expand strategy where it starts off small with a city to get its proverbial foot in the door and then increases the amount the city is buying from them every year. In other words, a for profit company will be pushing Seattle to

	used surveillance technology to surveille Black Lives Matter protesters.	spend even more money on its products every year. The city cannot afford this ineffective and expensive technology - especially in light of the fact that Seattle is anticipating a $250 million shortfall in 2025 Looking at four other US cities that have deployed RTCCs, the average cost is $7.16 per person. With Seattle's 2020 population of 737,015, this would put the full-scale (post-pilot-phase) RTCC deployment by SPD in the ballpark of $5.3 million, not including the additional costs for the CCTV and ALPR expansion. Even the paper referenced by

						SPD in the SIR mentions the "substantial costs associated with RTCCs, with initial costs ranging between several hundred thousand dollars to $11 million".	
75	This change will enable other states to circumvent WA state's Shield Law and Keep WA Working Act, which are meant to protect both people seeking reproductive healthcare and immigrant workers. SPD already has a real time crime center. SPD's existing RTCC (iBase) is on-premise, so it doesn't create the risk of data being obtained from third parties or legal requests from those	Threat of harm to immigrants ICE has a history of terrorizing immigrant communities. Jurisdictions that do not use local resources to enforce federal immigration laws have lower rates of crime, poverty, and unemployment than those that chose to collaborate. It was with this knowledge that the Keep Washington Working Act was passed to prevent data sharing between immigration and local law enforcement.	Creates a system ripe for abuse and potential to violate all residents' First and Fourth Amendment Rights Cloud-based software can be hacked. This happened in 2021 when hackers gained access to Verkada - giving them access to 150,000 cameras inside schools, hospitals, gyms, police stations, prisons, offices and women's health clinics RTCC	There is no value to the proposed change, only harm.	There are MANY effective tools the city could use to decrease community violence Violence interruption programs work. Neighborhoods that have adopted a Cure Violence Model or Group Violence Intervention Models have seen homicides and assaults decrease 30-50%. The city could scale effective community-led solutions such as the Regional Peacekeepers Collective	Protect our rights, do not make the proposed change. Use options that have been proven to make a positive difference instead.	Drop this proposal. NO cloud-based offsite RTCC!

outside Washington state. There is no reason for SPD to obtain a cloud-based RTCC which would weaken state laws and endanger women, trans folks, and immigrant residents.

Threat of harm to abortion and gender-affirming healthcare

Many anti-abortion states, including neighboring Idaho, have passed bounty hunter laws. This creates a market and demand to hunt down this data for people believed to have gone to Seattle to get reproductive healthcare. If SPD switches over to a cloud-hosted RTCC database, we enable the criminalizatio

RTCC software like Fusus can turn any camera into an automated license plate readers (ALPRs).

By moving to a cloud-based platform, Customs and Border Control (CBC) and ICE can access automated license plate reader data directly; circumventing Washington State Law.

ICE has a practice of accessing data directly from private ALPR surveillance companies that market their products to police, in order to circumvent any local sanctuary laws. The department gets a lot of use out of this data, as seen by them running thousands of searches of

software creates conditions that are ripe for police abuse, as it provides little, if any, oversight for how police use it, little documentation or auditable logs, and few transparency mechanisms.

RTCC software like Fusus recruits a vast assortment of privately owned cameras that allow the company to bypass laws and restrictions that normally limit police, including viewing camera footage without a warrant or ongoing consent from the owner.

The risk is not hypothetical as seen by other law enforcement agencies: In Pasco County,

coordinated by the Regional Office of Gun Violence Prevention and the Rainier Beach Action Coalition and their Restorative Resolutions project, which has already reduced violence in the Rainier Beach neighborhood by 33%.

Richmond, CA has chosen to invest in violence interruption and other community-led safety initiatives and they have seen a drop in the number of homicides. This is in contrast to neighboring cities like Oakland and San Francisco that have increased their police budgets and have not seen a decline in violent crime.

n of those seeking reproductive care.

The rate of out-of-state abortions, those coming from other states to seek abortion in Washington, increased by 36% in 2023 and included 20 different states including neighboring Idaho and states as far away as Texas and Alabama.

Anti-abortion groups have a history of using license plate data. RTCC software allows data to be shared across law enforcement agencies. Third party agencies in anti-abortion states could use this data to criminally prosecute those seeking abortion in Washington state.

Recently an Idaho

ALPR databases in a single month as early as 2019. ICE's utilization of this data shows the degree of risk it poses to vulnerable communities.

Threat of harm to all people exercising First Amendment Rights of free speech, public protest and assembly

Seattle has a long history of participatory democracy dating at least as far back as the 1919 general strike. Seattle has seen mass protests for labor rights, abortion rights, anti-war protests, and protests around issues of international trade policies, and most recently mass demonstratio ns advocating

Florida, which operates an RTCC, the sheriff's office's predictive policing system encouraged officers to continuously monitor and harass residents for minor code violations such as missing mailbox numbers and overgrown grass.

SPD has a track record of officers abusing their access to surveillance technology. In 2021 SPD Officer Swartz used police data to stalk his ex-girlfriend; in 2020, an officer accessed confidential information about a domestic violence investigation and shared it with someone involved; and just last year,

Both violent crime and property crime can be reduced by community investments. Investments restoring vacant land and community non-profits that tackle violence and build community lead to reductions in both violent crime and property crimes.

Many communities across the country are making investments in preventative community-centered approaches and are seeing a reduction in crime and violence in the community.

Violent crime can be reduced by investments in mental health treatment, providing substance-

mother and son were charged with kidnapping for allegedly taking a minor across state lines to access abortion care in Oregon.

The state of Texas has already attempted to get data from Seattle Children's Hospital for any Texas residents receiving gender-affirming care. As soon as SPD switches over to a cloud-hosted RTCC database, red states will start issuing subpoenas to access data directly from Fusus.

Threat of harm to women, sexual assault and stalking survivors, and vulnerable marginalized community residents

RTCC software enabled a

for a ceasefire in Gaza.

Unfortunately, police violence against protesters is not unprecedented. After SPD's betrayal of the public trust in the summer of 2020, the city recently paid a $10M settlement. Violence against protestors in 2020 is one of the principal reasons that Seattle remains under the consent decree that it has been under for excessive use of force since 2012.

SPD has used existing surveillance systems to spy on peaceful protestors. During the 2020 protests for racial justice, SPD used live video

an officer performed an unauthorized search for personal reasons to reveal a citizen's firearm ownership.

The privatization of policing represented by relying on private consumers to expand the camera network undermines democratic values, effectively excluding Seattle residents from being able to provide input and oversight on the growing Seattle surveillance apparatus.

RTCC software like Fusus continually adds new image recognition algorithms and integrations with third-party applications via the

abuse-treatment facilities, and access to affordable housing.

Poverty and income inequality are associated with violence, especially assault and homicide. Inequality predicts homicides better than any other variable. Evidence supports that this is a causal link. And direct income support has been found to reduce firearm violence.

Opening libraries and expanding library hours both reduce violence and property crimes.

Texas cop to search surveillance data from across the county, including Washington State, other states with abortion “sanctuary” laws, and non-police entities including the King County Housing Authority, for someone that had an abortion RTCC software makes it impossible to keep surveillance data from ICE. Local police departments are very cozy with ICE and RTCC makes it easier for them to casually share surveillance data. And, RTCC means ICE is able to search nationwide databases of surveillance data including data from	streaming to record peaceful protestors, and shared it with U.S. Marshalls, Washington State Department of Corrections, and to a private citizen volunteering at Seattle’s emergency operations center (EOC). SPD has continued to use existing surveillance to spy on protestors including including one on Sept. 23, 2023, that called for justice for the death of Jaahnavi Kandula, who died Jan. 23, 2023, as a result of being hit by SPD officer Kevin Dave while driving his officer vehicle as she walked through a marked crosswalk. RTCC software is a vast network	software’s AI capabilities. This continuous introduction of new and unvetted surveillance tools would be in violation of Seattle’s Surveillance Ordinance. Surveillance technology will NOT aid law enforcement in solving crime. The 2024 paper that SPD cites states that RTCC "appeared to have a relatively smaller impact on violent crime clearance (5% increase),” other studies of RTCC show no effect on violent crime clearance rates. In a 40 year systematic review with meta-analysis of the efficacy of CCTV the

police departments in Washington State, other states with "sanctuary" laws, and non-police entities including the King County Housing Authority. RTCC software was used by police to spy on "immigration protests" RTCC software companies like Fusus rely on private consumers to expand the camera network which gather enough data to reveal sensitive personal information, including where someone lives, works, and their religious affiliation. Individuals, homeowner associations, or businesses that opt into RTCC may be able to	of cameras which can include doorbell cameras, drones, robots, fixed surveillance cameras, helicopters, hidden cameras, police body cameras, and cameras in schools and churches, among other settings. RTCC opens up the opportunity for those exercising dissent to be tracked and targeted, and risks the threat of police retaliation. Surveillance is about the power to watch and intervene in a variety of situations, whether criminal or not, and surveillance technology has the potential to have a chilling effect on free speech	authors concluded there were "no significant effects observed for violent crime" and "a body of research on the investigatory benefits of CCTV has yet to develop." Only 1% to 0.2% of ALPR captured license plates are either on a hot list or associated with any crime. RTCC software is expensive RTCC software are subscription products meaning the city will have to pay for it every single year. RTCC software, and other companies selling subscriptions, operate on the land-and-expand strategy where it starts off

access the data directly from the vendor. Hostile individuals could access data to stalk or harass individuals. The threat to vulnerable communities is NOT hypothetical, as seen by the actions of other law enforcement agencies: NYP officers used mass surveillance technology to record and monitor everyone parked in front of a mosque, and Burmingham police also used this technology, in conjunction with other tools, to track Muslim residents. Homeless residents, who have no option for privacy, are likely to become targets of mass surveillance. California is	rights. In 2021 LAPD requested bulk camera data targeting Black Lives Matter protesters. In New York City there is evidence that NYPD has used surveillance technology to surveille Black Lives Matter protesters.	small with a city to get its proverbial foot in the door and then increases the amount the city is buying from them every year. In other words, a for profit company will be pushing Seattle to spend even more money on its products every year. The city cannot afford this ineffective and expensive technology - especially in light of the fact that Seattle is anticipating a $250 million shortfall in 2025 Looking at four other US cities that have deployed RTCCs, the average cost is $7.16 per person. With Seattle's 2020 population of 737,015, this would put the full-scale

	using AI to identify and target its homeless residents.	(post-pilot-phase) RTCC deployment by SPD in the ballpark of $5.3 million, not including the additional costs for the CCTV and ALPR expansion. Even the paper referenced by SPD in the SIR mentions the "substantial costs associated with RTCCs, with initial costs ranging between several hundred thousand dollars to $11 million".		
76	I am concerned about putting seekers of reproductive care and gender affirming care, and immigrants at risk of having their personal identifying information shared with law enforcement. Washington State has the Shield Act	While I would say it could help prevent or discourage youth gun violence, I do not think that is the case. What would really prevent youth gun violence is economic and cultural opportunities for youth and connectedness amongst our communities.	Our country is in a slide toward authoritarianism. We see officers in face masks seizing people without judicial warrants authorizing them to do so, and we know those who are detained in this way are not having	

and Keep WA Working Act which were passed to protect people, but a cloud-based RTCC would not be bound to follow those laws. I am also concerned about surveillance data being used against people exercising their first amendment rights in protest against the government. Especially considering the current national climate in which people are being detained when they haven't broken the law, I am very much opposed to moving to a cloud-based RTCC that makes Washingtonian's data available to third parties and circumvents Washington's	Surveillance cameras do not create any of those things, and in fact they destabilize families and communities if they are used to aid in the detention of immigrants.	their due process rights honored. Seattle should not be taking any steps that can make it easier for our vulnerable neighbors to be tracked down and kidnapped by federal agents.

	more robust privacy and human rights protections.				
77	RTCC, as it is currently being used and disseminated, seems fine, but an expansion to the "Cloud," making it accessible by ICE, etc, would be very detrimental to our civil liberties, especially at this wrought time when ICE is being used as a secret police by a president who doesn't respect the rule of law and the Constitution.				
78	Over stepping of citizens privacy.		Vote it down		
79	This cloud-based change (rather than the current on-premise system) will enable other states to share sensitive data about people and thereby circumvent	NONE. We have systems in place that are safer for citizens that work well. And there are many other approaches, such as violence interruption programs,	Consider ALL of these points and the data that backs them up: https://docs.google.com/document/d/14EhNiDMb7M8Z7TafyZsbxGOfdelDOGzR	I feel so strongly about this, that if my representative (and the city-wide representatives) vote in favor of this system, I will work very very hard to make	Why has City Council not publicized its consideration of this system more widely, held community hearings, and aggressively searched for feedback. (It has a ring of

WA state's Shield Law and Keep WA Working Act, which are meant to protect people seeking reproductive healthcare, gender-affirming care, and immigrant workers. We know the pressures are real because data from Washington Medicaid Services has been shared with DHS and ICE WITHOUT its permission (or even knowledge). It would also be a threat to demonstrator s exercising their first amendment right. (The city is still under a 2012(!) consent decree for abridging those rights!) Seattle already uses its existing surveillance system to watch	and investments in housing and mental health programs, that we could take to solve crime problems without the risks this system would place on us:	YxZNd3biwIE/edit?tab=t.0	sure they are not elected next time.	the House GOP passing legislation in the middle of the night.)

demonstrators. We do NOT need to expand this capability.

Surveillance technology does NOT help law enforcement in fighting crime! The 2024 paper that SPD cites states that RTCC "appeared to have a relatively smaller impact on violent crime clearance (5% increase)," other studies of RTCC show no effect on violent crime clearance rates. In a 40 year systematic review with meta-analysis of the efficacy of CCTV the authors concluded there were "no significant effects observed for violent crime" and "a body of research on the

	investigatory benefits of CCTV has yet to develop." RRTC is expensive! Let's use the money toward solving our housing problems rather than surveilling Seattleites. PLEASE DO NOT FORCE SEATTLE TO PARTICIPATE IN A GROWING SURVEILLANCE STATE. DO NOT VOTE FOR RRTC SOFTWARE!						
80	RTCC software like Fusus can turn any camera into an automated license plate readers (ALPRs). By moving to a cloud-based platform, Customs and Border Control (CBC) and ICE can access automated license plate reader data directly;	Yes, I do because it has been used in the past against peaceful protestors. Also, this data has been used to stalk and intimidate people for personal reasons. Outrageous! The data has also been used to monitor and track certain communities.	None.	Consider all the harms and the cost! There are many effective tools the city of Seattle could use instead that DO WORK! Violence interruption programs work such as the Regional Peacekeepers Collective which has reduced violence in the Rainier	Do not consign Seattle to becoming a Surveillance State! RTCC software like Fusu continually adds new image algorithms and integrations with third party applications via the software's AI capabilities - a nightmare which will	Yes! SPD already has a real time crime center. SPD's existing RTCC (i-base) is on-premise, so it does not create the risk of data being obtained from third parties or legal requests from those outside Washington state. There is no reason for SPD to

circumventing Washington State Law. ICE has a practice of accessing data directly from private ALPR surveillance companies that market their products to police, in order to circumvent any local sanctuary laws. The department gets a lot of use out of this data, as seen by them running thousands of searches of ALPR databases in a single month as early as 2019. ICE's utilization of this data shows the degree of risk it poses to vulnerable communities. Threat of harm to all people exercising First Amendment Rights of free speech,	Moving to a cloud platform allows CBC and ICE to access automated license plate reader data directly which circumvents Washington State Law. SPD has used surveillance data to spy on protestors and shared it with US Marshalls, Wa State Dept of Corrections and a private citizen. RTCC opens up the opportunity for those exercising dissent to be tracked and targeted, ans risks the threat of police retaliation. RTCC software like Fusus allow police to view camera footage without a warrant or ongoing consent from the owner. Surveillance technology will bot aid		Beach neighborhood by 33%. Both violent crime and property crime can be reduced by community investments. Violent crime can be reduced by investments in mental health treatment, providing substance-abuse-treatment facilities and access to affordable housing. Direct income support has been found to reduce firearm violence. Opening libraries and expanding library hours both reduce violence and property crimes.	result in multiple unforced errors not to mention invasion of privacy, violation of civil liberties at the very least. This continuous introduction of new and unvetted surveillance tools would be in violation of Seattle's Surveillance Ordinance.	obtain a cloud-based RTCC which would weaken state lawd and endanger women, trans folks, and immigrant residents.

	public protest and assembly	law enforcement in solving crime. RTCC deployment by SPD would cost approximately $5.3Million dollars.	
81	I do not want the surveillance state to be expanded, and I do not want cctv coverage of the city. It is absolutely reprehensible and will only lead to continued overpolicing of marginalized groups. I don't want my car to be tracked as I go from place to place, the police should not have that data.		None whatsoever.
82	I am very concerned about expanded surveillance. The research I am aware of shows no public safety benefits, and meanwhile are are increasingly	The proposed expansion areas furthermore are clearly highly racialized. This is not okay.	

	living in a police state. I want Seattle to be a community where everyone feels safe, but constantly under the microscope.				
83	Data centralization and pooling is terrifying -- with ICE tearing families apart and authorities from other states trying to enforce their draconian abortion control restrictions here, the best protection for Seattle's residents is data minimization. Don't collect data on us and above all do not plug that data into larger sharing networks.	I don't care if the tech is supposedly set up in a way that ICE/CBP would need a warrant to get to it. They have shown themselves to be completely untrustworthy and the only way to ensure that they can't get it is to not collect it --- or at the very least not put it out on the cloud.			
84	It doesn't appear to be very effective according to the research that's been done on it.	I don't want to assist ICE in their detention of people especially the way they've offered	Not enough to out weigh its cons.		l

		no legal process to many who are trying to obey our laws.					
85	Threat of harm to abortion and gender-affirming healthcare Many anti-abortion states, including neighboring Idaho, have passed bounty hunter laws. This creates a market and demand to hunt down this data for people believed to have gone to Seattle to get reproductive healthcare. If SPD switches over to a cloud-hosted RTCC database, we enable the criminalizatio n of those seeking reproductive care. The rate of out-of-state abortions, those coming from other states to seek abortion in Washington,	Threat of harm to women, sexual assault and stalking survivors, and vulnerable marginalized community residents RTCC software enabled a Texas cop to search surveillance data from across the county, including Washington State, other states with abortion “sanctuary” laws, and non-police entities including the King County Housing Authority, for someone that had an abortion RTCC software makes it impossible to keep surveillance data from ICE. Local police	Threat of harm to immigrants ICE has a history of terrorizing immigrant communities. Jurisdictions that do not use local resources to enforce federal immigration laws have lower rates of crime, poverty, and unemployme nt than those that chose to collaborate. It was with this knowledge that the Keep Washington Working Act was passed to prevent data sharing between immigration and local law enforcement. RTCC software like Fusus can turn any camera into an automated license plate readers (ALPRs). By moving to	Threat of harm to all people exercising First Amendment Rights of free speech, public protest and assembly Seattle has a long history of participatory democracy dating at least as far back as the 1919 general strike. Seattle has seen mass protests for labor rights, abortion rights, anti-war protests, and protests around issues of international trade policies, and most recently mass demonstratio ns advocating for a ceasefire in Gaza. Unfortunately , police violence against protesters is not	Creates a system ripe for abuse and potential to violate all residents’ First and Fourth Amendment Rights Cloud-based software can be hacked. This happened in 2021 when hackers gained access to Verkada - giving them access to 150,000 cameras inside schools, hospitals, gyms, police stations, prisons, offices and women’s health clinics RTCC software creates conditions that are ripe for police abuse, as it provides little, if any, oversight for how police use it, little	Surveillance technology will NOT aid law enforcement in solving crime. The 2024 paper that SPD cites states that RTCC "appeared to have a relatively smaller impact on violent crime clearance (5% increase),” other studies of RTCC show no effect on violent crime clearance rates. In a 40 year systematic review with meta-analysis of the efficacy of CCTV the authors concluded there were “no significant effects observed for violent crime” and “a body of research on the	There are MANY effective tools the city could use to decrease community violence Violence interruption programs work. Neighborhoo ds that have adopted a Cure Violence Model or Group Violence Intervention Models have seen homicides and assaults decrease 30-50%. The city could scale effective community-led solutions such as the Regional Peacekeeper s Collective coordinated by the Regional Office of Gun Violence Prevention and the Rainier Beach Action Coalition and

increased by 36% in 2023 and included 20 different states including neighboring Idaho and states as far away as Texas and Alabama. Anti-abortion groups have a history of using license plate data. RTCC software allows data to be shared across law enforcement agencies. Third party agencies in anti-abortion states could use this data to criminally prosecute those seeking abortion in Washington state. Recently an Idaho mother and son were charged with kidnapping for allegedly taking a minor across state lines to access abortion care in Oregon. The state of Texas has already attempted to	departments are very cozy with ICE and RTCC makes it easier for them to casually share surveillance data. And, RTCC means ICE is able to search nationwide databases of surveillance data including data from police departments in Washington State, other states with "sanctuary" laws, and non-police entities including the King County Housing Authority. RTCC software was used by police to spy on "immigration protests" RTCC software companies like Fusus rely on private consumers to expand the camera network which gather	a cloud-based platform, Customs and Border Control (CBC) and ICE can access automated license plate reader data directly; circumventing Washington State Law. ICE has a practice of accessing data directly from private ALPR surveillance companies that market their products to police, in order to circumvent any local sanctuary laws. The department gets a lot of use out of this data, as seen by them running thousands of searches of ALPR databases in a single month as early as 2019. ICE's utilization of this data shows the degree of risk	unprecedented. After SPD's betrayal of the public trust in the summer of 2020, the city recently paid a $10M settlement. Violence against protestors in 2020 is one of the principal reasons that Seattle remains under the consent decree that it has been under for excessive use of force since 2012. SPD has used existing surveillance systems to spy on peaceful protestors. During the 2020 protests for racial justice, SPD used live video streaming to record peaceful protestors, and shared it with U.S. Marshalls, Washington State Department	documentation or auditable logs, and few transparency mechanisms. RTCC software like Fusus recruits a vast assortment of privately owned cameras that allow the company to bypass laws and restrictions that normally limit police, including viewing camera footage without a warrant or ongoing consent from the owner. The risk is not hypothetical as seen by other law enforcement agencies: In Pasco County, Florida, which operates an RTCC, the sheriff's office's predictive policing system encouraged officers to continuously	investigatory benefits of CCTV has yet to develop." Only 1% to 0.2% of ALPR captured license plates are either on a hot list or associated with any crime.	their Restorative Resolutions project, which has already reduced violence in the Rainier Beach neighborhood by 33%. Richmond, CA has chosen to invest in violence interruption and other community-led safety initiatives and they have seen a drop in the number of homicides. This is in contrast to neighboring cities like Oakland and San Francisco that have increased their police budgets and have not seen a decline in violent crime. Both violent crime and property crime can be reduced by community investments. Investments restoring vacant land

get data from Seattle Children's Hospital for any Texas residents receiving gender-affirming care. As soon as SPD switches over to a cloud-hosted RTCC database, red states will start issuing subpoenas to access data directly from Fusus.	enough data to reveal sensitive personal information, including where someone lives, works, and their religious affiliation. Individuals, homeowner associations, or businesses that opt into RTCC may be able to access the data directly from the vendor. Hostile individuals could access data to stalk or harass individuals. The threat to vulnerable communities is NOT hypothetical, as seen by the actions of other law enforcement agencies: NYP officers used mass surveillance technology to record and monitor everyone parked in front of a mosque, and Burmingham	it poses to vulnerable communities.	of Corrections, and to a private citizen volunteering at Seattle's emergency operations center (EOC). SPD has continued to use existing surveillance to spy on protestors including including one on Sept. 23, 2023, that called for justice for the death of Jaahnavi Kandula, who died Jan. 23, 2023, as a result of being hit by SPD officer Kevin Dave while driving his officer vehicle as she walked through a marked crosswalk. RTCC software is a vast network of cameras which can include doorbell cameras, drones, robots, fixed surveillance cameras, helicopters,	monitor and harass residents for minor code violations such as missing mailbox numbers and overgrown grass. SPD has a track record of officers abusing their access to surveillance technology. In 2021 SPD Officer Swartz used police data to stalk his ex-girlfriend; in 2020, an officer accessed confidential information about a domestic violence investigation and shared it with someone involved; and just last year, an officer performed an unauthorized search for personal reasons to reveal a citizen's firearm ownership. The privatization	and community non-profits that tackle violence and build community lead to reductions in both violent crime and property crimes. Many communities across the country are making investments in preventative community-centered approaches and are seeing a reduction in crime and violence in the community. Violent crime can be reduced by investments in mental health treatment, providing substance-abuse-treatment facilities, and access to affordable housing. Poverty and income inequality are associated

	police also used this technology, in conjunction with other tools, to track Muslim residents. Homeless residents, who have no option for privacy, are likely to become targets of mass surveillance. California is using AI to identify and target its homeless residents.	hidden cameras, police body cameras, and cameras in schools and churches, among other settings. RTCC opens up the opportunity for those exercising dissent to be tracked and targeted, and risks the threat of police retaliation. Surveillance is about the power to watch and intervene in a variety of situations, whether criminal or not, and surveillance technology has the potential to have a chilling effect on free speech rights. In 2021 LAPD requested bulk camera data targeting Black Lives Matter protesters. In New York City there is evidence that	of policing represented by relying on private consumers to expand the camera network undermines democratic values, effectively excluding Seattle residents from being able to provide input and oversight on the growing Seattle surveillance apparatus. RTCC software like Fusus continually adds new image recognition algorithms and integrations with third-party applications via the software's AI capabilities. This continuous introduction of new and unvetted surveillance tools would be in violation of Seattle's	with violence, especially assault and homicide. Inequality predicts homicides better than any other variable. Evidence supports that this is a causal link. And direct income support has been found to reduce firearm violence. Opening libraries and expanding library hours both reduce violence and property crimes.

			NYPD has used surveillance technology to surveille Black Lives Matter protesters.	Surveillance Ordinance.	
86	It is unnecessary and an over reach of power. The SPD should not be in cooperation with ICE agents, rounding up many innocent people due to their skin color or physical presentation. This is Orwellian and a very wrong use of technology... against the people.	In this case, I do not. I mentioned in the CCTV answer that if there was a child or elder with dementia it might be helpful to identify where they were last seen, but beyond that, it becomes fascist.		Keep it human scale. People to people. If someone is committing a crime, then deal with it. Keep ICE out as much as possible. ICE agents are the minions of a racist, fascist administration that wants to go back to pre civil war times with all the power centered in white men who dictate what religion people should adhere to.	Look into your hearts. If you have or had loved ones who were terrified that they would lose everything they've worked for and been hard working contributors to our society, wouldn't you be frightened for them? Its really not a stretch.
87	we do not want ICE violating the privacy of the people of seattle. We do not want them harming or harassing the people of seattle. they do not need more	i'm sure there is value, but ICE has no problem breaking laws. Why make it easier for them?		consider who we are as a city	

	ways of violating us				
88	Privacy. Government using information against the people. Enabling autocracy.	None		Reduce surveillance	
89	This data is not for use to increase the surveillance of people in our community based on personal characteristics of race, lifestyle choices or immigration status.			Do not share This data with ICE.	
90	Surveillance state seems against our freedoms when there are plenty of cameras outside businesses. Making the people of seattle more scared, and people already have an issue being filmed in public. I don't see how they will protect us further. Face recognition		Who is going to be watching? Where is this content stored? What value does the city see? Is this a direct response to Trump's comments about a surveillance state?	How the people of seattle feel as a majority democratic city when the surveillance state was introduced by Trump. Based on his recent actions I doubt the city's intentions of implementing this in Seattle.	Listen to the people as the state still has power. Don't feel pressured into something the people don't want or our representatives become complacent and part of the problem. Introduce benefit to the people and be more outright in how you plan

	used wrongly/unjustly. I have experienced crime in this area where there would have				to use all of this.
91	My concerns are frankly innummerable. SPD's existing RTCC (iBase) is on-premise, so it doesn't create the risk of data being obtained from third parties or legal requests from those outside Washington state. A cloud-based RTCC creates the risk of data exposure, which would put essentially every person in Seattle at risk should a bad actor get their hands on the collected information. SPD already has what it needs in its current system, and there is no benefit to	Please see these links with more information on the dangers of this technology: https://www.wired.com/story/license-plate-reader-alpr-surveillance-abortion/ https://www.theguardian.com/us-news/2023/nov/01/idaho-mother-son-kidnap-charges-abortion https://www.thestranger.com/news/2023/12/21/79315926/texas-tried-to-get-seattle-childrens-hospital-health-records-on-trans-patients https://www.realchangenews.org/news/2024/08/07/inside-spd-s-	Absolutely none.	Please consider the cost of this technology - both the literal dollars, and the human price as well. The negative impact of cloud-based data storage cannot be overstated. Please make the right choice to protect the people you were elected to serve. You are in a unique position to make a real difference - do not squander that responsibility.	

anyone except those who would exploit our private data in expanding the system to a cloud-based structure. These bad actors are not theoretical - Washington State passed our Shield Law to protect those seeking necessary life-saving healthcare from other states, and there are bounty hunters and agencies in other states trying to track those people down to jail them, or worse. Moving to a cloud-based RTCC system will do nothing but undermine the very important sanctuary laws we have passed, and it is not an exaggeration to say that this choice would cost	use-aerial-surveillance-during-2020-protests https://www.thestranger.com/slog-am/2024/01/25/79356578/slog-am-seattle-settles-2020-protest-lawsuit-for-10-million-nitrogen-execution-scheduled-for-tonight-no-medical-care-for-floridas-transge https://www.aclu.org/news/civil-liberties/major-hack-of-camera-company-offers-four-key-lessons-on-surveillance https://www.eff.org/deeplinks/2023/05/neighborhood-watch-out-cops-are-incorporating-private-cameras-their-real-time https://projects.tampabay.com/projects/2020/investigations/polic

lives. ICE is already active in our communities, kidnapping residents who are here legally and have committed no crimes. These are our friends and neighbors who are disappearing, not faceless criminals, and families are being destroyed by these actions. Children are unable to go to school for fear of raids, and their parents can't so much as shop for groceries without fear. Cloud-based RTCC would enable ICE to continue and expend their illegal operations, and I very much doubt that they will stop with their current targets. History has shown over and over and	e-pasco-sheriff-targeted/intelligence-led-policing/ https://www.seattle.gov/Documents/Departments/OPA/ClosedCaseSummaries/2020OPA-0455ccs042621.pdf https://www.vera.org/community-violence-intervention-programs-explained

over and over again that this kind of violence will expand unchecked if given the opportunity, and cloud-based RTCC is exactly the kind of opportunity that will allow them to target anyone they want, for any reason, regardless of the law. Expanded surveillance has a chilling effect on first amendment rights, and puts American citizens in danger simply for speaking their minds. This affects EVERYONE, not just a few groups. Every single person in Seattle will be in significantly greater danger and at risk of physical threat with expanded surveillance. If we knew we could trust the

information collected would be used for public good, this might be a different story - but we know from experience and history that it will not be.

RTCC is also expensive. Looking at four other US cities that have deployed RTCCs, the average cost is $7.16 per person. With Seattle's 2020 population of 737,015, this would put the full-scale (post-pilot-phase) RTCC deployment by SPD in the ballpark of $5.3 million, not including the additional costs for the CCTV and ALPR expansion. On top of this, it has also not proven to be effective at reducing crime, making it

essentially useless for its stated purpose. There are many proven ways to reduce crime, like violence interruption programs and community-led safety initiatives. Why would we put more money towards something that does not work and makes us all less safe, when we could instead put that funding towards proven methods that reduce poverty, provide crucial resources to those that need them, and improve all of our lives?

Please protect your city, your community, and yourselves by refusing to expand RTCC.

92	I believe this adversely impacts our BIPOC and potentially our LGBTQIA+ communities.	This is NOT about crime prevention. A much better and proven solution is to use the same monies and resources towards intervention and support solutions.	None	See #2	Remember, this is NOT about crime "prevention".	This is NOT a proven crime prevention solution. Whereas intervention and support solutions are.	N/A
93	I am concerned that this technology will be used to track people's movements across the city and in turn, be used to track down and harm marginalized communities. I am concerned that this technology will be used to assist ICE kidnappings, punish those seeking healthcare, track/disappear the unhoused, and harm the LGBT+ community. This technology has no positive benefit. SPD has proven		None		If this city is truly as welcoming as it claims to be, it will oppose this technology. Do you want to lead a city whose values are not in line with its actions? Again, I emphasize that this technology will harm marginalized communities including BIPOC, immigrants, the unhoused, and the LGBT community. I thought I was supposed to be safe here.		

	themselves to be incompetent, ineffective, and consistently incapable of protecting our community. Why should I believe that they have our best interests at heart? This technology will do nothing but harm marginalized communities and I vehemently oppose its use and implementation.						
94	It is a violation of privacy, and too far along the road of a surveillance state. I do not feel comfortable having my tax dollars support a third-party surveillance company. I would rather have better training for officers.		This technology takes out the human element, which is already way too far gone. Again, I would rather support the training and development of human beings to deal with our complex issues as a city.	Police officers are already stretched so thin. I want their focus to actually be on protection and service, not surveillance.	Don't spend money on this technology! As a voter, I am paying attention and will vote and act and canvas accordingly.	Invest in human beings, and do more to provide a social safety net for the citizens of our city. Don't spend money on this invasive technology.	Thank you for the hard work of city government. Please do the right thing and help public servants by supporting them in other ways.
95	We are not living in normal times. Do not	AI is not ready for prime time. It's not the time to		Please -- don't capture tons of unnecessary	These times are not business as usual.		

	increase surveillance and accessible storage at this time.	watch everyone doing everything. The use is too easily shifted		data on a maybe or what-if basis	Democracy is eroding. This is not the time to increase searchable/shareable data.	
96	1) This is warrantless dragnet surveillance. The RTCC storing data for 30 days means SPD would be mapping people's lives being able to figure out where people live, where they work, where they worship, the routes they take to work, etc. This map would be available to SPD & everyone with access to SPD's data. There is no legitimate use for this kind of map, all it does is create conditions where abuses are both easy & incredibly disastrous. These abuses aren't hypothetical.		None, RTCC don't reduce crime or increase clearance rates, it doesn't even make people feel safer. This has been studies repeated. Lots of studies showing this were submitted just last year when SPD was first asking for it		How do you think any guardrails will keep the Trump Administration & ICE from accessing this data given their constant & blatant disregard for the law? How do you justify increasing surveillance now when ICE is kidnapping people on Seattle's streets with the assistance of SPD? How is there money for even more mass surveillance when the city is facing a budget deficit? Especially, when this is shown to not	Keeping people in Seattle safe would require removing this & other surveillance by SPD (ex. CCTV & ALPRs) and using that money to fund programs that are shown to reduce violence. Removing RTCC alone would free up millions of dollars per year that could go to programs that reduce violence.

In recent weeks we've seen small-ish abuses like yet another SPD officer getting caught using a police database to stalk someone to massive like ICE & cops looking for people who've had abortions accessing nationwide surveillance databases. Those nationwide searches included data from Washington State despite the state's Keep Washington Work and Shield laws. Nashville abandoned its pursuit of FUSUS (SPD's RTCC) in April due to these risks. https://nashvillebanner.com/2025/04/28/metro-nashville-fusus-freddie-oconnell/ reduce violence. Why do things that are proven to reduce violence (ex. housing access, food access, mental health access, libraries, & violence intervention programs) constantly get defunded while surveillance that doesn't reduce violence gets more money?

How do you think having Seattle under surveillance by the Trump Administration & ICE will impact tourism?

How do you think installing more surveillance which makes people's brains act similar to psychosis will increase safety or reduce violence?

The only reason reporters haven't discovered that SPD's existing data is being abused in nationwide searches like this is because SPD's CCTV & RTCC program has only been live for a month. There hasn't been any time for reporters, community members, anyone to get records on data access. There's barely been time for SPD's data to even be shared because it just went live at the end of May. SPD is ramming through this expansion before there's a chance for the community to see the full impacts of SPD's existing dragnet surveillance,

SPD storing this a private,

for-profit company's cloud guarantees this data will be shared. These systems are built to make data sharing between agencies as frictionless as possible, that's part of the sales pitch.

This is functionally a secret expansion of surveillance. SPD has not done any community outreach to let the public know this is being considered. SPD hasn't even done a press release or a post on social media. The only reason people know this is happening is because community members found single Seattle IT webpage that mentions it & have spread the word.

There cannot be any consent of the governed/community consent because SPD hasn't let them know it is happening.

Being subjected to constant surveillance is harmful. Whose Streets Our Streets identified the level of surveillance in Seattle as already having "a psychological effect on the people being surveilled" (http://stopsurveillancecity.files.wordpress.com/2024/09/338c7-wsosautomatedenforcementsummary.pdf) and that was before SPD launched its CCTV & RTCC pilot. The effect is that people's brains act in a manner similar to "psychosis

and social anxiety disorder" (https://scitechdaily.com/what-happens-to-your-brain-when-you-know-youre-being-watched/). Expanding surveillance will increase these impacts and make people less safe.

There is no reason to believe any information SPD has provided for this material update or the underlying SIR given SPD's lengthy history of lying during the SIR process. Just last year, SPD definitely told the people of Seattle that it would not be actively monitoring CCTV cameras which was a lie, the minute the cameras were approved SPD

demanded more money from the city to hire people to do active monitoring claiming that was the only way for them to work. SPD has also lied in the SIR for FLIR (https://www.realchangenews.org/news/2024/08/07/inside-spd-s-use-aerial-surveillance-during-2020-protests), and just last month SPD provided misled people during the SIR for StarChase/pursuit mitigation trackers by claiming it was required to conform to WA law (The law does not say that, it says police departments should end each individual pursuit as soon as possible based on existing policies & technology,

	not that departments need to acquire new technologies).		
97	The RTCC is an invasion of privacy that makes the city a more hostile place to live for normal people and doesn't make things any safer. As study after study has shown this kind of live surveillance is not a deterrent against crime but it does make quality of life worse for people who feel the constant surveillance. It's extremely unequitable disproportionately affecting communities of color and poor people who live in high density areas. SPD has not earned the trust of the community to be continuously	It has no value to the people of Seattle, just value to SPD and business owners who benefit from repression and the increased hostility of public space	City leadership already ignored the clearly spoken voice of the people on RTCC once. SPD, SPOG, and the vendors who you are sending our hard earned tax dollars to want these surveillance programs but the people who you actually need to vote for you do not. Consider that expanding the RTCC once again goes against the clear will of the voting public as well as the city's own committees that provide recommendations on equity in policing.

monitoring us, and if they had that trust they wouldn't need to. The RTCC also allows other agencies throughout the country to surveil us and make our expressed values around immigration and abortion access meaningless. By accepting the RTCC we invite other jurisdictions to exercise control over and surveil residents of our city including immigrants but also people who are coming here to access reproductive healthcare. The city cannot have a commitment to being a sanctuary city and upholding reproductive rights while allowing the RTCC

98	SPD already has a real time crime center. SPD's existing RTCC (iBase) is on-premise, so it doesn't create the risk of data being obtained from third parties or legal requests from those outside Washington state. There is no reason for SPD to obtain a cloud-based RTCC which would weaken state laws and endanger women, sexual assault and stalking survivors, transgender individuals, and lawful immigrants.	I don't see that the potential value of this technology is worth the risks to our civil rights. Please consider that the country already is quickly moving towards a fascist state. This technology will be used to further the agenda of a government intent on taking away the rights we have in a democratic society.	The City leadership should have as a top priority the protection of our democratic ideals, our civil rights and to keep our law enforcement agencies separate from national encroachment. Of course we want to reduce crime in our city, but not at the expense of our civil rights. Also, it seems that the City has made headway in reducing crime with the technology it already possesses. Please hire more police officers and reform criminal justice as necessary without adopting cloud based surveillance technology that will put us at such

				risk. Thank you.	
99	As our country lurches towards autocratic politicized police state, NOW is not the time to expand police surveillance powers, especially if data is to be shared with ICE.				
100	I oppose increased surveillance of Seattle people. I fear it being used by feds to kidnap people				
101	It will be used to target minorities, especially by ICE. I believe there are better options for reducing crime. When information goes into the cloud, local organizations have less control over it.	None.	Why don't we find better ways of preventing crime instead of setting up a big brother style system? There are too many ways for that sort of technology to be abused.	What sort of city do we want? Do we want a city where everyone works together to make a safe and welcoming place to live or visit? Or do we want some weird police state where everyone knows we are being watched by	Don't spend money on this. It won't have enough benefits to justify the cost. Technoloy ages out. In a few years, all of this tech will be obsolete. Lasting solutions involve people working together. It's a harder process and it

				someone, but we don't who that someone is or what they might do with the information.		certainly isn't flashy. But I would sleep better knowing that I don't have to worry about folks being snatched off the street, or wondering who is creating a database for their own, illegal purposes.
102	Invasion of privacy. Targeting of immigrants, queer people, bipoc, etc. We should not support Trump's targeting of individuals.		We need to support our immigrant community.	ICE is ripping families apart for no good reason other than quotas.	I don't want Big Brother watching!	
103	Please do not expand the use of RTCC to a third party vendor. My concerns are for the privacy and safety of citizens who might be targeted by this technology allowing the possibility to circumvent Washington State's Shield Law and Keep WA Working	I see some value in in-house, well-controlled surveillance to help with crime prevention and investigation.		Consider the potential harm that could arise if RTCC surveillance was released into the hands of potentially violent persons outside of the control of local SPD authority.		

	Act. Allowing a third party vendor access to sensitive records is a step too far, and has been rejected by other jurisdictions out of concern for people's safety. With a third party vendor, there is a greater possibility of data being accessed by those who might cause harm to potential persons under surveillance.						
104	A Real Time Crime Center is a software that uploads all of Seattle's surveillance to a cloud-based platform making it available to ICE, Customs and Border Patrol, and other law enforcement agencies across the country that will have access to the	No	None	It should not be made available to ICE and CPB	No	No	

	data without a warrant.	
105	SPD already has a real time crime center. SPD's existing RTCC (iBase) is on-premise, so it doesn't create the risk of data being obtained from third parties or legal requests from those outside Washington state. There is no reason for SPD to obtain a cloud-based RTCC which would weaken state laws and endanger women, trans folks, and immigrant residents. A move to the cloud creates a system ripe for abuse and potential to violate all residents' First and Fourth Amendment Rights -Cloud-based software can be hacked. This happened in	The paper referenced by SPD in the SIR mentions the "substantial costs associated with RTCCs, with initial costs ranging between several hundred thousand dollars to $11 million". We should redeploy funds to solutions that work. -Both violent crime and property crime can be reduced by community investments. Investments restoring vacant land and community non-profits that tackle violence and build community lead to reductions in both violent crime and property crimes. -Poverty and income

		2021 when hackers gained access to Verkada - giving them access to 150,000 cameras inside schools, hospitals, gyms, police stations, prisons, offices and women's health clinics.		inequality are associated with violence, especially assault and homicide. Inequality predicts homicides better than any other variable. Evidence supports that this is a causal link. And direct income support has been found to reduce firearm violence.
106		I worry about it circumventing protections that Washington has in place and endangers anyone on trumppian hate lists (trans folks, abortion seekers, immigrants). Please make it harder for	Lots of value! But also easy to make mistakes that could put many vulnerable people in very real danger. Let's make sure each step in new tech does more good than harm.	Privacy, civil rights, avoiding federal surveillance or making it easy for law enforcement to collaborate with authoritarian tactics of fear and surveillance

	folks outside Washington state to surveille our citizens.			
107	I'm concerned for our privacy. I'm concerned that these are mostly in POC areas. But mostly I'm alarmed that we are collecting data that can be terribly misused. It could be subpoenaed to prosecute people coming from out of state for abortion or gender-affirming care. Who knows what Trump and his cronies might do with them?	none whatsoever.		Consider that the adverse uses of these data would be far worse than any possible benefit.
108	this will endanger targeted groups	none, not needed	do not approve	

109	I am against surveillance in Seattle. I do not want police or artificial intelligence systems to watch me and my family as we go about our lives. Surveillance leads to self-censoring and a loss of individuality, creativity, and privacy. I do not want the federal government to legally or illegally access surveillance data collected in Seattle.	None.	The harmful impacts of surveillance and policing fall disproportionately on individuals who have already experienced violence from white supremacy and colonialism. This program is structurally racist. City leaders should stop pursuing these police technologies and instead use the millions they would cost on public-health-based safety and community supports, like housing, food access, and libraries.
110	Inappropriate to expand these systems given recent federal overreach.		
111	The overpolicing of communities is quite concerning.	I see no use of this overreaching surveillance	Please consider the effects it may have on our communities to be

	With only the use of constant surveillance we cannot understand the broader story of the situations we see unfold. I fear that this data will be used to wrongfully convict our friends and family		in the hands of the police		constantly watched by authority.		
112	I oppose the increased use of surveillance on my community. Linking up police access to the existing cameras and adding new one adds risk to all our communities especially immigrant, queer and POC people	Do not do this	Too much constitutionally protected private and personal data becomes available to all types of law enforcement SPD, ICE, KSC, national guard, WSP	No	Protecting our constitutional rights. Stopping ICE, keeping the government out of our lives.	As a voter I have been watching your votes and am disappointed in what you have been doing.	No
113	Surveillance data should be held within the jurisdiction responsible for it. Saying it would be cheaper to hold the data in a contractor's facility means that the city						

	doesn't value the security of the surveillance data. Once the contractor has our data stored out of state, it can be shared with other entities based on local laws, rather than subject to the laws we enacted to protect the data from exposing people in Washington to risks from outside jurisdictions.							
114	This technology infringes on the civil liberties of people who have committed no crimes, and exacerbates the already disproportionate targeting of the young, people of color, LGTBQIA people, etc, and does not require a	WA state and Seattle are facing a budget crisis and are facing record costs due to lawsuits against SPD and other agencies. There is no reason to believe that this will reduce crime or increase case resolution and every reason to believe it will be abused in	Negative value due to monetary cost for products, loss of civil liberties, liability issues, and other harms to our communities with no proven value to reduce crime.	There are other solutions to crime that actually work. I realize these often involve giving money to community organizations rather than the police but maybe, given SPDs track record, we shouldn't give them anything that they can abuse and get themselves	This proposal would result in so much liability for the city and SPD. Once you start collecting data on people do you have a plan in place to protect that data? Do you have a plan in place to ensure it will not be abused, or disclosed without authorization? What will	It is hard to truly appreciate the value of privacy until it is lost, and even harder to get it back, if it is possible at all. Do you want this as your legacy?	Please please please do literally anything else with the city's money. It would be more beneficial to turn it into confetti for a parade or to set it on fire than to spend it on this.

	warrant to be shared.	ways that end up costing even more money, and result in harm to our community.		into more trouble with.	you do if those plans fail?
115	In a time of extreme authoritarian overreach on the part of the federal government, any additional surveillance and data gathering at the local level (such as expanded RTCC) runs the risk of that data being acquired and misused by the federal government.		There is little or no demonstrated value in the expansion of RTCC		

	RTCC software is a cloud-based software platform designed for real-time crime centers to integrate multiple surveillance technologies such as cameras, automated license plate readers (ALPRs), CCTV, among other police surveillance tools. RTCC software like Fusus can turn any camera into an automated license plate readers (ALPRs) which gather enough data to reveal sensitive personal information, including where someone lives, works, and their religious affiliation.
116	The City Council is attempting to move the on-premise RTCC

database to an off premise, cloud-hosted database managed by a third-party, private company. This change will enable other states to circumvent WA state's Shield Law and Keep WA Working Act, which are meant to protect both people seeking reproductive healthcare and immigrant workers.

SPD already has a real time crime center. SPD's existing RTCC (iBase) is on-premise, so it doesn't create the risk of data being obtained from third parties or legal requests from those outside Washington state. There is no reason for SPD to obtain a cloud-

	based RTCC which would weaken state laws and endanger women, trans folks, and immigrant residents.			
117	False positives and the possible addition of AI tools reduces transparency and accountability.		The lack of trust in SPD will only get worse.	
118	With the FASCIST regime currently occupying our white house, NOW is NOT the	Where is the moral voice in the implementation of these -- I can't imagine there has been any.		

	time to create tools that they will use in any of their witch hunts, ie towards trans, immigrants, and political enemies. NO, just NO!!	Please stop, don't do this. And don't do this in our names, with our taxes!			
119	I am concerned the cloud-based storage part of this system will endanger women, trans folks, and immigrant residents by making data and surveillance available to out of state and federal government agencies. This is not a hypothetical – this is happening, and WILL happen to sensitive data on Seattle residents and visitors if we continue to contract for-profit company with out of state data storage servers vulnerable to secret	I don't see that this tech has any value. It is very expensive, it throws even more of our city budget to the police department which directly results in less funding for the social services and programs that actually keep our neighborhoods safe.	SPD has a track record of officers abusing their access to surveillance technology. SPD has lost the trust of wide swaths of Seattle residents because of their violent, escalating crowd-control tactics, poor leadership, right-wing police union, and significant representation of white supremacists within SPD ranks. What possible reason do we have to trust SPD with more surveillance tech? Why should we believe SPD will do what they say they	The current city leadership seems to believe they have a "mandate" from the voters regarding public safety. However, I would like them to consider that perhaps they have misinterpreted this "mandate" as they have run roughshod over democratic processes (such as public comment and community advisory committees) that have been informing them that their police legislation – RTCC and CCTV, SOAP	

	subpoenas and governmental pressure to share that data in ways that will be both legal and illegal.	as they collect and store this sensitive data?	and SODA zones, &etc. – are deeply unpopular and not what the people of Seattle want for our city.
120	Availability of this information from license plate ID to ICE etc.		
121	- Footage is stored for 30 days. Why is it stored for so long? - Nashville abandoned its pursuit on FUSUS (the RTCC SPD uses) in April 2025 because it didn't believe any guardrails would keep the Trump Administration & ICE from accessing it. - By moving to a cloud-based platform, Customs and Border Control (CBC) and ICE can access automated license plate reader data directly; circumventin	Richmond, CA has chosen to invest in violence interruption and other community-led safety initiatives and they have seen a drop in the number of homicides. This is in contrast to neighboring cities like Oakland and San Francisco that have increased their police budgets and have not seen a decline in violent crime. Why are we privileging strategies that have not worked to reduce	

g Washington State Law. - RTCC software like Fusus continually adds new image recognition algorithms and integrations with third-party applications via the software's AI capabilities. This continuous introduction of new and unvetted surveillance tools would be in violation of Seattle's Surveillance Ordinance.	violent crime over ones that do?

Appendix B: Public Comment Period (6/03/25 to 6/23/25)

122	I have significant concerns about the use of cloud-based RTCC solution will put sensitive data about Seattle residents and visitors within the reach of the Federal government, circumventing our state's Shield Law and Keep WA Working Act. This is concerning a wide range of people, but particularly so for immigrants, gender minorities, those seeking abortions, and protestors exercising their first amendment rights. Additionally, the use of solutions such as Fusus to expand police surveillance technologies, in particular to include the use of private security	A benefit to public safety has been claimed, however there is not evidence to support a signficant improvement to public safety.	The privacy and safety of Seattle residents, and those visiting Seattle, in the face of hostility from the Federal government and law enforcement from other states.

	cameras, represents a highly concerning increase in the polices ability to conduct wide-scale surveillance of Seattle residents.			
123	Increases to surveillance technology, at this time in history, is a terrible idea. The federal government will seek any existing tool to harm immigrants, their political opponents, and people seeking	Whatever good this could do, it will not outweigh the harm. Not now, not with this administratio n. Possibly not ever.	Please consider every thing that is happening in our country right now. Our most vulnerable communities are under attack. I am legitimately afraid the US is on its way to becoming a dictatorship,	Seattle will NOT be a sanctuary city, or a refuge for LGBTQ+ people and people seeking abortions if there is city wide surveillance.

	abortion and gender care.			if it isn't one already. I am already scared and increased surveillance is only going to make things worse.
124	I'm very concerned that this technology can be accessed by a national database, making it available to ICE, Border Patrol, and law enforcement across the country. This poses grave danger to all of us in these rife political times with a Federal Government pushing the boundaries of executive powers and overreach. I'm particularly concerned regarding the dangers posed by this technology for our marginalized communities (immigrants, transgender folks, and		I understand that this will add another tool in the 'tool belt' of law enforcement . That said, the risks far outweigh the benefits.	

	women). Is it not illegal in Washington State to share information with ICE? Does this technology not risk our status as a sanctuary state/city?				
125	The further erosion of privacy. Use to target specific vulnerable groups.		Put civil liberties and democratic values first. Don't let fear guide your decision making, but principles. What is the highest and best good for all?	Please protect our civil liberties. They are in grave danger at the moment and we need your help to maintain them. Thank you.	Thank you for standing up for our citizenry!
126	Major concerns. Mass surveillance, especially if the data gets into the hands of unaccountable and lawless government actors, is the antithesis to a free and democratic society. Right now the federal government is outright violating court orders and threatening to	The risks far outweigh the rewards.	How is the City of Seattle protecting residents against federal government overreach? How is the city protecting the human rights of its residents? What happens if this data gets into the hands of bad actors?	We are living in a country with federal leadership that outright violating civil liberties, refusing to obey judicial orders, and is not giving immigrants due process before sending to overseas prisons. Does the city of Seattle really want to give the federal government more information	

	send citizens to overseas prisons without due process. These cameras will help facilitate the human rights abuses of innocent individuals and people who should have a day in court to defend themselves.			that lead to the downfall of democracy and irrevocably ruins peoples lives?	
127	Data from Seattle's surveillance should NOT be available to ICE or border patrol without a warrant.	I'm fine with police accessing this data to help with crimes. However, this information should be only accessible to police.			
128	I am concerned that this could be used to violate the rights of people in Seattle.	The theoretical cases in which it could be helpful seem so unlikely that they are not worth mention.	How easy it would be for the data the City collects to be hacked, DOGE-ed, or otherwise leaked to entities that could use it in a harmful way.	Even where it's not being used, the existence of this technology could have a chilling effect on exercise of our First Amendment rights, and could make vulnerable people such as immigrants feel less safe and more	Please vote NO on surveillance technology.

					limited in our communities.
129	Many anti-abortion states, including neighboring Idaho, have passed bounty hunter laws. This creates a market and demand to hunt down this data for people believed to have gone to Seattle to get reproductive healthcare. If SPD switches over to a cloud-hosted RTCC database, we enable the criminalization of those seeking reproductive care.	RTCC software was used by police to spy on "immigration protests"	None	We do not need more surveillance	
130	Without regulation and appropriate oversight, the overreach of MAGA states to use data to find individuals seeking reproductive care is my primary concern. Also, it is		With this administration and city council, none	Use data! Track results! Be transparent about effectiveness /costs! Learn from other cities!	

	unclear to me how to keep this information from inappropriate use by ICE, rendering our vulnerable communities less safe and making Seattle less safe for all given proliferation of fear.						
131	Traffic cameras should not be incorporated into SPD's Real Time Crime Center. Increasing surveillance is an infringement on the privacy of Seattle residents. It will allow another avenue for federal authorities such as ICE to track individuals, going against Seattle's supposed status as a Sanctuary City.	Increased surveillance will likely affect marginalized communities at a disproportionate level compared to white Seattle citizens.	Traffic cameras should remain as is without being implemented into SPD.	No	Consider divesting funds from SPD and into social services.	No.	No.
132	Expanding the surveillance capabilities	I do not want to live in a city that abets the federal			Consider the harm you'll be inflicting, which vastly		

	of the city will only endanger its inhabitants, and will very likely be leveraged by state actors and agencies (i.e. ICE) to target immigrants and other vulnerable populations. Please do not move forward with this.	government in harming/targeting vulnerable communities.		outweighs the good these systems might do, and think about other areas that desperately need this funding.
133	There is already a real time crisis center. We do not need to partner with private companies that favor profit over any benefit to citizens.		None. Do not give our data to non public entities.	Imagine the misuse of this kind of amassing of data- the danger outweighs any benefit.
134	There is no need for a cloud-based RTCC, which would weaken state laws and endanger women, trans folks, and immigrant residents. It is expensive and a threat to our most vulnerable citizens.			Think about who in Seattle is actually impacted by this. Think about our most vulnerable citizens.

	Please carefully consider any unintended consequences of moving the RTCC database to be a cloud-hosted database managed by a third-party, private company. As I understand it, this change will enable others to circumvent WA state's Shield Law and Keep WA Working Act, which are meant to protect both people seeking reproductive healthcare and immigrant workers.		
135	SPD already has a real time crime center. SPD's existing RTCC (iBase) is on-premise, so it doesn't create the risk of data being obtained from third parties or legal requests	Please carefully consider any unintended consequences of moving the RTCC database to be a cloud-hosted database managed by a third-party, private company.	

	from those outside Washington state. A cloud-based RTCC - at least at this moment in time - could weaken state laws and endanger women, trans folks, and immigrant residents. Please carefully consider whether this is something that should be done now (or ever).			
136	This technology allows bounty hunters and ICE agents to track immigrants, abortion seekers, and likely seekers of gender affirming care, or anyone else targeted by our currently hard right, fascism-		The value is to the current federal government's non-democratic intentions. While it may have some small use in local traffic safety, the risk to privacy far outweighs this.	As a fifth generation Washington resident, all proud Republicans, whose ancestors came here on the preacher train in the late 1800s, I feel I can speak for many when I say that this program is not aligned

	inclined federal government.		even with the majority opinion among right wing folks here. We want our privacy, and we value it for others. Do not let the heat of today's political climate invade the needs of our state and the will of its majority - left and right alike - specially in Seattle, where we are a sanctuary city for a reason (the voting public has already extensively spoken on this issue).	
137	That this will inflict more harm than good on our King County communities, especially in areas that are underprivileged and underserved- by encouraging police overstep and presence when it is not warranted.	None.	The current authoritarian use of power that is happening in the White House and how it has already been affecting our communities and endangering lives. If you truly want to protect Seattleites, please	Again, please think carefully about the times we are currently living in and whether you want to actually protect the people of Seattle, or potentially cause irreparable harm under

	Over surveillance at this dangerous time in our country will only harm our neighbors, and facilitate police cooperation with ICE or military forces/federal powers. What happens when they come for US citizens? Will this technology help to hand them over? If this is actually about protecting Seattleites, this is not the way.		consider whether this tool would actually do that or would potentially endanger us all through an overpowered surveillance system that could be easily wielded against its own people? Or taken over by federal authority when they come for our city? Please rise to meet this moment, as this moment is not normal and we are truly facing the threat of fascism. And a President who thinks himself a king and does not follow the law or Constitution.	the guise of “protection”.
1 3 8	I oppose a surveillance state	None		

Appendix B: Public Comment Period (6/03/25 to 6/23/25)

139	Nashville abandoned its pursuit on FUSUS (the RTCC SPD uses) in April 2025 because it didn't believe any guardrails would keep the Trump Administration & ICE from accessing it. Many anti-abortion states, including neighboring Idaho, have passed bounty hunter laws. This creates a market and demand to hunt down this data for people believed to have gone to Seattle to get reproductive healthcare. If SPD switches over to a cloud-hosted RTCC database, we enable the criminalization of those seeking reproductive care. The rate of out-of-state abortions, those coming	SPD already has a real time crime center. SPD's existing RTCC (iBase) is on-premise, so it doesn't create the risk of data being obtained from third parties or legal requests from those outside Washington state. There is no reason for SPD to obtain a cloud-based RTCC which would weaken state laws and endanger women, trans folks, and immigrant residents. RTCC software like Fusus recruits a vast assortment of privately owned cameras that allow the company to bypass laws and restrictions that normally limit police, including viewing camera footage	I see no value in using this technology.	SPD's asked for these proposed material updates to the Surveillance Impact Reports for both their CCTV and Real-Time Crime Center (RTCC) 3 weeks after their CCTV and RTCC cameras went live on May 20, 2025 showing SPD never intended for this surveillance to be a short-term "pilot." SPD confirmed to Guy Oron that they have been providing "mutual aid" to ICE/Department of Homeland Security. Some of this "mutual aid" occurred while Interim Police Chief Shon Barnes was making the headline grabbing claim that he expects to go	The Community Surveillance Working Group's report on RTCC was "unsupportive of any ...deployment of the these two technologies [CCTV & RTCC]" due to "[t]he amount and urgency of the concerns and outstanding questions." The City leadership should not ignore the CSWG.	RTCC software are subscription products meaning the city will have to pay for it every single year. RTCC software, and other companies selling subscriptions, operate on the land-and-expand strategy where it starts off small with a city to get its proverbial foot in the door and then increases the amount the city is buying from them every year. In other words, a for profit company will be pushing Seattle to spend even more money on its products every year. The city cannot afford this ineffective and expensive technology - especially in light of the	There are MANY effective tools the city could use to decrease community violence besides increasing surveillance. Violence interruption programs work. Neighborhoods that have adopted a Cure Violence Model or Group Violence Intervention Models have seen homicides and assaults decrease 30-50%. The city could scale effective community-led solutions such as the Regional Peacekeepers Collective coordinated by the Regional Office of Gun Violence Prevention and the Rainier Beach Action Coalition and their Restorative

from other states to seek abortion in Washington, increased by 36% in 2023 and included 20 different states including neighboring Idaho and states as far away as Texas and Alabama. Anti-abortion groups have a history of using license plate data. RTCC software allows data to be shared across law enforcement agencies. Third party agencies in anti-abortion states could use this data to criminally prosecute those seeking abortion in Washington state. Recently an Idaho mother and son were charged with kidnapping for allegedly taking a minor across state lines to access abortion care in Oregon.	without a warrant or ongoing consent from the owner. The privatization of policing represented by relying on private consumers to expand the camera network undermines democratic values, effectively excluding Seattle residents from being able to provide input and oversight on the growing Seattle surveillance apparatus. RTCC software like Fusus continually adds new image recognition algorithms and integrations with third-party applications via the software's AI capabilities. This continuous introduction	to jail because he won't cooperate with the Trump Administratio n. SPD and Mayor Harrell refuse to respond to questions from Hard Pressed about how many times ICE has asked for data sharing. The only thing preventing ICE from accessing all of SPD's surveillance data (including 30 days of video and 90 days of license plate scans) is SPD's dubious claim that it will follow the Keep Washington Working Act & Washington Shield Law. Standing up to Trump means saying no to surveillance technology!	fact that Seattle is anticipating a $250 million shortfall in 2025. Looking at four other US cities that have deployed RTCCs, the average cost is $7.16 per person. With Seattle's 2020 population of 737,015, this would put the full-scale (post-pilot-phase) RTCC deployment by SPD in the ballpark of $5.3 million, not including the additional costs for the CCTV and ALPR expansion. Even the paper referenced by SPD in the SIR mentions the "substantial costs associated with RTCCs, with initial costs ranging between several hundred thousand dollars to $11 million".	Resolutions project, which has already reduced violence in the Rainier Beach neighborhood by 33%. Richmond, CA has chosen to invest in violence interruption and other community-led safety initiatives and they have seen a drop in the number of homicides. This is in contrast to neighboring cities like Oakland and San Francisco that have increased their police budgets and have not seen a decline in violent crime. Both violent crime and property crime can be reduced by community investments. Investments restoring vacant land and community

The state of Texas has already attempted to get data from Seattle Children's Hospital for any Texas residents receiving gender-affirming care. As soon as SPD switches over to a cloud-hosted RTCC database, red states will start issuing subpoenas to access data directly from Fusus. RTCC software enabled a Texas cop to search surveillance data from across the county, including Washington State, other states with abortion "sanctuary" laws, and non-police entities including the King County Housing Authority, for someone that had an abortion.	of new and unvetted surveillance tools would be in violation of Seattle's Surveillance Ordinance. In a 40 year systematic review with meta-analysis of the efficacy of CCTV the authors concluded there were "no significant effects observed for violent crime" and "a body of research on the investigatory benefits of CCTV has yet to develop." Only 1% to 0.2% of ALPR captured license plates are either on a hot list or associated with any crime.			non-profits that tackle violence and build community lead to reductions in both violent crime and property crimes. Many communities across the country are making investments in preventative community-centered approaches and are seeing a reduction in crime and violence in the community. Violent crime can be reduced by investments in mental health treatment, providing substance-abuse-treatment facilities, and access to affordable housing. Poverty and income inequality are associated with violence, especially assault and

				ICE is terrorizing immigrant communities under Trump. The Keep Washington Working Act was passed to prevent data sharing between immigration and local law enforcement. RTCC software like Fusus can turn any camera into an automated license plate readers (ALPRs). By moving to a cloud-based platform, Customs and Border Control (CBC) and ICE can access automated license plate reader data directly; circumventing Washington State Law. ICE has a practice of accessing data directly from private ALPR surveillance companies that market their products to
				homicide. Inequality predicts homicides better than any other variable. Evidence supports that this is a causal link. And direct income support has been found to reduce firearm violence. Opening libraries and expanding library hours both reduce violence and property crimes.

police, in order to circumvent any local sanctuary laws. The department gets a lot of use out of this data, as seen by them running thousands of searches of ALPR databases in a single month as early as 2019. ICE's utilization of this data shows the degree of risk it poses to vulnerable communities. RTCC means ICE is able to search nationwide databases of surveillance data including data from police departments in Washington State, other states with "sanctuary" laws, and non-police entities including the King County Housing Authority.

Appendix B: Public Comment Period (6/03/25 to 6/23/25)

Surveillance technology has the potential to have a chilling effect on free speech rights. RTCC software was used by police to spy on “immigration protests." In 2021 LAPD requested bulk camera data targeting Black Lives Matter protesters. In New York City there is evidence that NYPD has used surveillance technology to surveille Black Lives Matter protesters. Homeless residents, who have no option for privacy, are likely to become targets of mass surveillance. California is using AI to identify and target its homeless residents.

	SPD has a track record of officers abusing their access to surveillance technology. In 2021 SPD Officer Swartz used police data to stalk his ex-girlfriend; in 2020, an officer accessed confidential information about a domestic violence investigation and shared it with someone involved; and just last year, an officer performed an unauthorized search for personal reasons to reveal a citizen's firearm ownership.			
140	It has no real benefit and will harm women and minorities the most	I see no value except to strip individuals of their privacy	People in WA deserve their privacy and do not need their information uploaded to ICE so they	

			can be illiegally abducted
141	Data privacy is being violated by integrating traffic cameras into a crime center. Right now, the Trump administration, ICE, and "red" states with anti-abortion and anti-gender affirming care laws are using any data that they can get from other databases to attack people. Traffic cameras are about traffic laws, not other types of law enforcement. I am tired of being filmed everywhere. There are no rules about data storage. No one takes privacy or safety seriously. How long will these videos be stored? Where will	Traffic cameras make our streets safer by getting people to follow traffic laws. That's it.	If Seattle truly is a safe city for immigrants, trans people, people seeking abortions, etc., then we need to live by those values. This data will be abused. It will not be stored safely, and bad actors will get into it. This also expands SPD's budget. SPD has the LARGEST budget in the City. This means that we, as a city, value SPD over anything else, and we don't have other services because our elected officials have said that SPD is the most important department. We have a budget shortfall because of SPD's out-of-control

	they be stored? Who will have access? There are no governance thoughts put around this.			spending and coming in over budget every single year. It is fiscally irresponsible to keep expanding their budget.
142	That more surveillance will lead to the further over policing of communities that have already suffered from over policing. That these recordings will be shared with ICE and other federal law enforcement	Please don't do this.	No I do not. It is a slippery slope to go down with this.	This is a time where we should be coming together as a city. By installing this technology you are breaching a level of trust with your constituents. This will not be forgotten. Please please do the right thing and do

	that seek to target our city. And that it will lead to mistrust of the citizens of this city of their police force in a critical time where our relationship needs to be mended. This is not the way to mend that relationship.		institute this technology. This will not make our city safer and just adds to potential animosity between Seattle law enforcement and the populace.
14 3	SPD should not have access to traffic cameras. This will erode our civil liberties even further by making it even easier for police and ICE to target black and brown communities, immigrants, and anyone they don't like.	None, whatsoever.	Please focus your resources on building more housing, mental health resources, education, and reducing poverty. Police surveillance will not make us safer, nor will it solve the root causes of inequality and suffering, which make us unsafe.

144	RTCC software such as Fusus poses a threat to our civil liberties, especially our first amendment right of free speech, public protest, and public assembly. RTCC also harms by aiding in criminalizing people seeking abortions and gender-affirming healthcare. RTCC is a threat to women and survivors of sexual assault and stalking. RTCC harms immigrants by giving information directly to ICE, directly supporting the kidnapping of immigrants with no due process. Police control of RTCC cameras leads to censorship and selective	SPD already has a real time crime center. SPD's existing RTCC (iBase) is on-premise, so it doesn't create the risk of data being obtained from third parties or legal requests from those outside Washington state. There is no reason for SPD to obtain a cloud-based RTCC which would weaken state laws and endanger women, trans folks, and immigrant residents.	I do not see any value in this technology. Real safety comes from community care, equitable access to resources, stable housing, food security, childcare, education, and jobs that pay a living wage.	I want City leadership to deeply examine the questions, "What is safety? Do I want safety for everyone?" I want City leadership truly listen to the voices of marginalized people and those standing up for them in the community and let those voices be a guide for what safety could look like instead of increased surveillance.

	punishment. RTCC creates a system ripe for abuse and potential to violate all of our First and Fourth Amendment Rights. Do not expand and allow SPD to purchase another RTCC software to harm our neighbors.		
145	RTCC software makes it impossible to keep surveillance data from ICE. Local police departments are very cozy with ICE and RTCC makes it easier for them to casually share surveillance	ICE has a history of terrorizing immigrant communities. Jurisdictions that do not use local resources to enforce federal immigration laws have lower rates of crime, poverty, and unemployment than those	None. Nashville abandoned its pursuit on FUSUS (the RTCC SPD uses) in April 2025 because it didn't believe any guardrails would keep the Trump Administration & ICE from accessing it.

	data. And, RTCC means ICE is able to search nationwide databases of surveillance data including data from police departments in Washington State, other states with "sanctuary" laws, and non-police entities including the King County Housing Authority.	that chose to collaborate. It was with this knowledge that the Keep Washington Working Act was passed to prevent data sharing between immigration and local law enforcement.		
1 4 6	I'm against SPD obtaining a cloud-based RTCC which would weaken state laws and endanger women, trans folks, and immigrant residents.	Less surveillance, not more.	This a dangerous direction and a slippery slope eroding our freedom.	No to adding a cloud-based RTCC system. Our vulnerable communities would be targeted even more. We are NOT that type of community in Seattle.
1 4 7	This technology will not decrease crime and is ripe for abuse.		None	Investing in communities is the most effective way to decrease crime.

City of Seattle

2025 Surveillance Impact Report Executive Overview

Real-Time Crime Center

Seattle Police Department

Overview

This Executive Overview documents information about the collection, use, sharing, security, and access controls for data that is gathered through Seattle Police Department's (SPD) Real-Time Crime Center (RTCC). All information provided here is contained in the body of the full Surveillance Impact Review (SIR) document but is provided in a condensed format for easier access and consideration.

1.0 Technology Description

Real-Time Crime Center (RTCC) software provides a centralized location for real-time information and analysis. At its core, RTCC software integrates dispatch, cameras (such as CCTV and traffic monitoring cameras), 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.

2.0 Purpose

The purpose of RTCC software is to provide situational awareness to increase officer and citizen 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 aide 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.

3.0 Data Collection and Use

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, SDOT traffic monitoring cameras, 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.

SDOT traffic monitoring cameras (as referenced in the “Closed Circuit Television ‘Traffic Cameras’ (Transportation)” SIR) will be utilized in the RTCC software for law enforcement purposes.

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.

4.0 Data Minimization & Retention

The RTCC software is used to integrate data from various sources used by SPD into one place, a single 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.

5.0 Access & Security

Access

Only authorized SPD, OPA, and OIG 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 legitimate 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.

Security

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.

Retention period for data stored in RTCC software storage will be 30 days, data will be overwritten after that retention period expires. Data associated with criminal investigations will get 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.

6.0 Data Sharing and Accuracy

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.

Data may be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies,

as well as from insurance companies."

Discrete pieces of data collected by the 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 pursuant to properly 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.

7.0 Equity Concerns

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 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.