

Seattle's Real-Time Crime Center

A Civil Rights, Civil Liberties, and Governance Audit

POLICING PROJECT
NYU SCHOOL OF LAW

November 2026

About the Policing Project

The Policing Project at New York University School of Law partners with communities and police to promote public safety through transparency, equity, and democratic engagement. Our work focuses on front-end, or democratic, accountability — meaning the public has a voice in setting transparent, ethical, and effective policing policies and practices before the police or government act. Our goal is to achieve public safety in a manner that is equitable, non-discriminatory, and respectful of public values.

For more information, visit **policingproject.org**.

This report was authored by Barry Friedman, Max Isaacs, Katie Kinsey, Clare Garvie, Farhang Heydari, and Quincy Blair. Special thanks to Jenna Wong for her support.

Table of Contents

Executive Summary 3
- A. RTCCs and modern surveillance technologies collect information about everyone, not just criminal suspects. 4
- B. Limits on the use of RTCC data are an essential safeguard, but so too are mechanisms to ensure circumvention of safeguards does not occur. 5
- C. Because even strong data use safeguards are imperfect, collection becomes a key boundary. 6
- D. "Real time" describes only part of what RTCCs do, and it is important to address why the misnomer matters. 6
- E. The missions of an RTCC can (and do) expand and change. 7
- F. RTCCs present unique risks that may escape existing forms of oversight. 8

I. Seattle's RTCC 10
- A. Technologies in use 10
- B. RTCC workflows 11

II. Governance of the RTCC 14
- A. The Surveillance Ordinance and Surveillance Impact Reports 14
- B. Internal rules and practices 14
- C. Enforcement 14
- D. Key RTCC safeguards 15

III. Benefits: Theories & Evidence of Impact 17
- A. Theories of impact 17
- B. Evidence of impact 18

IV. Risks Analysis & Recommendations 19
- A. Privacy and chilling effects 19
- B. Data sharing 24
- C. Transparency and accountability 27
- D. Equity 34
- E. Auditing 35

Conclusion 36

Appendix A: Auditing Questions 37

Appendix B: Policing Project Evaluative Framework 39

Appendix C: Surveillance Technology Governance & RTCC Oversight 43
- A. Table 1: Surveillance Technology Approvals Process 43
- B. Table 2: SPD Internal Rules, Access, and Accountability 46

Appendix D: Seattle RTCC Technology & Databases 49
- A. Camera Systems 49
- B. Fusus 51
- C. Databases 52

Endnotes 54

Executive Summary

Across the country, law enforcement agencies are adopting real-time crime centers ("RTCCs") — centralized hubs that bring together a variety of surveillance technologies and data.[1] RTCCs help address a growing challenge for law enforcement: as agencies deploy an ever-wider array of surveillance technologies, they face the problem of using these tools effectively and managing the vast quantities of data they generate.[2] RTCCs offer a way to do both, bringing together dedicated personnel and systems in order to better coordinate the use of technologies. Most RTCCs integrate networks of cameras, but many also incorporate technologies such as automated license plate readers (ALPRs), drones, and criminal justice databases.[3] Increasingly, RTCCs incorporate artificial intelligence (AI) tools, allowing agencies to make connections in data that would otherwise be difficult or impossible to discern.[4]

RTCCs — and the surveillance and investigative capacity they centralize — offer potential benefits to public safety. RTCCs can help agencies make more effective use of tools they already possess, provide access to cameras and other sources of information that might otherwise go untapped, and identify connections that personnel could have missed.[5] A promised benefit is that more offenders will be identified, and there is some recent evidence to support this.[6] Additionally, the fact that more offenders may be apprehended, along with the existence of the networked surveillance technologies like cameras that feed into the RTCCs, may serve to deter further offenses.[7] If all goes as proponents of RTCCs suggest, the end result might be less crime. The research on RTCCs remains limited, however, and does not yet present a consistent picture.[8]

Even if these benefits are realized, the use of RTCCs and the technologies they integrate presents significant risks as well. The centralization of surveillance systems and data can enable far more powerful and intrusive forms of surveillance than any one system could accomplish on its own.[9] Centralization of data also can create opportunities for misuse, while the relative novelty of RTCCs and the lack of established policy models raise concerns about oversight and accountability.[10]

Balancing the benefits and risks is difficult (especially in the face of incomplete, and still developing, evidence), but one way to address the problem is to look for regulatory approaches that minimize the risks. Sometimes an analysis of costs and benefits will rule out using particular technologies altogether. More commonly, though, such an analysis can identify potential risks and indicate guardrails that can be put in place to address them.

In 2025, the City of Seattle created an RTCC, and that RTCC makes use of some — but not all — of the technologies used in other jurisdictions.[11] Seattle's RTCC has proponents and opponents, and the city is in the middle of a civic discussion about whether and how these technologies should be used. A research team from the University of Pennsylvania currently is assessing the efficacy of the RTCC — which goes to whether public safety benefits are being achieved.[12]

In May 2026, the Seattle Mayor's Office retained the Policing Project to conduct an independent civil rights and civil liberties review of its RTCC, to look at potential risks, and to identify whether existing guardrails are sufficient as well as whether others are necessary.

To complete this audit, we reviewed relevant public and nonpublic documents and conducted site visits in May and September 2026, which included observation of the RTCC and interviews with RTCC command staff and analysts. We also met with a variety of other City personnel, 911 dispatch staff, oversight bodies, advocates, and others. Before publication, the City and Seattle Police Department (SPD) had the opportunity to review a draft of this report for factual accuracy and to offer feedback. The Policing Project retained final editorial control over the substance and conclusions of this report, and the analysis and recommendations below are ours alone.

Our review does not evaluate whether or not the RTCC should expand its current operations or continue to exist at all. The longstanding position of the Policing Project is that the decision whether, and how, to use surveillance technology ultimately is a matter for local democratic processes to decide. Still, such deliberation requires transparency regarding what technologies are used, and an assessment of whether the appropriate guardrails are in place. Any use of surveillance technology should be governed by safeguards effective to avoid risks to civil liberties and rights. To that end, this report presents our findings and recommendations from the review we conducted.

Several important insights about RTCC governance emerge from our review, each informing our recommendations for Seattle. We summarize some of these insights and corresponding recommendations below; our full findings and recommendations appear in Part IV of the report.

A. RTCCs and modern surveillance technologies collect information about everyone, not just criminal suspects.

Historically, police surveillance would be preceded by an investigation. Officers would identify a suspect and then seek out information relevant to that individual.

But modern surveillance technologies invert this process. Rather than collecting information about particular individuals in connection with specific investigations, police now deploy systems that continuously gather and store vast amounts of information about the public at large. This is known as "indiscriminate" surveillance because data is being collected on individuals who are not suspected of any offense.[13]

This shift has significant implications for privacy. Under the traditional model, surveillance was generally directed at people or activities already of interest to law enforcement. Under the new model, everyone becomes a potential subject of surveillance, regardless of whether they have done anything to attract police attention. This has important implications for some of our findings and recommendations, especially around data collection and access.

B. Limits on the use of RTCC data are an essential safeguard, but so too are mechanisms to ensure circumvention of safeguards does not occur.

Restrictions on how RTCC data may be used — including clear rules regarding who may query data and for what purposes — are essential. Yet recent history demonstrates the frailty of these safeguards. Countless stories have emerged across the country in which surveillance data has been misused for personal purposes or shared with outside agencies in violation of applicable law.[14]

In Seattle's RTCC, personnel are subject to clear rules prohibiting the use of RTCC data for personal purposes or investigations related to immigration or certain forms of health care.[15] As detailed in our report, however, important gaps in SPD's data governance remain. We recommend that SPD:

- **Improve auditing features.** SPD should insist that Axon, its RTCC software vendor, develop new features that (a) require a case number or reason for any camera activation and (b) log any use of object detection or other AI features.
- **Establish internal auditing.** SPD should establish a formal policy for regular internal audits of the RTCC, including checks of whether data was accessed for any prohibited purpose and whether any unusual patterns in system access indicate misuse of tools or data.

C. Because even strong data use safeguards are imperfect, collection becomes a key boundary.

Once data exists, no city or agency can guarantee it will never be shared. Restrictions on data use can be effective in regulating an agency's internal access, but they are of limited utility against data breaches, hacking, or disclosures the law requires, whether in response to a public records request or to valid legal process such as a subpoena or a warrant from another jurisdiction. This means that decisions about what information to collect and how long it should be retained are no less consequential than decisions about who may use it. We recommend that SPD:

- **Make the five-day retention period a matter of formal policy.** SPD policy permits camera footage to be retained for up to 30 days. As a matter of practice, however, SPD has reduced this down to five days for raw CCTV footage, unless that footage is saved to a case file or must be preserved to respond to a legal request. SPD should codify its retention period in policy.
- **Limit unnecessary retention of data.** Once data has been saved to a case file, SPD's practice is to retain that data indefinitely, even after a case has been resolved. SPD should end this practice and should develop retention periods based on case status and disposition and not exceeding those recommended in Washington State's law enforcement records retention schedule.

D. "Real time" describes only part of what RTCCs do, and it is important to address why the misnomer matters.

The "real-time" label promotes RTCCs as a solution to improve an agency's emergency response operations — such as responding to violent crimes in progress. Although most (if not all) RTCCs, including Seattle's, serve this real-time function, many also support retrospective investigations.[16] This means that in addition to operating in "real time," RTCC analysts and those working with them can query retained data about events that have occurred in the past, in an effort to identify information relevant to investigations.

This dichotomy matters. In real-time response situations, immediate action by law enforcement is justified, as police must respond quickly to a situation presenting a threat to public safety. This means that investigators operate without judicial warrants or similar protections. Because the events are unfolding in real time, there also is less uncertainty about who the suspects might be.

Retrospective investigations, however, do not always entail such urgency, and therefore traditional privacy safeguards — such as obtaining a warrant or minimizing the amount of the data accessed — often are much more practicable. These safeguards also are important (if not essential) given that in a retrospective investigation, police may seek to identify a suspect from a universe of possible individuals, in data that investigators can comb through at any time. For these reasons, as explained in the report, warrants may well be *required* when RTCC technologies are used to track an individual's movements retrospectively.

Describing the entire enterprise as "real time" risks blurring the distinction between real-time operations and after-the-fact investigations, and extending permissions justified by emergencies to routine investigations. Accordingly, we recommend that SPD:

- **Limit warrantless tracking.** Warrantless tracking of individuals (i.e., the tracing of a person's location or movements across multiple camera clusters) should be permitted only when police are responding to an active incident and have probable cause to believe a crime is being or has been committed and that immediate action is needed to prevent physical harm to the officers or other persons, the destruction of relevant evidence, or the escape of the suspect. In all other circumstances, tracking generally should require a warrant supported by probable cause.

  Note: It is not "tracking" to check cameras located near a crime scene for suspects. In addition, given the fact that such cameras are near a known crime scene, there is adequate suspicion to justify examining them. Thus, no warrant should be required to do so.

E. The missions of an RTCC can (and do) expand and change.

The intrusiveness of an RTCC depends on the scope of surveillance it conducts, including the number of cameras and other technologies it integrates, and the software used to analyze the resulting data. But RTCCs are designed for expansion — private cameras can be integrated; software updates can give police access to powerful new features. Consequently, an RTCC that is authorized and regulated in one format can become substantially more powerful and intrusive without undergoing the scrutiny that typically accompanies the acquisition of new surveillance technology.

Seattle's RTCC has expanded already from its initial iteration, and SPD is able to integrate additional cameras and other surveillance tools.[17] Whether and to what

extent expansions like these should happen are matters to be resolved through democratic deliberation and appropriate policy-making channels. Policy improvements could be made to aid such discussions and ensure transparency and accountability around these and any future expansions. We recommend SPD:

- **Disclose all tools and features used.** At least twice a year, SPD should publish in a clear and conspicuous location on its website a full list of the tools and features it is actually using — and seeking approval to use — in the RTCC.
- **Disclose information about private camera integrations.** In a report to the City Council's Public Safety Committee, SPD should clarify its plans and policies for integrating private cameras. This report should include information on the number of cameras it plans to integrate and how those cameras are selected.
- **Make privacy safeguards uniform across cameras.** SPD should apply one set of rules to all cameras integrated at the RTCC to the greatest extent that is possible technically. This should include ensuring that non-public spaces are not recorded, whether through privacy masking or other means.
- **Ensure new features are turned off by default.** SPD and its RTCC vendor should memorialize in their contract that new RTCC surveillance features must be disabled by default, and only added after a determination regarding whether the new feature constitutes a "material change" (which, under local law, would require approval by the City Council).[18]

F. RTCCs present unique risks that may escape existing forms of oversight.

Part of the promised value of an RTCC is its ability to connect previously siloed data and technologies. In some RTCCs, this means the ability to search across dozens of police databases and records systems with a simple Google-like search.[19] In others, it means the ability to use drones, ALPRs, and cameras in conjunction with other technology to track an individual with precision.[20] In this way, surveillance tools can prove more powerful when integrated through an RTCC.

Because of this dynamic, a strong policy governing the RTCC is itself essential. Existing policies governing individual surveillance tools may prove inadequate when these systems are used in concert. Although SPD has an RTCC policy, it falls short in a few key respects. We recommend that SPD:

- **Define clearly how the RTCC may be used.** SPD should specify clearly the full range of incident types and other public safety situations for which the RTCC may be used, including standards governing situations in which the nature of an incident is uncertain or an incident may escalate into one that qualifies for RTCC involvement. During any review of the RTCC's authorization, the City Council should consider whether to limit further the circumstances in which the RTCC may be activated.
- **Clarify whether and how the RTCC may be used for passive monitoring.** SPD should clarify the types of events in which it might monitor cameras on an ongoing basis (i.e., not connected with an active incident), for how long, and for what purposes.
- **Develop rules for the surveillance of protests.** SPD should work with its accountability partners to develop rules around the use of the RTCC in relation to protests. These rules should conform to existing rules to the greatest extent possible — e.g., they should require authorization before accessing footage of protests or other political activities.

In sum, our report finds that Seattle has established an important foundation for governing the RTCC; still, significant policy gaps remain.

Ultimately, the decision of whether and how Seattle's RTCC and CCTV programs should be used belongs to the City and its residents. Should Seattle choose to continue these programs, it should act swiftly to address the shortcomings identified in this report. These measures are essential to realizing the potential public safety benefits of the RTCC while protecting civil rights and civil liberties.

I. Seattle's RTCC

This part describes Seattle's RTCC as it operates today. We begin by describing the technologies and databases available to RTCC personnel. We then turn to a description of the RTCC's two main workflows — one which supports officers responding to real-time incidents in the field and the other which supports investigators looking for evidence related to past incidents. Additional details regarding the RTCC's technologies and databases can be found in Appendix D.

A. Technologies in use

At the heart of the RTCC's operations are three key technologies.

First, the RTCC has access to several different camera systems. These include CCTV cameras operated by SPD in the three pilot sites initially approved by the City Council — currently a total of 303 cameras at 61 sites.[21] Each CCTV site is made up of a "cluster" of up to five cameras.[22] RTCC personnel also can access around 100 external security cameras located at nine SPD buildings throughout the city, as well as feeds from approximately 100 traffic cameras operated by Seattle's Department of Transportation.[23]

In addition, the RTCC has access to cameras owned by local businesses, which voluntarily share video feeds with SPD as part of a private-public camera network called Connect Seattle.[24] To participate in the program, businesses with cameras set up a hardware device that enables video footage to stream directly into the RTCC.[25] At the time of our audit, three businesses had shared a total of 23 cameras with the RTCC as part of this program.[26] SPD has taken a step towards expanding this integration by purchasing additional video streaming devices, but it has not yet made plans for their distribution.[27]

Second, the RTCC uses a software platform from Axon (a policing technology company) called Fusus, which enables personnel to view camera feeds from all of the various cameras SPD has integrated.[28] Fusus also provides RTCC personnel with information about ongoing incidents, the locations of officers, and a range of other information in a single visual interface (what Axon describes as a "single pane of glass").[29]

Third, RTCC personnel have access to various databases used across many SPD departments.[30] Among these is SPD's records management system (a platform called Mark43), which stores a wide range of agency records including incident,

booking, and arrest reports and records.[31] Other databases include Omnixx Force, a database owned and operated by Washington State Patrol that contains data about drivers and vehicles; the "Interstate Identification Index," which contains criminal history records; and LexisNexis's Accurint, which provides data such as addresses, telephone numbers, relationships, and information about property ownership.[32]

B. RTCC workflows

The technologies at the RTCC can be deployed in a variety of ways, but most of the RTCC's operations fall into one of two main workflows. First, RTCC personnel assist patrol officers responding to incidents on the ground in real time, typically in response to 911 calls for service. Second, RTCC personnel support investigations into past incidents by locating relevant evidence. Each of these workflows is described below.

1. Real-time response

Most of the RTCC's work involves supporting officers who are responding to incidents on the ground, mainly in response to 911 calls.[33] By accessing the cameras and databases available to them, analysts can provide officers with information about what is occurring at the scene or where a person of interest might have gone. The process of providing real-time support to officers typically comprises three steps.

Step One: Initial Activation. The process begins when RTCC personnel are alerted to an incident, which can happen in a few different ways. Most commonly, 911 dispatchers will enter information about a call for service in Seattle's computer-aided dispatch (CAD) system.[34] Personnel at the RTCC monitor this information proactively and look for opportunities to provide support.[35] RTCC personnel also listen to SPD's radio channels to follow developing incidents.[36] On occasion, responding officers in the field will request assistance from the RTCC directly.[37]

Although SPD's RTCC policy describes the RTCC's purpose as assisting with "serious and violent" crime, SPD's current practice does not limit RTCC assistance to a particular offense type.[38] Personnel may support any call for service. They decide where to focus based on a call's priority level noted in the CAD system.[39]

Step Two: Gathering Relevant Information. Once an analyst begins assisting with an incident, CAD plots the incident's location, which is displayed on an interactive map of Seattle in Fusus.[40] The map also displays any cameras and patrol cars in the surrounding area.[41] The analyst can open one or more live camera feeds, rewind footage, and view multiple feeds simultaneously.[42]

Currently, the process of reviewing camera footage is mostly a manual, analyst-directed process, although on rare occasions, RTCC personnel have used an AI-enabled "object detection" feature in Fusus to search through recorded video.[43] This feature enables personnel to search for ten object types: person, car, bus, train, motorcycle, boat, bicycle, backpack, suitcase, and handbag.[44] RTCC personnel stated they use this function only as a last resort because it frequently produces inaccurate or overinclusive results. During one incident relayed to us, for example, a search for a man wearing a gray top and gray bottom returned an image of a pigeon.[45] (Of course, this feature may well improve in time as the technology advances, which could make its use more attractive to personnel.)

RTCC analysts also can support responding officers by finding relevant information in the various databases to which they have access. For example, if an analyst knows the name of the suspect, they might search for that person's driver's license photo in Omnixx Force or check Mark43 to see if the individual has been involved in any past incidents.[46]

Step Three: Conveying and Saving Relevant Information. RTCC personnel can convey relevant information or data to officers on the ground in a few different ways. In some cases, analysts will access the CAD system and add information directly to the record associated with the incident, which patrol officers can then access from their mobile data terminals. For example, personnel may upload a driver's license photo to assist officers on the ground in identifying a particular person.[47]

Analysts can create a clip or still image in Fusus and save it to a repository known as FususVAULT, where it is kept for 30 days.[48] From there, personnel can transfer clipped video or images to Seattle's digital evidence management system, Evidence.com, where it then can be shared with officers in the field. SPD's current practice is to retain data on Evidence.com indefinitely.[49]

After an incident has concluded, RTCC personnel produce a record of their actions in an "RTCC supplemental report," which is uploaded to Mark43 under the corresponding CAD or investigation number.[50]

2. Retrospective investigations

RTCC analysts also assist with past incidents under investigation by SPD detectives. Rather than collecting and relaying information as events unfold, in this workflow, personnel look back through existing footage and other records to help a detective reconstruct and analyze an incident, and to locate supporting evidence. This typically proceeds in three steps.

Step One: Initial Request. The process begins when detectives send a request for assistance to the RTCC.[51] According to the RTCC's policies, detectives must explain what they are requesting the RTCC do, provide a valid case or CAD number, and provide the RTCC with a law enforcement-related reason for the request.[52]

Once received, personnel must perform two checks. First, they confirm that the case number provided is valid. Second, in compliance with Washington State law, they ensure that the request is not for a purpose related to immigration enforcement or the provision of certain forms of health care.[53]

Step Two: Gathering Relevant Information. Detectives typically request RTCC support to find video evidence of a past incident. This video data generally comes from one of three sources. ***First***, the footage might come from the cameras connected to the RTCC, such as SPD's own cameras. ***Second***, detectives might obtain video footage on their own and ask RTCC personnel to review it. For example, in one case, detectives obtained camera footage from a nightclub and surrounding buildings and asked RTCC personnel to flag any individuals matching a suspect description.[54] ***Third***, SPD maintains a voluntary registry of private cameras that are not integrated directly with the RTCC.[55] If police believe a registered camera may contain footage relevant to an investigation, detectives can send the owner a link through which the owner can provide the footage.[56] Regardless of the source, RTCC personnel may be asked to review the footage and create clips of any video that may be of potential investigative value.

Step Three: Uploading Evidence. If relevant video has been found, RTCC personnel upload it to SPD's digital evidence management system (a platform called Evidence.com) and notify the requesting detective.[57] As with the real-time workstream, RTCC personnel then prepare a supplemental report in Mark43 documenting the assistance they provided.[58]

II. Governance of the RTCC

This part provides a high-level overview of the policy structures that provide guardrails and oversight of the RTCC. It then highlights a set of key guardrails arising from these structures that impact how the RTCC operates. Additional information regarding the RTCC's governance can be found in Appendix C.

A. The Surveillance Ordinance and Surveillance Impact Reports

In accordance with the City's Surveillance Ordinance, any city agency seeking to acquire or use a new surveillance technology (such as the RTCC or CCTV systems) must first draft a surveillance impact report (SIR) and submit it for approval by the City Council.[59] The SIR includes a description of the technology and basic parameters for use.[60] The SIR process also requires community engagement and public review and comment, including through community meetings and review by the Community Surveillance Working Group, which produces a privacy and civil liberties impact assessment for the technology.[61]

Once a SIR is approved, the agency may procure and use the surveillance technology, but only in accordance with the parameters outlined in the SIR and any Council amendments.[62] If the agency wants to pursue any significant, or "material," changes to either the technology or how it will be used, it must submit an updated SIR to the City Council for approval.[63]

B. Internal rules and practices

In addition to the rules established through the SIRs, SPD has a publicly available use policy that sets additional parameters for its use of the RTCC.[64] SPD also is in the process of drafting standard operating procedures that will govern the day-to-day operations of RTCC personnel.[65] Finally, as discussed below, there are various informal practices that inform RTCC operations but are not reflected in written policy.[66]

C. Enforcement

Seattle has three entities that provide oversight of different aspects of SPD's use of surveillance technologies. This oversight comprises the Office of the Inspector General for Public Safety (OIG), which conducts annual audits of surveillance

technology use; the Office of Police Accountability (OPA), which investigates allegations of employee misconduct; and the Community Police Commission (CPC), which provides community input on surveillance policy and practice.[67] In addition, Seattle's IT Office produces an equity impact assessment annually for all surveillance technology used by city agencies, and can direct agencies to stop using a technology in the event of noncompliance with applicable law or policy.[68]

D. Key RTCC safeguards

The various policy structures described above play a significant role in shaping how the RTCC operates. Key safeguards around the RTCC's operations are described briefly below (and are discussed more fully throughout Part IV).

No passive, continuous monitoring. Under SPD policy RTCC personnel generally are prohibited from monitoring camera feeds or accessing other data.[69] In other words, the RTCC generally does not conduct continuous surveillance or virtual "patrols" of the city.[70]

No facial recognition. SPD is prohibited from using facial recognition technology in conjunction with any camera feeds or elsewhere in the RTCC system, per the terms of the SIRs and SPD policy.[71]

CCTV camera masking. SPD policy requires "permanent digital masking" of its CCTV cameras to prevent the recording of private spaces, like second-story windows.[72] Depending on the camera, the affected area appears either pixelated or blacked out in the feed available at the RTCC.[73]

Data retention. Data is retained for a set period of time before it is deleted. This data retention period varies depending on the system in question. As a matter of practice (but not policy), SPD retains CCTV footage for five days, although SPD is permitted by law to retain it for up to 30 days.[74]

Certain Fusus features disabled. SPD does not use every capability that the Fusus platform makes available. Fusus offers, for example, analytics that can generate crime or incident heat maps and identify relationships among people, events, trends, and other variables.[75] SPD represents that it does not use features that are prohibited by, or fall outside the uses authorized in, the SIRs, and we did not observe those features in use during the course of our audit.[76]

ALPR use suspended. SPD has not used ALPRs, either in or outside of the RTCC, since March 2026.[77] This follows the state's passage of S.B. 6002, which restricts

ALPR data collection at sensitive locations, including schools and houses of worship.[78] Because SPD used vehicle-mounted ALPRs that travel throughout the city, SPD determined it could not ensure compliance with the law's location-based restrictions and suspended use while it evaluates whether data collection can be automatically disabled in protected areas.[79]

III. Benefits: Theories & Evidence of Impact

Broadly speaking, Seattle's RTCC promises to do two things: (1) support more effective police response in real time, primarily in response to calls for service, and (2) improve investigations of crimes that have occurred.[80] In particular, in standing up the RTCC the City highlighted the need to "help detect, deter, and prevent" certain categories of criminal activity, namely "gun violence, human trafficking, and persistent felony crime." [81] It chose the RTCC as one way of addressing these issues in light of "unprecedented patrol and investigation staffing shortages."[82]

A. Theories of impact

As discussed in Part I, the RTCC has two main workflows. ***First***, it supports real-time response by allowing trained analysts, in response to a call for service or officer request, to access live camera feeds and databases to provide officers in the field with additional details about the reported situation or person(s) of interest.

It is not hard to see how this kind of added situational awareness could be helpful to patrol officers. Although officers receive information about calls from 911 dispatchers, that information is subject to the knowledge and reliability of the caller, often an uninvolved third party, and dispatch has limited access to external information sources to supplement the caller's description. RTCC personnel can provide information that might not be reported to dispatchers, such as whether the suspect is holding a weapon, what color of clothing they are wearing, or which direction they ran from a scene.[83] We witnessed one example of this in a 911 call, where a suspect in an assault was reported to be wearing a yellow shirt. By accessing cameras in the vicinity of the reported incident, RTCC personnel were able to observe that the suspect had changed clothing and give an updated description to responding officers.[84]

Second, the RTCC supports retrospective investigations. Here, stored camera footage can provide valuable evidence, particularly when investigators begin with little more than the location where an offense is believed to have occurred. RTCC personnel also can take on the labor-intensive task of reviewing large volumes of video, allowing detectives to focus their time on pursuing other leads or taking other investigative steps.

B. Evidence of impact

Although the potential benefits of the RTCC as described by the City are plausible, the current research base supporting these benefits is thin.[85] There is more robust research studying the public safety impacts of CCTVs on their own (i.e., not connected to an RTCC), but that research is best characterized as mixed.[86]

SPD has published some data on RTCC impact, including that officers and detectives are three times more likely to arrest a suspect when they receive support from RTCC analysts.[87] SPD statistics also reflect that in 2025, the RTCC assisted in 17 homicide cases, with its support helping to close 10 of these cases.[88] In SPD's data analysis, however, it defines RTCC "support" as a case in which an RTCC analyst takes any action (such as checking a camera), regardless of whether that action yielded any useful information or meaningfully impacted the investigation.[89]

OIG has engaged a research team from the University of Pennsylvania ("Penn") to conduct a fuller evaluation of the RTCC program's efficacy. Specifically, Penn is evaluating the City's theories of change that the RTCC would: bolster police effectiveness in public places where crime is concentrated; deter criminal behavior when public notice is posted; and gather evidence to hold offenders accountable.[90]

To evaluate these goals, Penn is exploring RTCC use by offense type, call source (e.g., 911 call for service, officer-initiated action), and location.[91] It also is examining whether the implementation of the RTCC was associated with changes to the number of felony criminal incidents, violent crime incidents, human trafficking offenses, criminal arrests, stops, and calls for service.[92] To evaluate investigative benefits, the Penn team is examining whether there have been increases in case clearance and successful prosecutions, and whether RTCC assistance and its associated technologies improve the likelihood of case clearance.[93]

This evaluation remains ongoing, with results expected to be published in late 2027.[94] Until these results are published, any assessment of the RTCC's overall effectiveness necessarily remains preliminary.

IV. Risks Analysis & Recommendations

Like other surveillance technologies, RTCCs and CCTV systems can pose substantial risks to civil rights and civil liberties. These risks take a variety of forms, including privacy intrusions, personal misuse of collected data, unauthorized data sharing, and more.

As discussed in Part II, SPD has adopted several meaningful safeguards. This part focuses on the gaps that remain — places where key safeguards are missing or rest on practice rather than written policy, where rules are unclear, or where commitments have not been met.

A. Privacy and chilling effects

The advent of powerful new surveillance technologies poses substantial risks to individual privacy. A few decades ago, one scarcely could have imagined that police would be able to recreate a person's past activities, movements, or associations with a quick search of a database. Yet a proliferation of cameras, sensors, and AI analytics is moving us ever closer to that reality, giving law enforcement unprecedented power to monitor individuals in their everyday lives.

This section examines the impact of RTCC surveillance on privacy, as well as specific concerns raised by the surveillance of protest activity. We first consider whether RTCC surveillance has Fourth Amendment implications. It is important to recognize, however, that the Fourth Amendment is *not* the last word in terms of what individual privacy requires. It is incorrect to understand Supreme Court decisions as providing authority or permission to engage in practices that impact personal privacy. The United States Constitution provides only a "floor" for government conduct — law enforcement cannot engage in activities that go below that floor. When the Supreme Court speaks to an issue, it is only stating what law enforcement may not do. It also bears noting that Washington State's Supreme Court often interprets the Washington State Constitution to confer greater rights than the Fourth Amendment, further restricting law enforcement activity.[95]

In addition, federal constitutional law in this area is in flux. That should not be surprising; it necessarily needs to evolve as technology itself evolves. For that reason, what is constitutional today may not be tomorrow. In order to ensure that evidence collected or used by police today will be deemed admissible in court at a later date, it is wise to try to anticipate the direction in which the law will evolve.

Perhaps most importantly, it is a matter of public deliberation, and ultimately is up to the Seattle City Council, to specify what local law enforcement is authorized (or not) to do with regard to surveillance. A judicial decision that certain law enforcement surveillance activities may not run afoul of either the U.S. or Washington State Constitutions is not a substitute for legislative authorization of the same. Communities may well choose to create limitations on permissible surveillance capabilities beyond what federal and state constitutional law require. Seattle's Surveillance Ordinance recognizes the importance of such democratic authorization when it comes to government surveillance, especially with regard to potential invasions of privacy. In fact, the Ordinance's surveillance technology approval process creates an explicit pathway for policymakers to make independent judgments about whether police practices are consistent with their own values and expectations of privacy.[96]

1. Fourth Amendment implications

The Fourth Amendment, which protects individuals against unreasonable government intrusions, provides a useful starting point for evaluating privacy concerns.[97] Courts have long relied on the Fourth Amendment to assess the constitutionality of surveillance tools, from thermal cameras to GPS trackers.[98] In what follows, we discuss police use of RTCC tools through the lens of the Fourth Amendment.

In determining whether a government practice violates the Fourth Amendment, courts begin by evaluating whether the practice constitutes a "search" or "seizure." If it does, a warrant based upon probable cause generally is required.[99] There are, however, exceptions. For example, under the "exigent circumstances" exception, police may conduct a search without a warrant when immediate action is needed, such as to prevent imminent harm to the public or when there is ongoing pursuit of a suspect.[100]

In addition, the Supreme Court has begun to recognize the difference between surveillance of someone suspected of a crime and surveillance of the entire public to build a database to use for retrospective (backward-looking) investigations. As the Court noted in *Carpenter v. United States*, a case involving police access to cell phone location records, the indiscriminate collection and retention of data for investigative use "gives police access to a category of information otherwise unknowable."[101] Police can "travel back in time to retrace a person's whereabouts" — and not just those who are under suspicion. Rather, the Court explained, "this newfound tracking capacity runs against everyone."[102]

Below, we explain why courts may find certain forms of RTCC surveillance to constitute a "search" under the Fourth Amendment. We then explain when a warrant should be required to conduct such surveillance.

a. Is RTCC surveillance a search?

Police activity constitutes a "search" under the Fourth Amendment when it violates an individual's "reasonable expectation of privacy."[103] In general, courts have held that traditional CCTV surveillance of particular locations does not constitute a search.[104] But those cases generally pertain to CCTV surveillance of a particular property or individual under investigation. Courts have not yet grappled with the implications of RTCCs, which integrate hundreds or thousands of cameras into a single system, enabling a form of indiscriminate surveillance and tracking of individuals that goes far beyond traditional CCTV monitoring. As explained below, the surveillance capabilities of expansive camera networks raise constitutional concerns that are not present in more limited forms of CCTV monitoring.

Of particular concern is the capability of RTCCs — with their large networks of cameras and ability to store and analyze the resulting data — to track an individual's movements. Although several decades ago the Supreme Court held that individuals have no expectation of privacy on open roads, in recent years, the Supreme Court repeatedly has ruled that certain forms of technology-driven location tracking by police constitute a search under the Fourth Amendment.[105] As the Court explained in a case involving cellphone location data, tracking a person's movements can reveal deeply personal information, including their "familial, political, professional, religious, and sexual associations."[106]

To be sure, Seattle's CCTV system is, at present, fairly limited, with cameras located only in particular neighborhoods and only at particular intersections and corridors. As such, the possibility of tracking a person beyond constitutional bounds may be somewhat limited. Yet RTCCs are dynamic systems. Seattle's program already has been authorized to expand from three deployment areas to six, and SPD has authorization to add private cameras, which potentially could number into the thousands.[107] As the network expands, it may come to resemble forms of location tracking that have raised serious Fourth Amendment concerns.

Although this area of law is unsettled, it is fair to say that RTCC-facilitated location tracking eventually may come under constitutional scrutiny, and that this

possibility may become more likely as the RTCC expands in scope and capabilities.

b. When is a warrant required?

As discussed above, when police wish to conduct a search, they generally must first obtain a warrant based upon probable cause. The reason for this is that a "search" is a serious infringement on a person's constitutionally protected reasonable expectation of privacy. This sort of intrusion is permitted when there is adequate "cause" (suspicion) to do so.[108] The reason for the warrant requirement — often discussed in legal decisions — is that the decision to conduct such a search should be made by a neutral magistrate who is removed from the immediacy of the investigation itself.[109] The Fourth Amendment recognizes exceptions to the requirement, however. This includes exigent circumstances in which there is a "compelling need for official action and no time to secure a warrant," such as when police are in active pursuit of a suspect following a crime.[110] (If law enforcement conduct constitutes a constitutional "search," the law never excuses the requirement that there be adequate "cause" — i.e., suspicion. Exigency simply excuses the officer from the requirement of getting a judicial determination that adequate suspicion exists.)

Here, a distinction must be drawn between real-time operations and retrospective investigations. In the context of real-time operations, RTCC personnel often are supporting officers responding to crimes in progress or other emergencies. When there is insufficient time to obtain a warrant, the exigent circumstances exception may permit warrantless surveillance. Retrospective investigations, by contrast, do not usually entail such urgency. Officers may well have time to seek judicial authorization before conducting a search, and when that is the case, the ordinary warrant requirement should apply.

In making this recommendation, two clarifications are in order. First, this rule would apply only to an activity — the tracking of an individual's movements — that raises constitutional concerns. It would not require police to obtain a warrant when reviewing footage for other purposes, such as examining a crime scene, searching for physical evidence, or determining whether an individual was present at a particular location, so long as officers did not then use the footage to track that individual's movements. It also should be reiterated that this rule would not require police to obtain a warrant when exigent circumstances exist, such as when there is a danger to public safety or the threat of destruction of evidence. (Still,

as noted, for any tracking that constitutes a legal "search," even in exigent circumstances, there still must be adequate suspicion.)

Second, it is up to Seattle and its policymakers to decide in the first instance whether some limited degree of tracking without a warrant should be permitted. For example, in weighing the relevant privacy and public safety interests, policymakers could decide to permit tracking across a limited number of cameras or for a limited duration of time without requiring a warrant. (Of course, if a case involving such tracking comes to court, the courts will decide what the constitutional limits are and whether they have been exceeded in a given situation.)

Questions have been raised about why law enforcement should ever need a warrant to examine data already in its hands, such as footage from its own CCTV cameras or records from its license plate readers. The answer is that possession and permission to search are different things, and the law has long treated them that way. For example, the Fourth Amendment sometimes distinguishes between seizing evidence and searching it: police who lawfully take a suspect's phone at arrest must first obtain a warrant to look through it.[111] A similar principle applies to information: testing a lawfully collected blood sample is itself a search; courts have required a new warrant before police search lawfully seized computer data for evidence of a different crime; and federal law requires a court order before investigators can obtain tax information the government already holds.[112] This distinction between possession and permission becomes critical when people have no meaningful option to avoid being subjected to surveillance.

Recommendation 1: Warrantless tracking of individuals (i.e., the tracing of a person's location or movements across multiple camera clusters) should be permitted only when police are responding to an active incident and have probable cause to believe a crime is being or has been committed and that immediate action is needed to prevent physical harm to the officers or other persons, the destruction of relevant evidence, or the escape of the suspect. In all other circumstances, tracking generally should require a warrant supported by probable cause.

Note: It is not "tracking" to check cameras located near a crime scene for suspects. In addition, given the fact that such cameras are near a known crime scene, there is adequate suspicion to justify examining them. Thus, no warrant should be required to do so.

2. Surveilling protests

Monitoring protests is among the most sensitive forms of police surveillance. There is a long history of law enforcement surveilling activists and social movements, from the Civil Rights Movement of the 1960s to more recent Black Lives Matter and anti-ICE protests.[113] Such surveillance can produce significant "chilling effects," causing individuals to change their behavior, self-censor, or refrain from participating in political activity out of fear that their presence will be recorded and used against them in some way.[114]

SPD has established rules for the surveillance of protests, which SPD's RTCC policy incorporates by reference.[115] These rules restrict video recording of public demonstrations to certain personnel and require prior authorization from a lieutenant or higher-ranked official, subject to certain exceptions.[116] These rules meaningfully constrain when officers may record demonstrators.

It is unclear, however, how these rules apply in the RTCC context. The existing rules are designed to govern situations in which officers affirmatively decide to record a demonstration, rather than situations in which cameras continuously record public spaces and incidentally capture protest activity. Because the RTCC integrates CCTV cameras that record continuously, demonstrations may be captured without any officer making a deliberate decision to record them or obtaining the authorization ordinarily required under SPD policy. This raises questions about whether the existing rules adequately address the surveillance of demonstrations through the RTCC.

> **Recommendation 2:** SPD should work with CPC and OIG to develop rules around the use of the RTCC in relation to protests. These rules should conform to existing rules to the greatest extent possible — e.g., they should require authorization before accessing footage of protests or other political activities.

B. Data sharing

Community members have expressed concern that RTCC data could be shared with outside law enforcement agencies seeking to enforce immigration laws or investigate reproductive or gender-affirming health care services. Washington State and the City of Seattle have adopted various laws restricting the sharing of data for these purposes, but these laws do not eliminate entirely the risk that outside agencies could obtain RTCC data for such investigations.[117] There are two ways in which outside agencies might still obtain access to such data: (1) through

a public records request to SPD; and (2) through compulsory legal process, such as a subpoena or warrant served on SPD (or on Axon, the company that stores some of SPD's video data). We discuss each potential pathway below.

1. Public records requests

Under Washington's Public Records Act (PRA), agencies such as SPD generally are required to make public records (including video footage) available to anyone who requests them, subject to certain exemptions and redactions.[118] Although it may seem unusual for another law enforcement agency to seek records through a public records request, SPD has stated it directs *all* external requests for CCTV footage, including those from other law enforcement agencies, to the PRA process.[119]

In October 2026, the Mayor's Office formalized a policy for reviewing "sensitive requests" for SPD data that governs these requests.[120] Under the policy, if SPD identifies a records request as relating to civil immigration enforcement or reproductive or gender-affirming health care, the request must be referred to the Mayor's Office General Counsel for review and SPD may not release any data until this review is complete.[121] If the General Counsel determines that the request relates to one of these purposes but is legally permissible, SPD may disclose the data only with the Mayor's consent.[122] Relatedly, city ordinances also require SPD to pause CCTV data collection for 60 days if the City is required to release CCTV data for use in civil immigration enforcement or a reproductive or gender-affirming health care matter.[123]

These processes provide some protection, but they cannot eliminate the risk that an outside agency could, through the PRA process, obtain data for an immigration- or health care-related investigation. Requesters generally are not required to disclose the purpose for which they seek records, so SPD may have no way to identify whether a given request pertains to one of the sensitive areas covered by the Mayor's Office policy.[124] And even when SPD can identify such a request, the grounds on which the City can deny it are narrow.[125]

So long as SPD retains CCTV footage, some risk exists that such footage could be disclosed under the PRA for purposes contrary to Washington's and Seattle's laws and policies. Ultimately, it is up to Seattle policymakers to determine whether that risk is acceptable.

2. Compulsory legal process

Another way an external agency could obtain SPD data is through a legal order such as a subpoena. There are two potential targets for such an order: SPD itself (which maintains the raw CCTV footage on local hardware) and Axon (which hosts video clips and associated reports in its cloud).[126] As with PRA requests, the Mayor's Office policy directs SPD to elevate subpoenas and other court orders for sensitive data that it receives to the Mayor's Office General Counsel for review before responding.[127]

Although Washington and Seattle laws generally prohibit public employees from sharing data for immigration enforcement or investigations involving protected health care, they cannot prevent federal agencies from obtaining a subpoena or other court order compelling disclosure of such data, or prevent compliance if such an order is issued.[128] Seattle could try to challenge, or "quash," such an order in court, but there is no guarantee it would succeed.[129] The outcome would depend on several factors, including the particular law being enforced, the circumstances of the investigation, and the nature of the data requested. The ultimate decision rests with a judge.

An agency also could seek to compel production of RTCC data from Axon, which stores some of SPD's video data on its cloud platform, Evidence.com. Under a federal law known as the Stored Communications Act, Axon is required to produce data to law enforcement pursuant to certain types of court orders.[130] Under the law, Seattle may have an opportunity to intervene to block disclosure, but it is not clear if Axon would do so, and — again — there is no guarantee that it would succeed.[131]

Short of ceasing to retain RTCC data altogether, SPD cannot eliminate fully the risk that such data could be obtained and used for purposes prohibited under Washington law. SPD's practice of retaining raw CCTV footage for only five days does help to mitigate risk by limiting the total amount of footage available for disclosure. However, video clips and other data stored on Evidence.com are retained by SPD indefinitely, resulting in a substantial and growing repository of data that outside agencies could seek to obtain.[132]

Recommendation 3: SPD should end its practice of indefinitely retaining all data stored on Evidence.com. Instead, it should develop retention periods for such data based on case status and disposition, not exceeding those recommended in Washington State's law enforcement records retention schedule.[133]

Recommendation 4: The City should adopt and publish a policy stating how it will respond in the event a demand arrives at SPD or Axon for RTCC data relating to an immigration- or health care-related investigation, including whether the City will intervene and seek to quash the order as a matter of course when a good-faith legal basis exists.[134]

3. Investigative assistance to outside agencies

Aside from the sharing of data, there is one additional situation in which SPD might share RTCC-related information with outside agencies: at times, SPD detectives will provide direct investigative support to outside agencies. For example, an outside agency might ask an SPD detective to determine whether a suspect was seen on camera at a particular place. The detective might then contact RTCC personnel to check camera footage. In this scenario, SPD would not share the footage itself with the outside agency, but might communicate any relevant findings — for example, whether the suspect was observed at the location in question.

The RTCC's draft standard operating procedures require analysts to confirm that the case in question does not relate to immigration enforcement or protected health care.[135] However, RTCC analysts do not always have information about the nature of the investigation in question.

Recommendation 5: SPD should finalize its draft RTCC procedures requiring analysts to verify that a request is tied to a valid SPD case and does not relate to immigration enforcement or protected health care. The procedures should direct analysts to decline any request the purpose of which they cannot confirm.[136] All requests should be logged, and that record should be made available for OIG's review during its annual audits.

C. Transparency and accountability

Clear, public rules are essential to the sound governance of surveillance systems. Without clear rules in place, officers lack guidance on how these systems may be used, supervisors lack standards for ensuring compliance, and the public cannot make decisions about whether surveillance system use is appropriate and in line with Seattle's values.

As noted above, Seattle's Surveillance Ordinance is the primary vehicle through which the City Council codifies rules for the use of surveillance technology.[137] Under the ordinance, city agencies must receive City Council approval prior to

acquiring a surveillance technology. Agencies obtain this approval by drafting a surveillance impact report (SIR) which describes the technology and basic parameters for its intended use.[138] If the City Council approves the SIR, the agency may use the technology, but only in accordance with the SIR and any Council amendments.[139] Any subsequent, significant changes to either the technology or how it will be used require an updated SIR approved by the City Council.[140]

In addition to the rules established through the SIRs, the RTCC is governed by SPD's policy for the RTCC, as well as by standard operating procedures (currently in draft form) that set additional parameters for its use.[141]

Although guardrails for the RTCC exist, there are three deficiencies that undermine transparency and accountability: (1) SPD has not followed through on certain commitments made in the SIRs; (2) some rules governing the RTCC are vague or not embodied in written policy, leaving critical protections to SPD's discretion; and (3) the rules addressing expansions of the RTCC are not adequate.

1. Outstanding SIR commitments

In the SIRs, SPD made two commitments related to the RTCC that remain outstanding. ***First***, SPD committed to creating a public data dashboard to report on RTCC use, including camera locations and the number of police actions taken.[142] At the time of this audit, the dashboard had not been published, although SPD states that it is close to being finalized.[143] ***Second***, SPD stated it would develop an "omnibus surveillance technology policy" that would address, among other things, internal processes for technology approval and procurement, tracking metrics, and retention requirements and limitations.[144] SPD personnel told us that drafting of the policy was underway but was delayed due to personnel turnover.[145]

There are several reasons why SPD should fulfill these commitments. Because they are promised in the SIRs, the law requires it. Following through on publicly stated promises also promotes public trust. And these particular commitments would fill key transparency and accountability gaps by disclosing important information about the RTCC's operations and establishing rules around topics not addressed under the existing RTCC policy, such as procurement.[146]

Recommendation 6: SPD should launch the data dashboard as soon as possible, and no later than three months from now (i.e., publication of this audit report). In addition to including the reporting criteria identified in the SIR (i.e., areas where cameras are recording, resulting number of police actions such as arrests or warrants), the

dashboard should include statistics on frequency of RTCC use, the types of offenses it was used for, the type of support provided, and a broader array of case dispositions (e.g., crisis referral, investigation open or pending).

Recommendation 7: SPD should finalize a draft of the omnibus surveillance technology policy to send to its accountability partners — CPC and OIG — for review within three months of publication of this audit report.

2. Vague and unwritten rules

Currently, certain key safeguards remain unclear or not written in formal policy, which creates uncertainty for the public about what the rules actually are and provides SPD with too much leeway to set them.

a. Qualifying offenses

The SIRs are vague in their descriptions of the RTCC's approved purposes. The City, in its proposal to stand up the RTCC, emphasized the need to combat "gun violence, human trafficking, and persistent felony crime."[147] But the SIRs contemplate the RTCC being used more broadly, including for "serious criminal event[s]" — a term that is not defined in law and that SPD currently interprets to include misdemeanors of all kinds.[148] For a time, the RTCC operated under guidance that limited its ability to assist with misdemeanors. SPD found this challenging from an operational perspective, stating that it is essential for it to have broad flexibility in determining which incidents the RTCC can support because minor incidents can escalate to become serious.[149] For example, during this time, in one instance, a call about an erratic driver came in; however, because personnel could not ascertain whether the driver was intoxicated, they did not take action.[150]

Still, the imprecise language around approved purposes is problematic for several reasons. ***First***, it can obscure the scope of public approval and facilitate mission creep, where technology approved for one purpose gradually comes to be used for others.[151] ***Second***, clarity around authorized purposes is essential to enable meaningful evaluation of the program's benefits and costs.[152] And ***third***, clarity and consistency are important to enable effective operation of the RTCC. During our RTCC observations, analysts cited the changing directives about whether they were authorized to assist with misdemeanors as causing confusion about when to engage.[153]

Whether to permit use of the RTCC for lower-level incidents is an important policy question. That is why SPD should articulate the incidents for which it wishes to use the RTCC, and the City Council should draw clear, unambiguous lines in its authorizing ordinances. Currently, neither has done so.

Recommendation 8: SPD should clearly specify the full range of incident types and other public safety situations for which the RTCC may be used, including standards governing situations in which the nature of an incident is uncertain or an incident may escalate into one that qualifies for RTCC involvement. During any review of the RTCC's authorization, the City Council should consider whether to further limit the circumstances in which the RTCC may be activated.

b. Data retention for video footage

One of the most consequential aspects of surveillance systems is how long the data is retained after it has been captured. If footage no longer exists, police cannot mine it to reconstruct a person's movements after the fact, cannot search it to identify people at a protest, and cannot share it with outside agencies, even when demanded by a court order.[154]

Currently, SPD's practice limits the retention of raw data from SPD-owned CCTV cameras to five days, which is well below the 30 days permitted by the SIRs and SPD policy.[155] This five-day retention, however, is a matter of practice and not written policy, and thus could be changed at any time.

Recommendation 9: SPD should make its five-day retention period a matter of written policy.

c. Integrations

An RTCC can include a range of different data sources and technology integrations, and both the benefits and risks of a system depend greatly on its particular makeup. Yet, neither the SIRs nor SPD's RTCC policy makes clear which technologies and features SPD currently is using. The SIRs give examples of "current or expected SPD technologies" integrated into the RTCC and mention numerous "potential features" that an RTCC *could* integrate.[156] In a similar vein, SPD's RTCC policy merely lists features that the RTCC "may use" — a list that includes a vague catch-all for "[o]ther systems not listed."[157]

Some level of generality might have been necessary for the initial SIRs, which the Surveillance Ordinance requires agencies to produce before deploying a system.[158] But continuing to rely on a general description of RTCC features when

it is up and running leaves the public without a reliable way to know which features and technologies actually are being used.

Recommendation 10: At least twice a year, SPD should publish in a clear and conspicuous location on its website a full list of the tools and features it is actually using — and seeking approval to use — in the RTCC.

d. Inconsistent safeguards across camera types

Seattle's RTCC integrates both public cameras and privately owned cameras.[159] From an operational perspective, the distinction between these different camera systems is slight. SPD can access private cameras through the RTCC and use such footage for real-time operational support and retrospective investigations much as it does footage from publicly owned cameras.

Yet, in several key areas, SPD safeguards differ depending on the camera type. For example, SPD ensures that its CCTV cameras don't record private spaces by applying "permanent digital masking," but does not require the same of non-SPD cameras.[160] Retention periods also vary by camera type — raw footage from SPD's CCTV cameras is retained for five days, whereas retention for private cameras is entirely up to the discretion of each camera owner.[161] And while SDOT has a public map of its traffic cameras, which the RTCC integrates, SPD's public camera location map only includes its CCTV cameras and not privately integrated cameras.[162]

Recommendation 11: SPD should apply one set of rules to all cameras integrated at the RTCC to the greatest extent that is possible technically.[163] This should include ensuring that non-public spaces are not recorded, whether through privacy masking or some other means.

e. Large-scale events

The rules around when and how the RTCC can monitor cameras in connection with large-scale events require clarification. RTCC policy states that the RTCC "will not conduct proactive activities or surveillance without a corresponding call for service" or "active case number."[164] At first glance, this would appear to prohibit passive monitoring of cameras absent an active incident. During the 2026 World Cup tournament, however, SPD created a case number for the World Cup and streamed live camera feeds at the RTCC throughout the event.[165]

There may be circumstances in which SPD may wish to activate cameras for large-scale events absent a call for service. But these circumstances should be articulated clearly in policy to avoid arbitrary and opaque decision-making.

Recommendation 12: SPD should clarify the types of events in which it might monitor cameras on an ongoing basis (i.e., not connected with an active incident), for how long, and for what purposes.

3. Future expansions

The intrusiveness of any RTCC depends on the scope and scale of the surveillance tools it integrates — how many cameras and other tools it incorporates, and what software it uses to analyze them. Seattle's RTCC is relatively modest today, but RTCCs are built to expand. Seattle's has grown from its initial iteration, with the addition of more cameras in more locations across the City.[166]

Such expansions require appropriate transparency and governance. This section outlines three areas in which clearer rules are needed to ensure changes to the RTCC are subject to appropriate oversight.

a. "Material changes"

Seattle's Surveillance Ordinance requires agencies to update SIRs and receive City Council approval whenever there is a "material change" to a previously authorized surveillance technology.[167] The Ordinance describes a material change as one that alters "the purpose or manner in which a surveillance technology may be used," including "technology upgrades."[168] The City's IT Office also has a surveillance policy which contains additional — albeit still general — guidance on how agencies should navigate the material change process.[169]

The current process for identifying material changes gives too much discretion to SPD. According to City policy, it is "incumbent upon departments" using a surveillance technology to define, identify, and report changes in capabilities or use.[170] In other words, responsibility for identifying material changes rests primarily with SPD itself. As the IT Office noted, it is essentially a "trust-based process" that depends on agencies themselves making an accurate and full disclosure of any changes.[171] Instead of leaving the material change determination to the sole discretion of SPD, there should be external, independent oversight to provide a meaningful check.

Recommendation 13: As part of its annual surveillance review of the RTCC, OIG should conduct a "material change" review, evaluating how current RTCC use and capabilities compare to those approved by the operative SIR. OIG should identify any changes it deems "material" that were not previously reported and thus require SPD to submit an updated SIR.

b. Private camera integrations

Through its Connect Seattle program, SPD can stream video directly into the RTCC from cameras owned by private businesses located anywhere in the city.[172] This private camera integration program has the potential to change fundamentally the scale and scope of the RTCC's camera network. The program is currently small. At the start of our audit, one business had integrated a total of 15 cameras.[173] During the course of our audit, two additional businesses signed up for the program, bringing the total number of cameras integrated to 23.[174] And there is reason to think it may expand further: SPD currently has in its possession, and available to distribute, approximately 100 devices that enable private camera integration. As of the time of publication of this report, SPD had not identified any particular recipients for these additional devices.[175]

Neither the SIRs nor any existing policies provide guidance regarding how far SPD may expand its private camera integrations.[176] The City Council did require SPD to provide a report to the Public Safety Committee on its plans for private camera use.[177] However, the report SPD submitted addressed a *separate* private camera program in which residents register their security cameras so that SPD can request footage in case of a nearby incident; cameras in this program are not directly integrated into the RTCC.[178]

Recommendation 14: In a report to the City Council's Public Safety Committee, SPD should clarify its plans and policies for private cameras that are directly integrated into the RTCC. This report should include information on the number of cameras it plans to integrate and how those cameras are selected.

c. New Fusus features

Axon, the developer of the Fusus platform, can add or modify Fusus features, changing how the software can be used without any action on SPD's part. SPD has asked Axon to disable new surveillance-related features by default, and Axon generally has done so.[179] But this agreement is informal and not recorded in SPD's contract with Axon.[180]

Recommendation 15: SPD and its RTCC vendor should memorialize in their contract that new RTCC surveillance features must be disabled by default, and only added after a determination regarding whether the new feature constitutes a "material change" (which, under local law, would require approval by the City Council).

D. Equity

Some community members have raised concerns regarding where SPD has located its CCTV cameras.[181] In particular, SPD data shows that the three initial pilot areas for the CCTV program have higher proportions of people of color than Seattle as a whole.[182]

This issue is not uncomplicated — on the one hand, if the cameras prove to help reduce or solve crime, then it makes sense to put them where crime is most prevalent.[183] SPD states that it decided on the three initial pilot areas based on an analysis of data on serious crime in the City.[184] On the other hand, this approach risks concentrating surveillance in communities that already are heavily policed.[185] With more surveillance comes the potential for disproportionate intrusions on privacy, as well as an increased likelihood of police scrutiny and enforcement.

Whatever approach Seattle takes, decisions about where to deploy surveillance should be transparent to the public and grounded in data. In both respects, SPD's current practices could be improved. First, SPD has not made public the data underlying its camera-placement decisions, making it difficult for policymakers and the public to evaluate those decisions. Second, SPD policy does not require periodic reassessment of camera placements to determine whether continued surveillance remains justified.[186] This is an important omission: public safety conditions change over time, and the circumstances that warrant surveillance in a particular area today may no longer justify it in the future (and vice versa).

Recommendation 16: SPD should disclose publicly the data and analysis underlying decisions about where cameras are deployed. If deployment is based on crime patterns, calls for service, operational needs, or other considerations, SPD should provide the relevant data. The agency need not reveal any sensitive operational information — only the data necessary to allow for a meaningful assessment of whether deployment decisions rest on a sound basis.

Recommendation 17: SPD should reassess at least annually whether the conditions that justified camera deployment continue to exist. Just as reassessment of changes in crime patterns, victimization, case clearance rates, or other investigative outcomes

informs where cameras are needed, this same data would help ensure that cameras do not simply remain in place because they once were justified.

E. Auditing

Rules governing surveillance technology protect the public only if they are followed; too often, however, they are not.[187] Recent reports from across the country have documented instances of police using or sharing surveillance data for purposes prohibited under state laws, including the unlawful sharing of data with federal agencies for purposes of immigration enforcement.[188] There also are numerous examples of officers in various departments misusing surveillance systems for personal purposes, such as stalking or monitoring current or former romantic partners.[189]

Auditing is essential to verify compliance with the law and identify and deter misuse. But effective auditing requires two things to be in place. First, systems must be designed in a way that facilitates auditing — that is, they must produce a record of system activity sufficient to detect potential issues.[190] Second, audits must be performed with enough regularity to ensure that any problems are identified and addressed promptly.[191]

SPD's auditing regime could be strengthened on both fronts. Fusus does log user activity in audit logs, but it does not require RTCC personnel to enter a case number or reason in connection with the viewing of camera feeds.[192] Therefore, auditors have no way of knowing whether surveillance footage was accessed for a prohibited purpose.[193] Moreover, according to SPD, Fusus does not log the use of certain features, such as the software's AI object detection capability.[194]

Regarding SPD's auditing process, OIG performs external audits of SPD's surveillance technologies, including the RTCC. These audits, however, are performed once a year.[195] Although SPD personnel also conduct occasional internal audits, these are informal, and neither their frequency nor their scope is established by binding policy.[196]

Recommendation 18: SPD should insist that Axon develop new features for Fusus that (a) require a case number or reason for any camera activation and (b) log any use of object detection or other AI features.

Recommendation 19: SPD should establish a policy for regular internal audits of the RTCC, including checks of whether data was accessed for any prohibited purpose and whether any unusual patterns in system access indicate misuse of tools or data.

Conclusion

The advent of RTCCs is changing the nature of police surveillance. By bringing together technologies, data, and dedicated analysts, RTCCs can make existing surveillance tools more effective. This can yield important public safety benefits. At the same time, however, such surveillance implicates important privacy interests and raises difficult questions of governance. RTCCs can facilitate widespread, indiscriminate surveillance of the public, collecting information about individuals who are not suspected of any wrongdoing. And they can lead to the tracking of individuals in ways that threaten individual privacy. Technology, moreover, is not standing still. The nature and usage of RTCCs are dynamic: as additional cameras, data sources, and analytics are incorporated, they can become increasingly powerful, risking greater intrusions upon individual privacy.

Through its Surveillance Ordinance, the SIR approval process, and SPD's written policies, Seattle has established an important foundation for governing the RTCC. Still, this report has indicated important gaps. Some existing safeguards are matters of informal practice rather than written policy; others are unclear or lack adequate mechanisms to ensure compliance. In yet other instances, existing rules do not adequately account for how RTCCs can enable or enhance forms of surveillance — such as tracking individuals' movements — beyond what traditional tools can accomplish on their own.

Ultimately, the decision of whether and how Seattle's RTCC and CCTV programs should be used belongs to the City and its residents. Should Seattle choose to continue these programs, it should act swiftly to address the shortcomings identified in this report. Doing so will help ensure that the RTCC operates within clear and enforceable limits, that its use remains transparent and accountable to the public, and that the City's approach to regulating surveillance keeps pace with evolving technology. These measures are essential to realizing the potential public safety benefits of the RTCC while protecting civil rights and civil liberties.

Appendix A: Auditing Questions

In contemplating the City expanding the surveillance infrastructure, what are the most protective policies, practices, and data governance safeguards that protect privacy, civil rights, and civil liberties?[197]

(1) What governance structures, written policies, and oversight mechanisms currently exist to manage the RTCC system, and how could they be improved to mitigate risk to privacy, civil liberty, civil and constitutional rights? This includes how policies are created, updated, enforced, and reviewed over time, and whether accountability is clearly assigned when policies are violated.

(2) What policies govern the lifecycle of RTCC data, including retention, level of access, deletion, and audit logging? Are the policies operationalized? Are there structural gaps between written policy and actual data management behavior? Does the current infrastructure make policy compliance verifiable and enforceable?

(3) The City's goal is for RTCC data to not be used for federal immigration enforcement, to criminalize those seeking reproductive or gender-affirming care, for SPD personnel to misuse data outside sanctioned law enforcement activities, or for state agencies to act contrary to Seattle's values. Do the current policy framework, contractual provisions, and technical infrastructure, including protections against disclosure through legal process or Public Records Act requests, adequately prevent these uses? Where gaps exist, what specific policy, contractual, or infrastructure changes are recommended?

(4) What policies and contractual provisions regulate whether and how state, county, federal, and fusion center partners access RTCC data or outputs, and are those access rules subject to equivalent restrictions as SPD's internal use? Is there evidence these policies are being followed? Does Seattle's current governance framework adequately address the risk of data protections eroding once data enters multi-jurisdictional sharing networks, and what policy or infrastructure controls should exist that currently do not?

(5) What specific civil rights and civil liberties risks does the RTCC pose particularly for marginalized communities and are current policies, oversight mechanisms, and contractual remedies sufficient to mitigate foreseeable harm? Do you have policy recommendations on how jurisdictions could remedy when harm occurs? This includes scenarios where federal or state authorities compel the vendor or the City to produce data, and an assessment of whether accountability is clearly assigned, accessible, and meaningful for impacted individuals.

(6) What policies and governance provisions regulate how vendor-introduced capabilities, including software updates, new integrations, and capability expansions, are reviewed and approved before deployment? Additionally, what policies govern the integration of privately-owned camera footage into the RTCC ecosystem, including retention, access, and civil liberties protections for data captured by private actors that enters a law enforcement data system? Are current policies and oversight structures adequate, or does vendor and private-actor dependency create governance gaps that policy alone cannot close?

Appendix B: Policing Project Evaluative Framework[198]

New technologies promise to make policing safer and more effective. But there is widespread concern about these technologies, including invasions of privacy, inaccuracy, and perpetuation of racial bias. Too often, adoption of new policing technology is debated as a matter of being "for" or "against" it. We believe the better approach is to figure out if society can benefit from a particular technology. Then, if there are benefits to be had, the question becomes whether it is possible to minimize or eliminate any harm. (Some harms, like constitutional violations, are impermissible in any degree.) We also believe it is essential that any decision to use technology has democratic legitimacy.

We evaluate policing technologies using this framework, which we apply in a flexible manner depending on the scenario under review:

Potential Benefits. Any analysis necessarily begins by asking about the assumed benefits of the technology. Particularly when use of a technology has attendant social (and hard) costs, it is important to identify the specific problem the technology is designed to address or solve, or the social improvement it is intended to bring. We do so in the following stages:

1. **Specify the Problem & the Benefit:**
   - What is the specific problem(s) the tech is intended to solve?
   - How important/what is the magnitude of the problem the tech is expected to solve?

2. **Evaluate Certainty of the Benefit:**
   - How certain is it that the technology will address the problem?
   - Have there been evaluations (either internal or external)?
   - Are there product performance concerns that might limit effectiveness?
   - If the tech succeeds in addressing the problem, will benefits be evenly distributed, or do they favor one segment of society over another?
   - What countermeasures might individuals take in response to the adoption of this tool, and how much would such countermeasures reduce the expected benefits?

3. **Evaluate Unintended or Secondary Benefits:**
   - Minimize criminalization of low-level offenses?
   - Additional control and protection of personal data?
   - Mitigation of racial and/or identity bias?

- Improved transparency or public trust?
- Better compliance with U.S. constitutional requirements?
- Other societal benefits?

Potential Costs. Only if a technology has identifiable, concrete benefits should one turn to considering potential costs, including attendant social costs. To facilitate this technology-specific evaluation, we evaluate a number of criteria that often arise in the case of new policing technologies.

4. **Transparency:**

    - **With the Public.** Do members of the public know about and/or consent to this information capture? Does the company itself make the public aware of where and how its product operates? How does the company's public description of its capabilities compare to actual capabilities? How does the company's public description of benefits compare with actual benefits? How open is the company in dealing with the public and media?

    - **Public Clients of Technology Companies**. How and to what extent are customers prevented, permitted, encouraged, or required to inform or engage with the public about the customer's decision to acquire or use the technology? To share information about the nature of the product or data it generates?

5. **Personal Information Privacy:**

    - **Data capture**. What information can or does the tech capture, measure, collect, or use? Is all of this data relevant and necessary to accomplish the purpose of the technology? From whom is this data collected?

    - **Data aggregation and mining**. Does the tech aggregate data and if so, how? Is the data stored in an anonymized fashion? Does the system analyze data to identify previously unknown facts or patterns (a.k.a. data mining)?

    - **Data retention**. Is data retained by the company or the customer? What are the guidelines/limits for doing so? How long is data retained? Can individuals request access to or deletion of their personal data?

    - **Data ownership and sharing**. Who owns the data collected? Who has access to that data? Does the company use any third-party data processors and for what purpose? Can customers share data with a third party? Does the company or the customer sell or otherwise monetize data?

- **Data control and security**. How/where is data stored? Is personally identifiable information separately stored and or encrypted? What are the physical, technical, and administrative protocols for data storage and access? Are there built-in audit trails to determine what type of data is collected and/or accessed by an end user? What are the protocols in place for a data breach? Will those whose data is acquired be notified? Is there risk of physical harm to individuals or locales in the event of a security breach?

- **Compliance**. How does the vendor monitor compliance with data policies?

6. **Racial or Other Identity Disparities:**

   - Disparities in design (e.g., whether the technology itself has any inherent bias, including algorithmic bias relating to personal identity, for example, by employing unrepresentative training data or exhibiting algorithmic bias)?

   - Disparities in operation (e.g., whether the technology might be deployed or used in ways that create or exacerbate identity bias and/or disparities)?

7. **Increased Criminalization:** Will use of the tech lead to more people being stopped, ticketed, arrested, or incarcerated? If so, for what type of crimes? Is enforcement of these crimes a net contribution to society or a net harm (i.e. are you contributing to low-level criminalization)?

8. **Evidentiary Risk:** Does the tech produce evidence to be used at trial? Under what circumstances? Does it meet chain-of-evidence, Daubert, and other rules of evidence? Are there protocols in place to ensure all necessary information is turned over to prosecutors and the defense?

9. **Constitutional Risk:** To the extent not already discussed, does use of the technology risk directly or indirectly violating constitutional rights, including but not limited to:
   - 1st Amendment (speech, press, religion, assembly, association, petition);
   - 2nd Amendment (right to bear arms);
   - 4th Amendment (searches, seizures, excessive force);
   - 5th Amendment (self-incrimination, Brady & impeachment evidence, due process);
   - 6th Amendment (right to counsel, speedy/public trial, cross-examine witnesses);
   - 8th Amendment (cruel & unusual punishment, excessive bail, excessive fines/fees);
   - 14th Amendment (equal protection)?

10. **Other Potential Social Costs:** Are there other potential social costs that have not yet been considered, including but not limited to:
    - Whether there might be a unique impact on any specific subgroup (e.g., youth, LGBTQ communities, particular religious groups, socioeconomically disadvantaged communities)?
    - Whether there are historical considerations that may make particular communities distrustful of this technology?
    - The potential for mission creep (either over time or in response to critical events)?
    - The impact of how others in the industry will respond?
    - Global/international human rights impact?

11. **Less Costly Technologies?** Once the social and other costs are identified, unless it is all benefit and no cost, there is one important last question: Are there alternative means of addressing the problem or providing the social benefit that are less costly, less-invasive, or avoid the costs identified here?

Operational Concerns. In addition to considering potential costs and benefits, there are several categories of operational concerns that one must always keep in mind when thinking through the potential impact of new policing technologies:

12. **Tactical Impact:** How will the product impact the performance of police officers? Will these changes create additional risks for officers or for the public?

13. **Integration Risks:** Can the tech freely integrate with other tech, and how might such integrations impact the risks discussed above? Can it be augmented with outside software (e.g., adding face recognition to CCTV or body-worn camera)?

14. **Intended Use vs. Actual Use:** Can the product be used differently than originally intended? Does this different downstream use present additional risks to consider? What are the vendor's terms-of-use and do they adequately limit how the tech can be used? Other than terms of use, what policies, procedures, or design features exist to limit, monitor, or audit downstream use or misuse?

15. **Internal Policies & Procedures:** Has the agency implemented a use policy? What internal policies and protocols are in place to ensure the product is used in the manner described above?

16. **Training:** What type of training do analysts, officers, and supervisors receive? Does the vendor provide ongoing training and/or support?

Appendix C: Surveillance Technology Governance & RTCC Oversight

This appendix provides an overview of Seattle's current surveillance technology governance system and additional RTCC-specific oversight. Table 1 describes the surveillance technology approval process mandated by the City's Surveillance Ordinance and the steps SPD and other entities took to comply with this process for the RTCC. Table 2 provides additional information about SPD policies and internal procedures that apply to the RTCC and CCTV programs.

A. Table 1: Surveillance Technology Approvals Process

Step	What the law requires	RTCC and CCTV
1. Surveillance determination	• An agency submits a "privacy and surveillance assessment" to Seattle IT, which examines whether it meets the Ordinance's definition of "surveillance."[199] • Technology that meets the definition and does not qualify for any exemption or exception requires a Surveillance Impact Report (SIR) that must be approved by City Council.[200] SMC 14.18.010, 14.18.020(B); POL-203 §§ 1–4	• SPD submitted its CCTV assessment in October 2023 and its RTCC assessment in November 2023.[201] • Seattle IT found that both systems qualified as surveillance technologies and required SPD to draft SIRs.[202]
2. Draft SIR	• An agency's SIR for a qualifying technology must: describe the technology, its purpose, proposed use, and fiscal impact; include a use and data management policy (deployment rules, storage, retention, access, sharing, and training); address community engagement and civil liberties and disparate impact considerations, along with a mitigation plan; and include a Racial Equity Toolkit.[203] SMC 14.18.040	• SPD produced draft SIRs for the CCTV and RTCC systems in early 2024, along with a SIR for an acoustic gunshot location system, which the Mayor later withdrew.[204]

Step	What the law requires	RTCC and CCTV
3. Public engagement	• Before seeking City Council approval, an agency must hold one or more community meetings with opportunity for public comment and written response. The SIR must compile all comments received and the agency's responses.[205] SMC 14.18.020(C), 14.18.040(B)(4)	• Public comment for the initial RTCC and CCTV SIRs opened in February 2024.[206] SPD engagement included two citywide meetings and 15 neighborhood meetings, yielding more than 1,000 public comments, most raising concerns about the impact of the technologies on civil rights and liberties.[207]
4. Independent review	• The Community Surveillance Working Group (CSWG) provides a privacy and civil liberties impact assessment for a SIR.[208] • The City's Chief Technology Officer (CTO) may respond in writing, and the Office of the Inspector General (OIG) may prepare an equity impact assessment for SPD technologies as well.[209] SMC 14.18.080(B), 14.18.020(G), 14.18.050(C)	• CSWG issued its assessment of the RTCC and CCTV systems in July 2024, identifying 12 major issues, including possible First and Fourth Amendment infringements and risk of disparate impact on minority communities. Of the six members who reviewed the SIRs, three were "against," two were "unstated, with broad concern," and one was "for CCTV within stated pilot, and for RTCC."[210] • The Community Police Commission (CPC) released an official statement in March 2024 that it did "not oppose a time-limited and location-limited surveillance pilot" to reduce gun violence, despite a number of civil rights concerns.[211] • The Office of Civil Rights issued an additional analysis recommending, among other things, limiting CCTV to serious violent offenses and barring private camera opt-in.[212]
5. Council approval	• City Council approves (or denies) the SIR by ordinance. If approved, the agency may then acquire and use the technology "only in accordance with the procedures and protocols set forth in the SIR," as well as any City Council amendments.[213]	• City Council approved the RTCC and CCTV SIRs on October 8, 2024, with amendments, including requiring reporting on evaluations and private camera integration, vendor warrant-notice terms, and limits on Public

Step	What the law requires	RTCC and CCTV
	SMC 14.18.020(A), (F)	Records Act disclosure of CCTV data.[214]
6. Changes – material and non-material	• Minor or "non-material" updates to an approved surveillance technology need only be noted in the SIR but do not require further City Council approval.[215] • Agencies must report "material changes" — "changes to the purpose or manner in which a surveillance technology may be used" — to Seattle IT and submit an updated SIR that must receive Council approval.[216] • The CTO may order an unreported change removed from service.[217]	• In August 2025, SPD submitted an updated RTCC SIR to allow RTCC access to SDOT traffic cameras and an updated CCTV SIR to add CCTV deployment in the Stadium District, the Capitol Hill Nightlife District, and around Garfield High School.[218] • City Council approved both updated SIRs in September 2025.[219] • The CCTV ordinance also created a 60-day pause on CCTV data collection if the City or its vendor receives a warrant, subpoena or court order for camera data in a civil immigration or protected health care matter.[220]
	SMC 14.18.020(F); POL-203 § 10	
7. Ongoing review and enforcement	• The CTO files an annual Surveillance Technology Community Equity Impact Assessment report that reviews whether surveillance technologies disproportionately affect any communities.[221] • OIG conducts an annual review of SPD's use of surveillance technology and compliance with approved SIRs.[222] • The CTO must direct a noncompliant department to cease use, and a person injured by a material violation may seek injunctive or declaratory relief after 90 days' written notice to the City.[223]	• The CTO's 2025 Assessment referenced the RTCC and CCTV programs, but concluded "not enough data exists" at the time to do an accurate analysis.[224] • The CTO's 2026 Assessment did not report findings on either program, but noted SPD's plans to manage performance measures, including disparate impact, and pointed to the forthcoming Penn audit results.[225] • OIG issued its first annual review of the RTCC and CCTV systems on September 30, 2026, finding that SPD "implemented appropriate policies and processes" for each but recommending additional guidelines for private camera integration and user auditing.[226]
	SMC 14.18.050–14.18.070	

B. Table 2: SPD Internal Rules, Access, and Accountability

In addition to the Surveillance Ordinance and the SIRs, the RTCC is governed by SPD's own internal policies, which can be found in its publicly available policy manual (linked here), as well as SPD standard operating procedures and RTCC user access limits. This section also describes the remedies available for misuse or abuse of the RTCC system.

SPD RTCC Policy and Procedures	
RTCC Policy (Policy 12.100)	Sets the basic rules for the RTCC. Includes provisions describing integrated technologies, provisions for community notice of technologies at use, rules for access, training, and data governance.[227]
Standard Operating Procedures (draft)	Drafted but not formalized at the time of our review. The draft covers basic steps in the RTCC's core workstreams: real-time response to calls, investigation support, and "response for operations," which covers event support.[228]

Other SPD Policies Relevant to RTCC	
12.050: Criminal Justice Information Systems	Requires that queries of criminal justice databases be made only for legitimate law enforcement purposes.[229]
6.060: Collection of Information for Law Enforcement Purposes	Restricts collecting information about a person's political or religious activities or sexual orientation, limits video recording of lawful demonstrations, and requires SPD's Criminal Intelligence Unit to purge any information collected in connection with a demonstration within five days unless longer retention is approved by a lieutenant.[230]
5.140: Bias-Free Policing	Requires that law enforcement decisions be based on observed behavior or specific intelligence rather than "discernible personal characteristics" such as age, disability status, gender identity, race or religion.[231]
7.010: Submitting Evidence; 7.090: Photographic Evidence	Governs how RTCC video clips and stills are preserved as evidence; establishes Evidence.com as SPD's storage platform for photo and video evidence.[232]
12.080: Disclosure of Department Records	Governs release of RTCC data in response to public records requests.[233]
5.002: Responsibilities of Employees Concerning Alleged Policy Violations	Governs how alleged policy violations are reported and investigated.[234]

Access Controls	
Who has access to RTCC systems	Limited to authorized employees of SPD, the Office of Police Accountability ("OPA"), OIG, Seattle IT, and the vendor.[235] In its recent audit, OIG observed that 31 accounts accessed the RTCC's software platform, Fusus, in 2025 and all accounts belonged to individuals who had an operational need to access the platform.[236]
Personnel requirements	All RTCC personnel undergo background checks.[237] All SPD employees are bound by SPD's Criminal Justice Information policy, which restricts sharing sensitive criminal justice information such as identity and biographic data and criminal history.[238]
System authentication	SPD's Fusus system administrator grants Fusus access through the City's single sign-on service, and access is limited to authorized personnel with login credentials.[239]

Data Sharing with External Entities	
Washington State Fusion Center	The Washington State Fusion Center employs personnel from local agencies including SPD. However, there is no interface between the Fusion Center and the RTCC; Fusion Center personnel, including SPD staff, cannot view RTCC feeds or access data outside of the channels for state and local law enforcement entities described below.[240]
Federal agencies	Federal requests for data must go through SPD's interagency portal or the PRA.[241] SPD directs all outside-agency requests for CCTV footage to the PRA process.[242] Requests identified as relating to civil immigration enforcement or protected health care are elevated to the Mayor's Office General Counsel. SPD reports it does not currently share RTCC data through any task forces.[243]
State and local policing agencies	State and county agency requests — including from agencies in Washington — must go through the interagency portal, subject to the same limitations as listed above for federal requests.[244] SPD reports it does not currently share RTCC data through any task forces.[245] No data from the RTCC is shared with external agencies via the regional LinX database.[246]
King County prosecutors, defense counsel, and courts	As with other investigative information, RTCC data may be shared with prosecutors, defense attorneys, and the courts in connection with criminal prosecutions or misconduct allegations.[247]
Any requester (PRA)	RTCC data may be shared with any individual under the state's Public Records Act subject to the provisions of that law. Agencies generally may not require a requestor to identify themselves or state a purpose for the request.[248] Disclosures are subject to various redactions, such as masking the identities of victims and witnesses in surveillance footage.[249]

Consequences for Misuse	
Written policy	The RTCC policy and the SIRs provide that "[p]ersonal or inappropriate use or dissemination of information can result in internal discipline, termination, or penalties under federal or state law."[250]
Internal RTCC practice	SPD personnel described a progressive discipline structure: a first violation results in additional training, a second in a reprimand, and a third in referral to OPA.[251]
Surveillance Ordinance	Failure to follow the restrictions in a SIR can result in suspension of a surveillance technology capability.[252]

Remedies for Impacted Individuals	
Misconduct complaint	An individual who believes the RTCC policy was violated may file a complaint with OPA.[253]
Lawsuit	A person surveilled and injured by a material violation of the Surveillance Ordinance may sue the City for equitable relief to stop or correct the violation, but not for money damages.[254]

Appendix D: Seattle RTCC Technology & Databases

This appendix provides additional information about the technologies and data sources available to SPD's RTCC at the time of our review.

A. Camera Systems

RTCC personnel can directly view feeds from four camera sources. They can also request recorded video footage from a fifth source — privately owned cameras that owners register with SPD — but these cameras are not integrated with the RTCC and therefore do not provide direct viewing access. The table below represents the status of camera footage accessible by the RTCC at the time of this audit.

Integrated Camera Source	Ownership & Authorization	Details	Privacy/Masking	Storage and Retention
1. **SPD CCTV cameras**	Owned and operated by SPD in 3 deployment areas approved by City Council in 2024.[255] 3 additional areas approved by Council, currently paused.[256]	303 cameras at 61 sites.[257] Each site contains a "cluster" of up to 5 cameras: 4 fixed and 1 pan-tilt-zoom.[258] Wireless; transmit data through cellular connection.[259] No audio recorded.[260]	Second-story windows and similar private areas are masked on the camera itself; masked areas appear pixelated or blacked out and cannot be unmasked later.[261]	Raw footage stored on city-owned hardware at each camera site and retained for 5 days.[262]
2. **SPD building security cameras**	Owned and operated by SPD.[263] Security cameras are exempt from the requirements of the Surveillance Ordinance.[264]	116 cameras at 9 SPD buildings: all precincts, Harbor Patrol, the K9 building, and the evidence building.[265]	Masking applied to footage that captures non-public areas (digital or physical, depending on camera features).[266]	Raw footage integrated into the RTCC retained for 5 days; external footage also stored on City servers outside the RTCC for 31 days.[267]

Integrated Camera Source	Ownership & Authorization	Details	Privacy/Masking	Storage and Retention
3. SDOT traffic cameras	Owned and operated by the Department of Transportation (SDOT). RTCC integration authorized by City Council in 2025.[268]	RTCC integrates a subset totaling 96 cameras.[269] Live feeds are publicly available online.[270] SDOT controls pan, tilt, and zoom; the RTCC may ask SDOT to move a camera by giving a CAD number and reason.[271]	No masking applied by SPD.[272] Lower-resolution cameras placed principally to monitor traffic.[273]	The RTCC keeps one day of footage, stored in Fusus.[274]
4. Connect Seattle integrated private cameras	Business-owned cameras streamed live to the RTCC through a fususCORE device.[275] Private camera integration is discussed in SIRs, though scope and scale are not articulated.[276] Businesses agree to Axon's Connect Seattle terms.[277]	3 locations have connected 23 cameras.[278] Single-family homes are not eligible.[279] SPD has purchased 100 fususCORE devices to give to businesses at its discretion; each can support several cameras.[280] No audio.[281]	Currently no masking by SPD.[282]	Storage and retention controlled by the business; SPD currently sets no minimum or maximum.[283]
Non-integrated Camera source	**Ownership & Authorization**	**Details**	**Privacy/Masking**	**Storage and Retention**
5. Connect Seattle registered private cameras (not integrated)	Registry maintained by SPD — no live access by RTCC.[284] Authorized as part of RTCC and CCTV programs by City	Includes 893 cameras at 159 locations.[286] Residents and businesses may register cameras with SPD.[287]	No masking (n/a). Sharing is voluntary; camera owners can refuse to share footage.[289]	Controlled by the camera owner.

Integrated Camera Source	Ownership & Authorization	Details	Privacy/Masking	Storage and Retention
	Council in 2024, with required report submitted to the Public Safety Committee in 2025.[285]	No live access. The registry shows camera locations and owner contact information; analysts can send owners a link to upload footage voluntarily. Access is limited to RTCC staff and technicians, as a matter of practice.[288]		

B. Fusus

The RTCC uses Axon's Fusus, a cloud-based software platform that enables personnel to view integrated technologies such as camera feeds, incident details, officer locations, and other information in one computer interface. Features SPD uses include:

Capability	Description
Map and dispatch integration	An interactive map of Seattle. When an incident is entered into Versaterm, SPD's Computer-Aided Dispatch (CAD) system, Fusus displays the incident's location on the map, together with nearby RTCC-connected cameras and the locations of patrol units.[290] Map layers show public geographic information, such as railroad lines and utility poles, and SPD has added floor plans for certain public buildings.[291]
Live camera viewing and playback	Personnel can select a camera on the map to view its live feed or rewind to review earlier footage, up to the camera's retention limit. They can display several cameras at once — for example, by drawing a shape around an area and arranging the selected feeds in a grid.[292]
Video clipping and storage	Personnel can clip relevant footage or stills, which are saved to FususVAULT, a cloud workspace hosted on Amazon Web Services, for 30 days. Clips are uploaded to Evidence.com, Axon's cloud-based digital evidence platform, once a case event number exists.[293] SPD staff told us that Evidence.com data currently is kept indefinitely, a practice that began under SPD's consent decree.[294]

Capability	Description
Object detection	Searches recorded video for 10 object types, including: person, car, bus, train, motorcycle, boat, bicycle, backpack, suitcase, and handbag.[295] Analysts report using it rarely because results are unreliable. Fusus does not currently log whether personnel use this feature.[296] A newer Axon "head-detection" feature (i.e., identifying and enabling the tracking of an individual's head in footage) has been left disabled.[297]

C. Databases

RTCC personnel have access to various databases managed by SPD and other government agencies, as well as commercial databases.[298] Only Mark43 and Versaterm are integrated into Fusus.[299] Databases include:

Database	Operator	Contents	Examples of RTCC use
Mark43	SPD	Records management system that includes all incident, arrest, and supplemental reports. It is searchable by person, vehicle, phone number, and other fields.[300]	Checking prior criminal history information; filing RTCC supplemental reports.[301]
Versaterm CAD	Seattle 911 center	Computer-aided dispatch records for calls for service.[302]	Monitoring calls; may also add information, such as photos, to a call record.[303]
Omnixx Force	Washington State Patrol	Department of Licensing data, principally driver's license photos.[304]	Finding a recent photo of a named suspect or verifying identity.[305]
DAPS (Driver and Plate Search)	WA State Department of Licensing	Vehicle and driver records, searchable by plate (including partial plates), Vehicle Identification Numbers, name, or vehicle description.[306]	Searching partial plates; connecting plates to residences; available on six of eight RTCC terminals.[307]

Database	Operator	Contents	Examples of RTCC use
Interstate Identification Index ("Triple I")	FBI	State and federal criminal history records.[308]	Accessing criminal history records from across the U.S.[309]
King County JMS	King County	Booking photos.[310]	Used when no license photo is available.[311]
Accurint	LexisNexis (commercial)	Addresses, phone numbers, relatives, and property ownership.[312]	Used to obtain contact information for someone. Rarely used; requires a report number and reason to log in.[313]
Law Enforcement Information Exchange ("LinX")	Regional law enforcement data-sharing network developed by the Naval Criminal Investigative Service ("NCIS"), a federal agency.	Incident and case records from participating agencies.[314]	Used to access case numbers or other case information from regional jurisdictions; typically used for non-emergency cases.[315] No data from the RTCC is shared with external agencies via LinX.[316]

Endnotes

[1] *E.g.,* MEGHAN CAMELLO ET AL., NAT'L INST. OF JUST. CRIM. JUST. TECH. TESTING & EVALUATION CTR., REAL-TIME CRIME CENTERS: INTEGRATING TECHNOLOGY TO ENHANCE PUBLIC SAFETY 1–2 (2025).

[2] *See id.,* at 1–3 (discussing potential value RTCCs can provide, including helping agencies "face challenges with siloed data").

[3] *See generally* Alex Billmeier et al., *Evolving Technologies in Law Enforcement: Documenting the Continued Growth of Real-Time Crime Centers*, POLICE J.: THEORY, PRACTICE & PRINCIPLES (Mar. 21, 2026) (conducting a national survey of real-time crime centers and finding that RTCC use of CCTV and ALPR cameras was "nearly universal"*); see also* Kimberly Przeszlowski, *Real-Time Crime Centers Are Transforming Policing — A Criminologist Explains How These Advanced Surveillance Systems Work*, THE CONVERSATION (Aug. 2024), https://theconversation.com/real-time-crime-centers-are-transforming-policing-a-criminologist-explains-how-these-advanced-surveillance-systems-work-232468 ("Real-time crime centers often focus on video surveillance, using closed-circuit television systems, license plate scanners, body cameras worn by officers and drone cameras."); Rachael Arietti, *Do Real-Time Crime Centers Improve Case Clearance? An Examination of Chicago's Strategic Decision Support Centers*, 90 J. CRIM. JUST. 1, 102145 (2024) (RTCCs centralize data, "often including CCTV, automated license plate readers, gunshot detection technology, and intelligence databases").

[4] *E.g.,* Philip Lukens, *An Introduction to How AI Is Transforming Real Time Crime Centers*, POLICE1 (Mar. 11, 2024), https://www.police1.com/tech-pulse/an-introduction-to-how-ai-is-transforming-real-time-crime-centers.

[5] *See* Camello, *supra* note 1, at 3 (listing potential RTCC public safety benefits, including "facilitating operational efficacy" by enhancing data sharing across information sources and technologies and "supporting investigations" by enabling officers to connect different evidence streams).

[6] *See, e.g.*, Rob T. Guerette & Kimberly Przeszlowski, *Does the Rapid Deployment of Information to Police Improve Crime Solvability? A Quasi-Experimental Impact Evaluation of Real-Time Crime Center (RTCC) Technologies on Violent Crime Incident Outcomes*, 40 JUST. Q. 950, 962 (2023) (finding that RTCC-assisted violent crime cases had 66% better odds of being cleared, but that there was no impact on clearance times); Arietti, *supra* note 3, at 6 (finding that RTCC involvement in Chicago was "associated with modest increases in case clearance").

[7] *See* Camello *supra* note 1, at 3.

[8] *See, e.g.*, Camello, *supra* note 1, at 4 (observing that "there is limited research in assessing RTCCs as a whole on criminal justice outcomes"); Arietti, *supra* note 3, at 1 ("Despite the rapid diffusion of RTCCs across the U.S., few formal evaluations have been done to assess their impact on criminal justice."); Kimberly Przeszlowski et al., *The Centralization and Rapid Deployment of Police Agency Information Technologies: An Appraisal of Real-Time Crime Centers in the U.S.*, 96 POLICE J.: THEORY, PRACTICE & PRINCIPLES 553, 566 (June 15, 2022) (in a national survey of RTCCs, surveyed agencies were asked to provide information on "all applicable measures" of RTCC effectiveness due to a "dearth of empirical research on real-time crime center efficacy" but "less than half of the sample surveyed employed measures to track common outcomes"). As discussed *infra* Part III, there is a more robust literature evaluating the public safety impacts of CCTV cameras on their own, not connected to an RTCC, though that literature is inconsistent in its conclusions.

[9] *Cf*. Andrew Guthrie Ferguson, *Real-Time Crime Centers and the Brady Puzzle,* 106 B.U. L. Rev. at 6 (forthcoming 2026, manuscript at 6) (arguing that by centralizing and aggregating data collection in combination with AI analytics, RTCCs give police a "virtual time machine to go back and investigate crimes" and "offer completely new capabilities which police have never possessed before").

[10] *See* Camello, *supra* note 1, at 1, 20–21 (discussing concerns raised by RTCCs, ranging from privacy and data security concerns to accountability and oversight concerns).

[11] *See* Amy Sundberg, *Recent SPD Surveillance Audits Highlight Overreach, Vulnerabilities,* Urbanist (Oct. 7, 2026), https://www.theurbanist.org/recent-spd-surveillance-audits-highlight-overreach-vulnerabilities (describing the RTCC's launch in May 2025). SPD operated an earlier, unrelated unit also called the "Real Time Crime Center" beginning in 2015. *See SPD Announces Agile Policing Strategy, Unveils Real-Time Crime Center*, SPD Blotter (Oct. 7, 2015), https://spdblotter.seattle.gov/2015/10/07/spd-announces-agile-policing-strategy-unveils-real-time-crime-center. For example, as discussed *infra* Part I.A.*,* Seattle's RTCC currently integrates CCTV cameras but not ALPRs or drones, which are commonly used in other RTCCS. *See generally* Billmeier, *supra* note 3 (surveying RTCCs across the country and describing the variety of technologies used by these units, including cameras, ALPRs, drones, and gunshot detection).

[12] *See* Agreement No. IG2025-03 between the City of Seattle, Office of Inspector General for Public Safety, and the Trustees of the University of Pennsylvania (on file with author) [*hereinafter* Agreement No. IG2025-03]. The evaluation is being conducted by the University of Pennsylvania's Crime and Justice Policy Lab on behalf of OIG. *See infra* Part III.B.

[13] *See generally* Barry Friedman, *The Constitutionality of Indiscriminate Data Surveillance,* 174 U. Penn. L. Rev. 293 (2026).

[14] *See, e.g.*, Sadie Gurman & Eric Tucker*, AP: Across US, Police Officers Abuse Confidential Databases*, Associated Press (Sept. 28, 2016), https://apnews.com/general-news-699236946e3140659fff8a2362e16f43 (documenting hundreds of instances in which officers misused law enforcement databases to look up romantic partners, journalists, and others for personal reasons); Joseph Cox & Jason Koebler, *A Texas Cop Searched License Plate Cameras Nationwide for a Woman Who Got an Abortion*, 404 Media (May 29, 2025), https://www.404media.co/a-texas-cop-searched-license-plate-cameras-nationwide-for-a-woman-who-got-an-abortion (revealing that a Texas officer conducted a nationwide search of more than 83,000 Flock cameras, including cameras in states like Washington where abortion is legal); *Leaving the Door Wide Open: Flock Surveillance Systems Expose Washington Data to Immigration Enforcement*, Univ. of Wash. Ctr. for Hum. Rts. (Oct. 21, 2025), https://jsis.washington.edu/humanrights/2025/10/21/leaving-the-door-wide-open (finding that at least eight Washington agencies enabled direct sharing of license plate reader data with U.S. Border Patrol in 2025).

[15] *See, e.g.*, Seattle Police Dep't Manual § 12.100-POL-4(3)–(4) (eff. Mar. 1, 2026) [*hereinafter* SPD Policy 12.100]; *see also* Wash. Rev. Code §§ 10.93.160, 7.115.020 (2024) (placing restrictions on agencies collecting, sharing, or using information relating to immigration or citizenship status or protected health care services, respectively).

[16] *See* Camello et al.*, supra* note 1, at 3, 5; *see also generally* SPD Policy 12.100, *supra* note 15 (describing RTCC role as both "assisting with calls for service" and supporting "ongoing investigations").

[17] *See* Seattle Police Dep't, 2025 Surveillance Impact Report: Real-Time Crime Ctr. 5 (2025) (material update adding integration of SDOT traffic-monitoring cameras) [*hereinafter* 2025 RTCC SIR]; Seattle

Police Dep't, 2025 Surveillance Impact Report: Closed-Circuit Television Camera Sys. 10–11 (2025) [*hereinafter* 2025 CCTV SIR] (material update adding CCTV deployment areas in the Stadium District, the area surrounding Garfield High School, and the Capitol Hill Nightlife District). The RTCC can integrate privately-owned cameras through SPD's Connect Seattle Program. *See, infra* Part I.A. The City Council also authorized SPD to use StarChase, a GPS tracker launched from a patrol car onto a fleeing vehicle. *See* Seattle, Wash., Ordinance127236 (2025).

[18] Seattle, Wash., Mun. Code § 14.18.020(F) (2025) [*hereinafter* SMC].

[19] *See, e.g.,* Thomas Brewster, *How a Former Palantir Exec Built a Google-Like Surveillance Tool for the Police*, Forbes (Aug. 13, 2024), https://www.forbes.com/sites/thomasbrewster/2024/08/13/how-a-former-palantir-exec-built-a-google-like-surveillance-tool-for-the-police (describing Peregrine, a platform used by some policing agencies that lets officers "quickly scan[] court records, arrest reports," and other datasets, taking "data siloed across an array of older, slower systems, and ma[king] it accessible in a simple, speedy app"). SPD does not use Peregrine.

[20] *See, e.g.*, *San Francisco Police Department Real-Time Investigation Center (RTIC) Assists in Over 500 Arrests, Historic Crime Drop*, San Francisco Police Dep't (Apr. 9, 2025), https://www.sanfranciscopolice.org/news/san-francisco-police-department-real-time-investigation ("Officers can identify and follow suspect vehicles from a distance with drones and ALPR alerts."); *LPR and Drone Technology Leads Officers to Multiple Arrests*, Fairfax Cnty. Police Dep't News (Sept. 4, 2026), https://fcpdnews.org/2026/09/04/lpr-and-drone-technology-leads-officers-to-multiple-arrests (after a license plate reader alert, "[t]he Real Time Crime Center (RTCC) launched a Drone as First Responder (DFR) to track the vehicle from above"); *Aerodome and Flock Safety Forge Strategic Partnership to Expand Drone-as-First-Responder Technology for Public Safety Agencies*, Flock Safety (July 24, 2024), https://www.flocksafety.com/blog/aerodome-and-flock-safety-forge-strategic-partnership-to-expand-drone-as-first-responder-technology-for-public-safety-agencies (describing drones dispatched automatically when Flock license plate readers detect a flagged vehicle).

[21] *See* Seattle Police Dep't, Responses to Policing Project Follow-Up Questions, (Oct. 14, 2026) (on file with author) [*hereinafter* SPD Oct. 14 Responses].

[22] Policing Project Interview with Seattle Police Dep't Personnel (May 27, 2026) (on file with author).

[23] *See* SPD Oct. 14 Responses, *supra* note 21.

[24] *See Connect Seattle*, Seattle Police Dep't, https://communityconnectseattle.org (last visited Oct. 14, 2026).

[25] *See id*.

[26] *See* SPD Oct. 14 Responses, *supra* note 21.

[27] *See id.* ("SPD has 100 cores to allocate to businesses. At the time of w[ri]ting, [n]o decision has been made on how these will be distributed.").

[28] *See* Axon, Statement of Work for the Implementation of Axon Fusus for Seattle Police Department [*hereinafter* SOW] (on file with author) (Fusus "provid[es] a platform to view public and community video sources for incident situational awareness and investigations").

[29] *See generally id.*; *see also Single Pane of Glass*, Axon, https://www.axon.com/products/axon-fusus/single-pane-of-glass-technology-integration (last visited Nov. 4, 2026).

[30] *See* Seattle Police Dep't Responses to Policing Project Follow-Up Questions (Aug. 25, 2026) (on file with author) [*hereinafter* SPD Aug. 25 Responses] (listing the databases RTCC analysts can access as "MARK43 (RMS), OMNIXX, DAPS, Accurint, LINX, CRIMES, CARFAX, Versaterm (CAD)").

[31] *Id.; see* SPD Policy 12.100, at § 12.100-5(2) (requiring RTCC personnel to document their work "in an RTCC report in Mark43," the department's "records management system").

[32] *See* Policing Project Interviews with Seattle Police Dep't Personnel (May 27, 2026) (on file with author) (Omnixx Force "provides DMV data, photos mainly" and is managed by the State Patrol; Accurint, a LexisNexis product, is used "to get addresses or phone numbers" and "[c]an show relationships (family) and property ownership"); Policing Project Interviews with Seattle Police Dep't Personnel (May 26–28, 2026) (on file with author) (noting analysts' handling of "Triple I (Interstate Identification Index)" data); *see generally* DATAMAXX, OMNIXX FORCE USER MANUAL VERSION 2.2 (Apr. 28, 2023) (describing Omnixx Force); 34 U.S.C. § 40316 (defining the Interstate Identification Index System); *Accurint for Law Enforcement*, LEXISNEXIS, https://risk.lexisnexis.com/products/accurint-for-law-enforcement (last visited Nov. 4, 2026) (describing Accurint).

[33] *See* Policing Project Interview with Seattle Police Dep't Personnel (May 26, 2026) (on file with author) (RTCC personnel estimating that patrol support accounts for 80–85% of their work). When reporting on RTCC activities, however, SPD does not distinguish between real-time and investigative support, making an exact breakdown hard to quantify. SPD noted that ultimately, everything RTCC does eventually supports investigations." *See* SPD Aug. 25 Responses, *supra* note 30, at Q10.a.iv.

[34] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 33 ("It starts with a CAD call, 911 enters a ticket or event. CAD calls appear on the map."); Policing Project Interview with CARE Department Dispatch Staff (May 26, 2026) (on file with author) (RTCC and dispatch "have same access to same CAD.").

[35] See SPD Policy 12.100, at § 12.100-POL-3(3) ("RTCC personnel will monitor calls for service."); SPD Aug. 25 Responses, *supra* note 30 ("RTCC staff react to CAD Calls for service.... [M]any times the RTCC personnel are working on calls prior to patrol being dispatched.").

[36] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 33 ("Much of the work is radio focused; communication with patrol."); DRAFT RTCC PROCEDURE§ 12.100-PRO-1(2)–(3) (Jan. 21, 2026) (on file with author) (directing analysts to "[n]otify over the air" and "[u]pdate pertinent information over the radio and to CAD").

[37] *See* Policing Project Interview with Seattle Police Dep't Personnel (May 27, 2026) (on file with author).

[38] SPD Policy 12.100, at § 12.100-POL-1(1); Policing Project Interview with Seattle Police Dep't Personnel (Sept. 28, 2026) (on file with author); Policing Project Interview with City of Seattle Staff (Sept. 29, 2026) (on file with author).

[39] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 38 (SPD personnel explained that the RTCC supports "all calls for service" but "prioritize[s] by level," with "[m]ost serious crimes ... first and then if time we move down the list"; SPD's civilian RTCC lead adding that analysts "will reach out and handle these low-level ones when time permits"). For more information on CAD call priorities, *see*, Jonah Spangenthal-Lee*, Your Guide to Calling 9-1-1 in Seattle*, SEATTLE CARE DEP'T (Oct. 8, 2025), https://withcare.seattle.gov/2025/10/08/your-guide-to-calling-9-1-1-in-seattle.

[40] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 33 ("CAD calls appear on the map"; analyst "assigns themself to call and looks to see if cams are available"); Seattle Police Dep't Response to Policing Project (Oct. 27, 2026) (on file with author).

[41] *See* Policing Project Interview with Seattle Police Dep't Personnel (May 27, 2026) (on file with author) (with map layers, drawing tools, and registry cameras displayed on a map); *see also Map Interaction & Navigation*, AXON (July 28, 2026), https://www.axon.com/help/fusus/software/fusus/map.htm, (describing video livestreaming features supported by Fusus).

[42] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 33 ("Then they grab a camera, and back up the footage to see if they can see the crime"); Policing Project Interview with Seattle Police Dep't Personnel *supra* note 41 ("Scrubber at bottom allows you to go forward/back over the 5-day retention"; "Can set up cameras in grid mode"); *see also Live Video, Playback & Clips*, AXON (July 28, 2026), https://www.axon.com/help/fusus/software/fusus/camera-operations.htm.

[43] Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 33. This capability was authorized by the City Council's approval of the program's SIRs. SEATTLE POLICE DEP'T, 2024 SURVEILLANCE IMPACT REPORT: REAL-TIME CRIME CENTER 7 (2024) [*hereinafter* 2024 RTCC SIR] (describing 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").

[44] *See* SPD Aug. 25 Responses, *supra* note 30; Policing Project Interviews with Seattle Police Dep't Personnel (May 26–27, 2026) (on file with author).

[45] *See* Policing Project Interviews with Seattle Police Dep't Personnel (May 26–27, 2026) (on file with author).

[46] *See* Policing Project Interviews with Seattle Police Dep't Personnel (May 26–28, 2026) (on file with author).

[47] *See* Policing Project Interviews with Seattle Police Dep't Personnel, *supra* note 37.

[48] *See* SPD Aug. 25 Responses, *supra* note 30 ("The FususVault is a workspace and intended to be a temporary repository for videos. Video and stills are stored in FususVAULT for every piece of work that is completed. The video and stills are kept for 30 days."); Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 37.

[49] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 37 ("Evidence.com data is forever").

[50] DRAFT RTCC PROCEDURE § 12.100-PRO-2 ("Document actions taken by completing an RTCC supplemental report in the RMS system under the original GO [general offense] or Event Number.").

[51] *See id.*

[52] *See* SPD Aug. 25 Responses, *supra* note 30; DRAFT RTCC PROCEDURE § 12.100-PRO-2. *See also* 2025 RTCC SIR, *supra* note 17, at 13; 2025 CCTV SIR, *supra* note 17, at 12 (data "may only be viewed or extracted for legitimate law enforcement purposes").

[53] *See* DRAFT RTCC PROCEDURE § 12.100-PRO-2.

[54] *See* Policing Project Interviews with Seattle Police Dep't Personnel, *supra* note 45.

[55] *See Residential Camera Registry,* SEATTLE POLICE DEP'T, https://communityconnectseattle.org/camera-registration (last visited Nov. 4, 2026).

[56] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 37. RTCC personnel are not involved in this step. *See* Seattle Police Dep't Responses to Follow-Up Questions (Oct. 22,

2026) (on file with author) [*hereinafter* SPD Oct. 22 Responses] ("We currently do not have RTCC staff do this request. This would … come directly from the detective themselves, or have the Video Unit make this request[] as they do this type of knock and talk request already.").

[57] *See* SPD Aug. 25 Responses, *supra* note 30.

[58] *See* DRAFT RTCC PROCEDURE § 12.100-PRO-2(4) ("Document actions taken by completing an RTCC supplemental report in the RMS system under the original GO or Event Number.").

[59] *See* SMC §§ 14.18.020(A), (B)(1), 14.18.040. *See* Appendix C for more details.

[60] *See* SMC § 14.18.040.

[61] *See* SMC §§ 14.18.020(C), 14.18.080(B).

[62] *See* SMC § 14.18.020(F) ("Following Council approval of the acquisition and the terms of the SIR, the department may acquire and use the approved surveillance technology only in accordance with the procedures and protocols set forth in the SIR."); *see, e.g.,* SEATTLE, WASH., Ordinance 127297 (Sept. 22, 2025) (adopting the 2025 CCTV SIR pursuant to various amendments).

[63] *See* SMC § 14.18.020(F)

[64] *See* SPD Policy 12.100, at § 12.100, *supra* note 15.

[65] *See generally* DRAFT RTCC PROCEDURE § 12.100, *supra* note 36.

[66] *See*, *e.g.,* SPD Aug. 25 Responses, *supra* note 30, at Q2.b (no formal agreement that new Fusus features be disabled by default), Q5.a (no written policy governing access to the camera registry), Q6.b (five-day retention period decided internally by SPD RTCC management); *see generally* DRAFT RTCC PROCEDURE, *supra* note 36.

[67] *See* SEATTLE, WASH., Ordinance 125315 (2017) (Seattle's Police Accountability Ordinance); SMC § 14.18.060. The CPC predates this ordinance, having been created under the 2012 Memorandum of Understanding (MOU) between the City and the U.S. Department of Justice. It was made permanent and independent by Ord. 125315 (2017). *See* Memorandum of Understanding between the United States and the City of Seattle (July 27, 2012) (establishing the CPC and describing its duties).

[68] *See* SMC §§ 14.18.050(A), 14.18.070(A).

[69] *See* SPD Policy 12.100, at § 12.100, *supra* note 15.

[70] *See* SPD Aug. 25 Responses, *supra* note 30 (explaining that although "CCTV monitoring was discussed" at the outset, SPD "did not have the staffing required to be patrol forward," which "morphed into the current policy of not monitoring cameras unless there was a call for service (via 911 or officer/command staff 'on-view' or initiation)"); Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 37.

[71] *See* 2025 RTCC SIR, *supra* note 17 at 4, 7–8; 2025 CCTV SIR, *supra* note 17 at 6–7; SPD Policy 12.100, at § 12.100, *supra* note 15.

[72] *See* SEATTLE POLICE DEP'T POL'Y MANUAL § 12.100.

[73] *See id*.

[74] SPD personnel told us the decision to retain CCTV footage for five days was based on an assessment of privacy concerns and feedback from investigations and RTCC staff, reflecting "the most common period in which a major crime investigator would make a request for camera footage." *See* SPD Aug. 25 Responses, *supra* note 30; *see also* SPD Policy 12.100, at § 12.100-POL-1(1) ("CCTV camera footage is authorized up to a 30-day retention period (actual retention periods may be

shorter due to operational needs/privacy interests but will not exceed 30 days)."); 2025 CCTV SIR, *supra* note 17, at 7.

[75] *See* SOW, *supra* note 28 § 1(i); *Data Visualization,* AXON, https://www.axon.com/products/axon-fusus/analytics-and-data-visualization (last visited Oct. 30, 2026) (describing Fusus data visualization capabilities as including "mapping data into defined objects, discovering relationships between people, events, trends, and other variables).

[76] *See* SPD Aug 25 Responses, *supra* note 30, at Q2.b; Policing Project Interviews with Seattle Police Dep't Personnel (May 26–28, 2026) (on file with author).

[77] Email from Nick Zajchowski, SPD, to Policing Project (Mar. 20, 2026) (on file with author).

[78] *See Mayor Wilson Announces Next Steps on Surveillance Pilot Project,* SEATTLE OFF. OF THE MAYOR (Mar. 19, 2026), https://wilson.seattle.gov/2026/03/19/mayor-wilson-announces-next-steps-on-surveillance-pilot-project; S.B. 6002, § 3(4)(a), 69th Leg., Reg. Sess. (Wash. 2026) (enacted as ch. 239, 2026 Wash. Sess. Laws).

[79] Policing Project Interview with Seattle Dep't Personnel, *supra* note 33; *see also* SEATTLE OFF. OF THE MAYOR, *supra* note 78.

[80] *See, e.g.,* 2025 RTCC SIR, *supra* note 17, at 3–4.

[81] Letter from Mayor Bruce Harrell to City Council Members (Sept. 12, 2024), at 1; *see also* Briefing Memorandum from Tim Burgess, Deputy Mayor & Kerry Keefe, Mayor's Off. Dir. of Pub. Safety to City Council Members (Oct. 6, 2023), at 1.

[82] 2025 RTCC SIR, *supra* note 17, at 5; *accord* 2024 RTCC SIR, at 4–5.

[83] *See* Policing Project Interview with Seattle Police Dep't Personnel (May 28, 2026) (on file with author).

[84] *See id.*

[85] *See, e.g.,* Arietti, *supra* note 3, at 1 (examining whether RTCCs improve rates of case clearance for violent, property, and overall crime in Chicago and observing that "few formal evaluations have been done to assess their impact on criminal justice outcomes"); Przeszlowski, *supra* note 8, at 566 (conducting a national appraisal of the nature of real-time crime centers by surveying 44 local police agencies housing these units and noting a "dearth of empirical research on real-time crime center efficacy").

[86] *See, e.g.,* Young-An Kim & James C. Wo, *A Spatial Examination of the Presence of CCTV Cameras and Neighborhood Crime,* AM. J. CRIM. JUST. (2026) (finding that associations between camera placement and reductions in violent and property crime "is not uniform but is instead contingent on neighborhood characteristics" — with reductions in violent crime being weaker, and reductions in property crimes negligible, in high-poverty neighborhoods); Eric L. Piza et al., *CCTV Surveillance for Crime Prevention: A 40-Year Systematic Review with Meta-Analysis*, 18 CRIMINOLOGY & PUB. POL'Y 135, 143–44, 148 (2019) (finding an overall 13% crime reduction associated with CCTV, with the largest impacts on crime in parking lots but only small, statistically insignificant effects on violent crime and in studies of U.S.-based camera systems).

[87] *See* Seattle Police Dep't, *New Analysis: RTCC Triples the Odds That a Victim Receives Justice*, SPD BLOTTER (Mar. 5, 2026), https://spdblotter.seattle.gov/2026/03/05/new-analysis-rtcc-triples-the-odds-that-a-victim-receives-justice. In August 2026, KOMO quoted former deputy mayor Tim Burgess saying cases were "nearly three times as likely" to result in an arrest. Chris Daniels, *Seattle Event Groups Urge Mayor Wilson to Reactivate CCTV Cameras After Deadly Shooting*, KOMO NEWS

(Aug. 3, 2026), https://komonews.com/news/local/seattle-event-groups-urge-mayor-wilson-to-reactivate-cctv-cameras-after-deadly-shooting-state-ballpark-public-facilities-chihuly-garden-glass-large-crowds-ceo-harvest-music.

[88] *See* Aaron Granillo, *Seattle's Real Time Crime Center Triples Arrest Odds, According to Police Review*, MyNorthwest (Mar. 5, 2026), https://mynorthwest.com/crime-blotter/seattle-crime-center-arrest/4212713.

[89] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 32.

[90] *See* Agreement No. IG2025-03, *supra* note 12, at 3 (on file with author). This evaluation was required as part of the City Council's approval of the CCTV and RTCC SIRs. *See* Seattle, Wash. Ordinance 127111, pmbl. & § 2 (Oct. 8, 2024) (RTCC); Seattle, Wash. Ordinance 127110, Preamble, § 2 (Oct. 8, 2024).

[91] *See* Agreement No. IG2025-03, *supra* note 12, at 3–4.

[92] *See id.*

[93] *See id.* at 3–5.

[94] *See* Dan Griffin, *Seattle CCTV Audit Decision Potentially Delayed After "Miscommunication,"* Fox13 Seattle (Sept. 29, 2026), https://www.fox13seattle.com/news/seattle-cctv-audit-delayed.

[95] *See, e.g.,* State v. Chrisman, 676 P.2d 419, 423 (Wash. 1984) (articulating a difference between the state and federal "plain view" rule under the Fourth Amendment).

[96] *See* SMC § 14.18.020 (requiring City Council approval by ordinance before a department acquires surveillance technology).

[97] U.S. Const. amend. IV.

[98] *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34–35 (2001) (holding that use of a thermal imaging device to identify high-intensity lamps inside a home constituted a search); United States v. Jones, 565 U.S. 400, 404 (2012) (holding that attaching a GPS tracker to a vehicle constitutes a search).

[99] *See* Riley v. California, 573 U.S. 373, 382 (2014).

[100] *See* Kentucky v. King, 563 U.S. 452, 460 (2011).

[101] *See* Carpenter v. United States, 585 U.S. 296, 312 (2018).

[102] *See id.*

[103] *See* Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

[104] *See* United States v. Tuggle, 4 F.4th 505, 529 (7th Cir. 2021); United States v. Houston, 813 F.3d 282, 287–88 (6th Cir. 2016); United States v. Bucci, 582 F.3d 108, 116 (1st Cir. 2009). *But see* United States v. Cuevas-Sanchez, 821 F.2d 248, 251 (5th Cir. 1987).

[105] *Compare* United States v. Knotts, 460 U.S. 276, 285 (1983), *with* United States v. Jones, 565 U.S. 400, 404 (tracking via GPS), Carpenter v. United States, 585 U.S. 296, 313 (2018) (tracking via cell site location information), *and* Chatrie v. United States, 609 U.S. 605, 611 (2026) (tracking via Google location history data).

[106] *See* Carpenter v. United States, 585 U.S. at 311 (2018).

[107] Seattle, Wash., Ordinance 127297 (Sept. 22, 2025); Seattle, Wash., Ordinance 127111 (Oct. 8, 2024).

[108] *See* Brinegar v. United States, 338 U.S. 160, 175–76 (1949) (stating that the probable cause requirement serves "to safeguard citizens from rash and unreasonable interferences with privacy and from unfounded charges of crime").

[109] *See* Johnson v. United States, 333 U.S. 10, 14 (1948) (stating that the decision whether to permit a search must be made by "a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime").

[110] *See* Michigan v. Tyler, 436 U.S. 499, 509 (1978).

[111] *See* Riley v. California, 573 U.S. 373, 386 (2014).

[112] *See* United States v. Mitchell, 652 F.3d 387, 407 (3d Cir. 2011) (en banc) (characterizing DNA sequencing as a "second search" after the initial search of collection); United States v. Ganias, 755 F.3d 125, 137–41 (2d Cir. 2014) (indefinite retention of hard drive data beyond the scope of a warrant authorizing seizure of the data violated the Fourth Amendment); 26 U.S.C. § 6103(i)(1) (requiring court order for disclosure of tax information for use in criminal investigations).

[113] *See generally* S. Rep. No. 94-755, Book II (1976) (Church Committee report); *see, e.g.,* Minn. Dep't of Hum. Rts., Investigation into the City of Minneapolis and the Minneapolis Police Department 35–37, (Apr. 27, 2022) (finding that MPD officers used covert social media accounts to monitor Black individuals and organizations unconnected to any criminal investigation).

[114] *See* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms."); NAACP v. Alabama ex rel. Patterson, 357 U.S. 449, 462 (1958) (recognizing the "vital relationship between freedom to associate and privacy in one's associations" and that exposure may "induce members to withdraw . . . and dissuade others from joining").

[115] *See* SPD Policy 12.100, at § 12.100-POL-4(3) ("All information must be gathered and recorded in a manner consistent with manual section 6.060 – Collection of Information for Law Enforcement Purposes.").

[116] *See id.*; Seattle Police Dep't Manual § 6.060-POL-3(3) (rev. May 1, 2025) [*hereinafter* SPD Policy 6.060].

[117] *See* Wash. Rev. Code § 43.17.425 (2024) (prohibiting state agencies from using assets to assist in immigration enforcement); Wash. Rev. Code § 10.93.160 (2024) (restricting state and local law enforcement agencies from providing certain information to federal immigration authorities); Wash. Rev. Code § 7.115.020 (2023) (prohibiting officials from cooperating with efforts by any out-of-state agency to enforce laws restricting certain health care services, including gender-affirming and reproductive health care). *See* SMC § 4.18.016 (2026) ("No City officer or employee shall provide any nonpublicly available personal information about any person to any non-City employee or non-City officer for use in the enforcement of civil immigration laws" without consent or unless required by law or court order).

[118] *See* Wash. Rev. Code § 42.56.070(1) (2026) (agencies "shall make available for public inspection and copying all public records," unless the record falls within a specific exemption). The PRA is to be "liberally construed and its exemptions narrowly construed." *Id.* § 42.56.030.

[119] Email from SPD personnel (Nov. 4, 2026) (on file with author) [hereinafter Nov. 4 SPD Email] ("all requests from outside agencies for CCTV footage go through the PDR Unit"); Policing Project Interview with Seattle Police Dep't Off. of Gen. Couns. (June 10, 2026) (on file with author) [hereinafter OGC Interview] (government agency requests for CCTV data are forwarded for "normal public disclosure process with redactions"). Outside agencies may also be able to request other SPD records, such as reports documenting RTCC analysts' work, through SPD's interagency data request portal. *See* OGC Interview, *supra*.

[120] Mayor's Office Policy: Review of Sensitive Requests for SPD Data §§ 1–2 (v.10.3.2026) (on file with author) [hereinafter Mayor's Office Policy].

[121] *Id.* §§ 1–2.

[122] *Id.* §§ 3–4.

[123] Seattle, Wash., Ordinance 127297, § 3 (Sept. 22, 2025) (requiring a 60-day pause in CCTV use if the City or its vendors receive a warrant, subpoena, or court order, or are otherwise required by law, to release data for use in federal civil immigration enforcement), amended by Seattle, Wash., Ordinance 127412, § 2 (Apr. 6, 2026); *see* Mayor's Office Policy, *supra* note 120, at 1 & § 5.

[124] The PRA provides that agencies "shall not distinguish among persons requesting records, and such persons shall not be required to provide information as to the purpose for the request," except to establish whether disclosure would violate certain specified provisions or an "other statute which exempts or prohibits disclosure of specific information or records to certain persons." WASH. REV. CODE § 42.56.080(2). It is not clear that Washington's shield law or the Keep Washington Working Act is such a statute. *See infra* note 125.

[125] *See* WASH. REV. CODE § 42.56.030 (PRA "shall be liberally construed and its exemptions narrowly construed," and "[i]n the event of conflict between the provisions of this chapter and any other act, the provisions of this chapter shall govern."). Given the text of Washington's shield law, WASH. REV. CODE § 7.115.020, and the Keep Washington Working Act, WASH. REV. CODE § 10.93.160, it is not clear that either would provide a legal basis to deny a PRA request for records otherwise subject to disclosure. The Keep Washington Working Act's relevant restrictions on local law enforcement agencies concern responses to federal immigration "notification requests" (requests for advance notice of an individual's release from custody) and the provision of "nonpublicly available personal information." WASH. REV. CODE §§ 10.93.160(4)(b), (5); WASH. REV. CODE § 43.17.420(11) (defining "notification request"). The CCTV footage and other RTCC data in question that the PRA requires SPD to disclose arguably do not fall within either category. We are unaware of any court decision that directly addresses whether either the shield law or the Keep Washington Working Act provides a basis to deny a PRA request.

[126] *See* SEATTLE OFF. OF THE MAYOR, *supra* note 78 (discussing local storage of the raw video footage); *fususVAULT & Evidence.com*, AXON (July 20, 2026), https://www.axon.com/help/fusus/software/fusus/vault-management.htm (describing how video evidence can be stored as clips that are uploaded to Axon's cloud).

[127] *See* Mayor's Office Policy, *supra* note 120.

[128] *See* 8 U.S.C. § 1225(d)(4) (granting to immigration officers administrative subpoena power to require testimony or documents relating to a civil immigration matter); WASH. REV. CODE § 43.17.425 (2024); WASH. REV. CODE § 7.115.020 (2023). In a civil case, an agency could issue an administrative subpoena, under which SPD would be required to disclose the requested data if the agency obtained a court order to enforce it. To accomplish this, the requesting agency would need to show that it has statutory authority to make the request, the demand is not overbroad, and the information sought is reasonably relevant to the inquiry at hand. *See* See v. City of Seattle, 387 U.S. 541, 544 (1967). In a criminal case, a federal agency could obtain a grand jury subpoena for the data, which requires an even lower standard of proof. Grand jury subpoenas are presumptively valid; to resist it, SPD would bear the burden of showing that the request is unreasonably broad or that there is no reasonable nexus between the information sought and the subject of the investigation. *See* FED. R. CRIM. P. 17(c)(2);

United States v. Morton Salt Co., 338 U.S. 632, 642–43 (1950); United States v. R. Enters., Inc., 498 U.S. 292, 299–301 (1991).

[129] *See* FED. R. CRIM. P. 17(c)(2) (permitting a court to quash or modify a subpoena "if compliance would be unreasonable or oppressive"). As a matter of law, it is unlikely that a *state* agency could obtain such a subpoena against SPD. State subpoenas generally do not run outside the issuing state, so an out-of-state agency must ask a Washington court to issue a corresponding subpoena. *See* WASH. REV. CODE §§ 5.51.010–5.51.020.

[130] *See* 18 U.S.C. § 2703. By hosting RTCC and broader SPD camera footage, investigative files, and other data through its Evidence.com platform, Axon serves as a "remote computing service" for the purposes of the Electronic Communications Privacy Act ("ECPA"). *See* 18 U.S.C. § 2711(2). This law allows for government entities to compel disclosure of a customer's — in this case SPD's — records directly from the company holding them despite the presence of state or local laws that otherwise might protect that information. *See* 18 U.S.C. § 2703(a).

[131] SPD's contract with Axon contains a provision that appears to acknowledge concerns arising from data-sharing under ECPA. The contract requires Axon to notify SPD if the company receives a court order for SPD data and to "object to any warrant or subpoena on the grounds that [Axon] does not have possession, custody or control over SPD evidence" and requires SPD to notify City Council should the vendor receive any such legal order. Amendment to Contract No. 3640 (Public Safety Body Worn Video System) between City of Seattle and Axon Enterprise, Inc., Attachment 01, § 5.4 (Notices) (executed Nov. 18, 2024) (on file with author). This is in line with amendments to Ordinances 127110 and 127111 that require SPD to include in any contract with an RTCC vendor "1) a requirement that the vendor immediately notify SPD if the vendor receives a warrant or subpoena seeking SPD Real-Time Crime Center data for any purpose, including purposes related to reproductive healthcare or gender-affirming medical services; and 2) a requirement that the vendor retain legal counsel to challenge any such warrant or subpoena and advise of outcome or existence of warrant after expiration." SEATTLE, WASH., Ordinance 127111, § 4 (Oct. 8, 2024); Seattle, Wash., Ordinance 127110, § 3 (Oct. 8, 2024).

[132] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 41.

[133] *See* WASH. STATE RECORDS COMM., LAW ENFORCEMENT RECORDS RETENTION SCHEDULE, v. 9.0, at 1 (June 2026), https://www.sos.wa.gov/sites/default/files/2026-06/law-enforcement-records-retention-schedule.PDF (providing that records "must be retained for the minimum retention period as specified in this schedule" and that "Washington State Archives strongly recommends the disposition of public records at the end of their minimum retention period").

[134] The policy need not disclose the legal arguments the City would advance in any particular case. By ordinance, if the City or its vendor receives a warrant, subpoena, or court order for CCTV data in a federal civil immigration enforcement matter, SPD must pause use of the CCTV camera systems for 60 days and report to City Council within two business days; Council may then extend the pause or end the program. *See* Seattle, Wash., Ordinance 127297 § 3 (Sept. 22, 2025), amended by Seattle, Wash., Ordinance 127412, § 2 (Apr. 6, 2026).

[135] *See* DRAFT RTCC PROCEDURE § 12.100-PRO-2(1)(a)–(c); Policing Project Interview with Seattle Police Dep't Personnel (Oct. 27, 2026) (on file with author).

[136] SPD personnel informed us that the draft procedure currently is under attorney review. *See* Policing Project Interviews with Seattle Police Dep't Personnel (Oct. 26–27, 2026) (on file with author).

[137] *See* SMC ch. 14.18 (2018).

[138] *See* SMC § 14.18.020(A) (department must, "prior to acquisition, obtain Council ordinance approval of the acquisition and a surveillance impact report for the technology"); SMC § 14.18.040(B) (listing required SIR contents).

[139] *See* SMC § 14.18.020(F) ("Following Council approval of the acquisition and the terms of the SIR, the department may acquire and use the approved surveillance technology only in accordance with the procedures and protocols set forth in the SIR.").

[140] *See* SMC § 14.18.020(F). This "material change" process places primary responsibility for identifying material changes on the agencies that own or operate the technology, but directs Seattle's IT Department to monitor for material changes as well. *See* SEATTLE INFO. TECH., SURVEILLANCE POL'Y POL-203, at 4–5 (Dec. 30, 2022) (on file with author) [*hereinafter* POL-203].

[141] *See* SPD Policy 12.100, *supra* note 15; DRAFT RTCC PROCEDURE, *supra* note 36.

[142] *See* 2024 RTCC SIR, *supra* note 43, at 24; 2025 RTCC SIR, *supra* note 17, at 24; SEATTLE POLICE DEP'T, 2024 SURVEILLANCE IMPACT REPORT: CLOSED-CIRCUIT TELEVISION CAMERA SYSTEMS 23 (2024) [*hereinafter* 2024 CCTV SIR]; 2025 CCTV SIR, *supra* note 17, at 24; *see also* Seattle, Wash., Ordinance 127110 (Oct. 8, 2024) (recitals); Seattle, Wash., Ordinance 127111 (Oct. 8, 2024) (recitals).

[143] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 38.

[144] *See* 2024 RTCC SIR, *supra* note 43, at 36; 2025 RTCC SIR, *supra* note 17, at 9; 2025 CCTV SIR, *supra* note 17, at 8.

[145] *See* Email from Seattle Police Dep't Personnel to Policing Project Staff (Aug. 28, 2026) (on file with author) ("This was an initiative that was put forward by former COO Maxey. Momentum on this policy has since stalled since his departure."). *But see* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 38 (discussing how the omnibus policy has been put in motion again).

[146] *See* 2025 RTCC SIR, *supra* note 17, at 9, 31.

[147] Briefing Memorandum from Tim Burgess, *supra* note 81, at 1 ("Gun violence, human trafficking, and other persistent felony crimes are concentrated at specific places…."); *see also* Letter from Bruce Harrell, *supra* note 81, at 1 (pilot will "prevent gun violence, human trafficking, and persistent felony crime").

[148] *See* WASH. REV. CODE § 9.94A.030 (defining "most serious offense," "serious violent offense," and "violent offense" but not the terms used in the SIRs); 2025 RTCC SIR, *supra* note 17, at 3 (software "is used to alert RTCC staff to a serious criminal event"); 2024 RTCC SIR, *supra* note 43, at 3; *see also* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 39.

[149] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 38 (explaining that restricting use to certain qualifying offenses is problematic because a final call type doesn't always match the initial type — for example, a call about a person yelling may be classified as a nuisance initially but result in assault charges).

[150] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 83.

[151] Use of policing technologies often expands far beyond their original purposes: fusion centers created for counterterrorism purposes now pursue "all crimes" and "all hazards," while license plate readers introduced to locate stolen vehicles now are used for minor matters such as unpaid fines. *See* MICHAEL GERMAN & JAY STANLEY, WHAT'S WRONG WITH FUSION CENTERS? 6 (ACLU, Dec. 12, 2007); Dave Maass, *"No-Cost" License Plate Readers Are Turning Texas Police into Mobile Debt Collectors and*

Data Miners, ELEC. FRONTIER FOUND. (Jan. 26, 2016), https://www.eff.org/deeplinks/2016/01/no-cost-license-plate-readers-are-turning-texas-police-mobile-debt-collectors-and.

[152] *See* Agreement No. IG2025-03, *supra* note 12, ex. A (evaluating the pilot against the City's stated aim to "address ongoing gun violence, vehicle theft, human trafficking, and persistent felony crime," including changes in felony and violent crime incidents); Press Release, Seattle Cmty. Police Comm'n, CPC Official Statement on SPD's Technology Assisted Crime Prevention Pilot Program (Mar. 21, 2024), https://www.seattle.gov/documents/Departments/CommunityPoliceCommission/Press%20Releases/2024/CPC%20Statement%2003.21.24%20SPD%20technology.pdf (CPC "does not oppose a time-limited and location-limited surveillance pilot with the primary aim of reducing gun violence in our City" and two years "is enough time for SPD and OIG to determine whether or not these technologies reduce gun violence in Seattle").

[153] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 22 (discussing how changes in scope and "grey area" around when RTCC personnel can engage has created uncertainty and reluctance to engage proactively).

[154] SPD chose this retention period as "a good balance between protecting people's privacy and having a history of footage that could potentially be useful in investigations." SPD Aug. 25 Responses, *supra* note 30.

[155] *See id.*; SPD Policy 12.100, at § 12.100-POL-1(1); 2025 CCTV SIR, *supra* note 17, at 7. The five-day limit applies to SPD's own CCTV cameras; retention for private cameras differs. *See infra* "Inconsistent safeguards across camera types."

[156] *See* 2025 RTCC SIR, *supra* note 17, at 7–8; 2024 RTCC SIR, *supra* note 43, at 7–8.

[157] *See* SPD Policy 12.100, at § 12.100-POL-1(3).

[158] *See* SMC § 14.18.020(A). This may be particularly true for systems like the RTCC, which are designed to integrate different functionalities.

[159] At the time of this audit, three locations had integrated a total of 23 cameras with the RTCC through the Connect Seattle Program. *See* SPD Oct. 14 Responses, *supra* note 21. Connect Seattle also includes a voluntary registry of private cameras that are not integrated into the RTCC. The registry shows the locations of participating cameras and their owners' contact information, so that RTCC personnel can ask an owner to provide footage relevant to an investigation. SPD told us that access to the registry is limited to RTCC staff and technicians, although no written policy governs that access. *See* Memorandum from Brian Maxey, SPD Chief Operating Officer, to Councilmember Bob Kettle, *Connect Seattle Plan* 1 (Mar. 31, 2025), Clerk File 323332; SPD Aug. 25 Responses, *supra* note 30; *infra,* Appendix D.

[160] *See* SPD Policy 12.100-POL-2(1) ("Permanent digital masking will be used on cameras that have non-public spaces within their field of view…."); Policing Project Interviews with Seattle Police Personnel, *supra* note 22.

[161] *See* SPD Aug. 25 Responses, *supra* note 30; Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 22.

[162] *See* SEATTLE OFF. OF CITY AUDITOR, 2024 ANNUAL SURVEILLANCE TECHNOLOGY USAGE REVIEW 6 (Sept. 30, 2025) (SDOT cameras appear on the Traveler Information Map); *Public Space Cameras (CCTV)*, SEATTLE POLICE DEP'T, https://www.seattle.gov/police/community-policing/community-programs/cctv (last visited Oct. 30, 2026); Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 38. OIG's recent review includes a map of CCTV locations integrated into the RTCC. *See* OFF. OF

INSPECTOR GEN. FOR PUB. SAFETY, ANNUAL SURVEILLANCE REVIEW: TECHNOLOGY ASSISTED PUBLIC SAFETY PILOT PROGRAM 4 (Sept. 30, 2026) [*hereinafter* OIG TAPS Review].

[163] SPD personnel identified several technical limits on applying uniform rules across camera types. SPD applies privacy masking at the camera level and cannot add it to private or other third-party cameras once they are integrated into the RTCC. SPD instead proposed integrating only cameras that view public areas, such as streets and sidewalks. Retention of private camera footage is set by each business on its own hardware, and SPD cannot change it without either an agreement with each business or a technical change by Axon. SPD indicated, however, that it could adopt a policy limiting RTCC personnel to reviewing footage no more than five days old, regardless of how long the owner retains it. SPD also expressed support for publishing the locations of private cameras at the block level. *See* Policing Project Interviews with Seattle Police Dep't Personnel (Sept. 28–29, 2026) (on file with author).

[164] SPD Policy 12.100 (introductory section), *supra* note 15; *see also* SPD Aug. 25 Responses, *supra* note 30, at Q1.a (describing "the current policy of not monitoring cameras unless there was a call for service"); Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 22.

[165] *See* SPD Aug. 25 Responses, *supra* note 30 (World Cup "events had a case event number created for them prior to cameras being streamed," and the feeds "were shown in a gallery of small thumbnails to show crowd size and movement"); *see also* Tyler Cunnington, *Seattle Mayor Explains Decision to Turn on CCTV Cameras for World Cup: 'Credible Threat,'* KOMO NEWS (June 7, 2026), https://komonews.com/news/local/seattle-mayor-explains-decision-to-turn-on-cctv-cameras-for-world-cup-credible-threat-fifa-soccer-security-data-privacy-federal-government-immigration-abortaion-police-crime-homicide-shooting-assault-soccer.

[166] *See* Seattle, Wash., Ordinance 127297 (Sept. 22, 2025) (CCTV) (approving expanded CCTV deployment locations); Seattle, Wash., Ordinance 127298 (Sept. 22, 2025) (RTCC) (approving the integration of SDOT cameras).

[167] *See* SMC § 14.18.020(F).

[168] *Id.*

[169] The policy also states that the City's IT Privacy Office will "provide guidance and assistance, as available, to departments in updating SIRs to reflect material changes." POL-203, at 4–5.

[170] POL-203, at 4.

[171] Policing Project Interview with Seattle Info. Tech. Priv. Off. Staff (May 28, 2026) (on file with author). *See, e.g.*, *infra* "Private camera integrations."

[172] A business connects its existing security system into the RTCC with a small device called a fususCORE. *Connect Seattle*, SEATTLE POLICE DEP'T, https://communityconnectseattle.org (last visited Oct. 30, 2026) ("All you need is a small CORE device that you plug into your camera system."); SPD Aug. 25 Responses, *supra* note 30.

[173] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 33.

[174] *See* SPD Oct. 14 Responses, *supra* note 21.

[175] *See* SPD Aug. 25 Responses, *supra* note 30 ("SPD has 100 cores to allocate to businesses. At the time of w[ri]ting, No [*sic*] decision has been made on how these will be distributed.").

[176] *See* OIG TAPS Review, *supra* note 162, at 10 (SIRs "provide no criteria for deployment," and "citywide expansion of private cameras appears neither expressly permitted nor prohibited"); *see also id.* at 11

(Recommendation 2: SPD should "adopt policies and procedures to specify criteria for integrating privately owned cameras").

[177] *See* Seattle, Wash., Ordinance 127111, § 3 (Oct. 8, 2024).

[178] *See* Memorandum from Brian Maxey, *supra* note 159, at 1 (describing the camera registry, and noting only that a "Connected Registration option may be implemented for businesses").

[179] For example, Axon recently developed a "head-detection" capability — an algorithm to locate heads in video feeds to facilitate later tracking and identification. *See A Quick Guide to Head Recognition with AI*, AXON, https://www.axon.com/blog/head-recognition-with-ai (last visited Oct. 20, 2026). SPD personnel told us this new feature was disabled by default and has not been enabled to date. *See* SPD Aug. 25 Responses, *supra* note 30.

[180] *See* SPD Aug. 25 Responses, *supra* note 30 ("There is no formal blanket agreement to have new features disabled by default."); *see generally* Amendment to Contract No. 3640, *supra* note 131; AXON, *supra* note 28.

[181] *See, e.g.*, SEATTLE OFF. FOR CIVIL RIGHTS, POLICY BRIEFING MEMO TO COUNCILMEMBER ALEXIS MERCEDES RINCK RE: COUNCIL BILL 121052 AND COUNCIL BILL 121053, at 4 (Aug. 28, 2025); 2024 CCTV SIR, 51–52 (2024); Amy Sundberg, *Harrell Pushes to Expand Recently Passed Surveillance Camera Pilot Program*, URBANIST (Aug. 4, 2025), https://www.theurbanist.org/harrell-pushes-to-expand-recently-passed-surveillance-camera-pilot-program.

[182] For the initial pilot locations, SPD completed a "Racial Equity Toolkit" ("RET") to identify and mitigate any potential impacts on racial equity associated with the surveillance technology. Census data included in the RET show that the Chinatown-International District is approximately 73% non-white, including a population that is 49.2% Asian, compared to 16.9% citywide. The Downtown Commercial Core has a Black population of 11.1%, compared to 6.8% citywide, and Belltown has an Asian population of 30.4%. The Aurora Avenue North deployment area has a Latino population of 11.3%, compared to 8.2% citywide. *See* 2024 RTCC SIR, *supra* note 43, at 28 (citing U.S. Census Bureau Decennial Census; OPCD); 2024 CCTV SIR, *supra* note 142 at 27.

[183] *See* David Weisburd, *The Law of Crime Concentration and the Criminology of Place*, 53 CRIMINOLOGY 133, 135–38 (2015); Anthony A. Braga et al., *Hot Spots Policing and Crime Reduction: An Update of an Ongoing Systematic Review and Meta-Analysis*, 15 J. EXPERIMENTAL CRIMINOLOGY 289, 305 (2019); Piza et al., *supra* note 86, at 148–49; *cf*. Bennett Capers, *Crime, Surveillance, and Communities*, 40 FORDHAM URB. L. J. 959, 988–89 (2013); Bennett Capers, *Race, Policing, and Technology*, 95 N.C. L. REV. 1241, 1280 (2017); Alexandra Natapoff, *Underenforcement*, 75 FORDHAM L. REV. 1715, 1716–18, 1723 (2006).

[184] The 2024 CCTV SIR explains that "[g]un violence, human trafficking, and other persistent felony crimes are concentrated at specific geographic places in the city," and that cameras would be installed at locations where such "crime is concentrated," with specific areas "selected based on the data analysis." 2024 CCTV SIR, *supra* note 142, at 3, 43. SPD has since told us that it did not prepare a specific placement analysis; SPD's understanding is that the Mayor's Office relied on calls-for-service and shots-fired heat maps prepared by SPD's analytics team. *See* Email from Seattle Police Dep't Personnel to Policing Project Staff, *supra* note 145 ("SPD did not create and [*sic*] specific analysis for CCTV camera placement . . . I assume they looked at CFS and shots fired heatmaps to make their decision."). SPD personnel told us that the pilot areas account for roughly twenty percent of the city's violent crime. *See* Policing Project Interview with Seattle Police Dep't Personnel, supra note 33 (pilot areas "account for 20% of the violent crime and 10% of all crime in the city"); Policing Project Interview

with Seattle Police Dep't Personnel, supra note 22 (CCTV viewshed covers roughly "20% of violent crime" hot spots).

[185] *See* Vincent M. Southerland, *The Master's Tools and a Mission: Using Community Control and Oversight Laws to Resist and Abolish Police Surveillance Technologies*, 70 UCLA L. Rev. 2, 16–24 (2023); Jeffrey Fagan et al., *Stops and Stares: Street Stops, Surveillance, and Race in the New Policing*, 43 Fordham Urb. L. J. 539, 547–50 (2016); Bernard E. Harcourt & Tracey L. Meares, *Randomization and the Fourth Amendment,* 78 U. Chi. L. Rev. 809, 815, 854–59 (2011).

[186] *See* Email from Seattle Police Dep't Personnel to Policing Project Staff, *supra* note 145 ("SPD did not create and [*sic*] specific analysis for CCTV camera placement …. I do not have any record of specific reports used"); *cf*. 2024 CCTV SIR, *supra* note 142, at 21–29; SPD Policy 12.100, at § 12.100-POL-1 (neither providing for periodic reassessment of deployment locations); 2025 RTCC SIR, *supra* note 17, at 23 (noting the "RET" is "specific to the initial pilot areas").

[187] Seattle's Surveillance Ordinance establishes requirements for the review of SPD's use of surveillance technology. *See* SMC § 14.18.060; OIG TAPS Review, *supra* note 162, at 2 (OIG "is required by Seattle Municipal Code (SMC) 14.18 to review surveillance technologies used by the Seattle Police Department"). Note that this audit does not evaluate whether SPD has complied with all the rules governing the RTCC's functions and how often misuse or mistakes have occurred; that responsibility rests with OIG. Rather, we seek to identify any logging or internal review gaps that might hinder an effective compliance process.

[188] *See, e.g.*, Peter Dujardin, *Smithfield Police Violated State Law By Sharing Flock Data with FBI After ODU Shooting,* Virginian-Pilot (Oct. 11, 2026), https://www.pilotonline.com/2026/10/11/smithfield-police-shared-flock-data-with-fbi-after-odu-shooting-that-violated-state-law (stating a Virginia police department shared ALPR data with the FBI in violation of a state statute); Tomo Chien, *SFPD Let Georgia, Texas Cops Illegally Search City Surveillance Data on Behalf of ICE*, S.F. Standard (Sept. 8, 2025), https://sfstandard.com/2025/09/08/sfpd-flock-alpr-ice-data-sharing (stating San Francisco police let out-of-state police run more than 1.6 million searches of the city's ALPR database, in violation of a state law prohibiting out-of-state data sharing).

[189] *See, e.g.*, Sam Sachs, *Georgia Officer Fired, Accused of Misusing Flock Safety System to Track Ex-Girlfriend*, WSB-TV (Oct. 8, 2026), https://www.wsbtv.com/news/local/clarke-county/north-georgia-officer-terminated-accused-misusing-flock-safety-system-track-ex-girlfriend/6DRWCJN55FGDVJGAGB6WMMVROA (stating a police officer was charged after allegedly using ALPRs to track the location of an ex-girlfriend); Joe Schroeder, *Indiana Sheriff's Deputy Allegedly Used Flock Cameras to Track Wife, Ex-Girlfriend*, Fox59 (Sept. 25, 2026), https://fox59.com/news/indynews/indiana-sheriffs-deputy-arrested-for-flock-camera-misuse-intimidation-and-official-misconduct (stating an officer used ALPRs to track the movements of several people including ex-girlfriends, his wife, and a man his wife knew); Anastasia Lennon, *Police Chief Recommends Termination of 2 Officers Found to Use Flock to Track Romantic Partners,* New Bedford Light (Sept. 3, 2026), https://newbedfordlight.org/police-chief-recommends-termination-of-2-officers-found-to-use-flock-to-track-romantic-partners (stating two officers were under review for criminal charges for using ALPRs to track ex-romantic or current romantic partners).

[190] *See* Nat'l Inst. of Standards & Tech., Special Publication 800-53, Rev. 5: Security and Privacy Controls for Information Systems and Organizations 67 (2020) (audit records should establish what type of event occurred, when and where it occurred, its source and outcome, and the identity of the individuals involved); *see also* OIG TAPS Review, *supra* note 162, at 8 (without a case number or

justification requirement, "SPD lacks a way to prevent, control, or audit improper use of the technology").

[191] Nat'l Inst. of Standards & Tech., Special Publication 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations 70 (2020).

[192] *See* SPD Policy 12.100, at § 12.100-POL-5(2); Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 22.

[193] OIG's 2026 review reached the same conclusion. *See* OIG TAPS Review, *supra* note 162, at 8 ("Absent this requirement, SPD lacks a way to prevent, control, or audit improper use of the technology."). Its Recommendation 1 provides that "SPD should request Axon implement a requirement for RTCC analysts to provide a case number and/or justification for each instance they view CCTV camera footage in the Axon Fusus software." *See id.*, at 9. SPD responded that it "has already requested this feature as an enhancement for Fusus but will submit a formal request," with an estimated implementation date of October 16, 2026. *See id.*, at 22.

[194] SPD informed us that it has requested Axon make the system's logging functions more robust. *See* SPD Aug. 25 Responses, *supra* note 30, at Q2.c ("No the FUSUS log does not currently track this activity. A request to the vendor has been made to make the Audit Logs more robust."). SPD reports that despite having object recognition capability, they do not often use this function. *See* OIG TAPS Review, *supra* note 162, at 7.

[195] *See* SMC § 14.18.060; OIG TAPS Review, *supra* note 162.

[196] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 22.

[197] *See* Agreement No. MO 2026-02 between the City of Seattle and Policing Project (2026) (on file with author).

[198] *Responsible Use of Policing Tech: Evaluative Framework*, Policing Project, https://www.policingproject.org/tech-framework (last visited Nov. 4, 2026) (reproduced in Agreement No. MO 2026-02 as Exhibit B, at 25–31). Note that this is meant to serve as a guide for analysis, not a definitive checklist for a particular project or work product.

[199] *See* POL-203, *supra* note 140, §§ 1–3 (Dec. 30, 2022) (on file with author) (listing criteria and stating that "[p]rior to acquiring non-standard technology, departments must complete the online Privacy & Surveillance Assessment form").

[200] *See* SMC §§ 14.18.010, 14.18.020(A), (B)(1); POL–203, *supra* note 140, at §§ 1–4.

[201] *See* Seattle Info. Tech., Priv. Assessment No. 4678, *Closed Circuit Television Camera Systems* (submitted Oct. 24, 2023) (on file with author); Seattle Info. Tech., Privacy Assessment No. 4729, *Axon Fusus Real Time Crime Center Software* (submitted Nov. 22, 2023) (on file with author).

[202] *See* Seattle Info. Tech., 2023 Fourth Quarter Surveillance Technology Determination Report 5, 48–49, 90–91 (2023) (providing criteria reviews for Case Nos. 4678 and 4729).

[203] *See* SMC § 14.18.040(A)–(B); *see, e.g.*, 2025 RTCC SIR, *supra* note 17, at 22 (outlining that "[d]epartments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit ("RET")").

[204] *See Public Comment Period Opening for the Technology Assisted Crime Prevention Pilot Technologies*, Seattle Info. Tech. (Feb. 2, 2024), https://techtalk.seattle.gov/2024/02/02/public-comment-period-opening-for-the-technology-assisted-crime-prevention-pilot-technologies;

Memorandum from Derrick Wheeler-Smith, Dir. of Off. of C.R., to Pub. Safety & Human Services Comm. (May 22, 2024) ("The Executive has since retracted its request for AGLS.").

[205] *See* SMC §§ 14.18.020 (C), 14.18.040 (B)(4).

[206] *See* SEATTLE INFO. TECH., *supra* note 204.

[207] *See* Ben Dalgetty, *Mayor Harrell Announces Crime Prevention Technology Pilot Next Steps Following Public Input*, SEATTLE OFF. OF THE MAYOR (May 31, 2024), https://harrell.seattle.gov/2024/05/31/mayor-harrell-announces-crime-prevention-technology-pilot-next-steps-following-public-input; 2024 CCTV SIR, *supra* note 142, apps. D–G (2024); 2024 RTCC SIR, *supra* note 43, apps. D–G (2024).

[208] SMC § 14.18.080(B)(1).

[209] SMC §§ 14.18.020(G), 14.18.050(C).

[210] *See* 2024 RTCC SIR, *supra* note 43, at 38–40.

[211] Press Release, Seattle Cmty. Police Comm'n, CPC Official Statement on SPD's Technology Assisted Crime Prevention Pilot Program (Mar. 21, 2024), https://www.seattle.gov/documents/Departments/CommunityPoliceCommission/Press%20Releases/2024/CPC%20Statement%2003.21.24%20SPD%20technology.pdf

[212] *See* Memorandum from Derrick Wheeler-Smith, *supra* note 204.

[213] SMC § 14.18.020(A), (F); *see, e.g.,* Seattle, Wash., Ordinance 127110 (Oct. 2024) (approving the 2024 CCTV SIR with several amendments, reflected in sections 2–4).

[214] *See* Seattle, Wash., Ordinance 127110 §§ 2–4 (Oct. 8, 2024); Seattle, Wash. Ordinance 127111, §§ 2–4 (Oct. 8, 2024).

[215] SMC § 14.18.020 (F) ("[N]on-material updates may be made to the SIR by a department without Council action so long as the change is clearly marked as such in the SIR.").

[216] *Id.* ("Any 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….").

[217] *See* POL–203, *supra* note 140, at § 10.

[218] *See* 2025 CCTV SIR, *supra* note 17, at 10–11; 2025 RTCC SIR, *supra* note 17, at 5; Council Bill 121052 (Sept. 9, 2025) (considering the updated CCTV SIR); Council Bill 121053 (Sept. 9, 2025) (considering the updated RTCC SIR).

[219] *See* Seattle, Wash., Ordinance 127297 (Sept. 22, 2025); Seattle, Wash., Ordinance 127298 (Sept. 22, 2025).

[220] *See* Seattle, Wash., Ordinance 127297, § 3 (Sept. 22, 2025), *amended by* Seattle, Wash., Ordinance 127412, § 2 (April 6, 2026).

[221] *See* SMC § 14.18.050(A).

[222] *See* SMC § 14.18.060.

[223] *See* SMC § 14.18.070.

[224] *See* SEATTLE INFO. TECH. DEP'T, 2025 SURVEILLANCE TECHNOLOGY COMMUNITY EQUITY IMPACT ASSESSMENT AND POLICY GUIDANCE REPORT 4–5, 13–14 (2025).

[225] *See* SEATTLE INFO. TECH. DEP'T, 2026 SURVEILLANCE TECHNOLOGY COMMUNITY EQUITY IMPACT ASSESSMENT AND POLICY GUIDANCE REPORT 13–15 (2026).

[226] OIG TAPS Review, *supra* note 162, at 2, 22.

[227] *See* SPD Policy 12.100, at § 12.100.

[228] Draft RTCC Procedure § 12.100-PRO-1–3.

[229] *See* Seattle Police Dep't Pol'y Manual § 12.050 (rev. eff. Apr. 15, 2026).

[230] *See* Seattle Police Dep't Pol'y Manual § 6.060 (rev. eff. May 1, 2025).

[231] Seattle Police Dep't Pol'y Manual § 5.140 (eff. Aug. 1, 2019).

[232] *See* Seattle Police Dep't Pol'y Manual §§ 7.010 (eff. Mar. 9, 2014), 7.090 (eff. Nov. 1, 2021).

[233] *See* Seattle Police Dep't Pol'y Manual § 12.080 (eff. Mar. 1, 2019).

[234] *See* Seattle Police Dep't Pol'y Manual § 5.002 (eff. July 15, 2018).

[235] SPD Policy 12.100, at § 12.100, at POL-3(1) (eff. Mar. 1, 2026) (listing access as limited to "authorized department employees, the Office of Police Accountability (OPA), and the Office of the Inspector General (OIG)"); OIG TAPS Review, *supra* note 162, at 12 (observing users included RTCC personnel, SPD staff and administrators, Seattle Information Technology Department, and the vendor).

[236] *See* OIG TAPS Review, *supra* note 162.

[237] *See* Seattle Police Dep't Pol'y Manual §§ 10.020-POL-3(2) (rev. eff. June 8, 2026) (requiring background checks for access to criminal justice information), 12.050-POL (12) (rev. eff. Apr. 15, 2026) (requiring renewed background checks every five years). *See* 2025 RTCC SIR, *supra* note 17, at 12 (2025) (describing background check requirements for RTCC personnel).

[238] *See* Seattle Police Dep't, Pol'y Manual § 12.050 (rev. eff. Apr. 15, 2026).

[239] *See* SPD Aug. 25 Responses, *supra* note 30) ("The System Administrator grants access to FUSUS. This is done via the City of Seattle's Single Sign on Service utilizing Microsoft Entra ID. The system admin logs into the City of Seattle's active domain controller and puts the employee credentials into the Fusus Group, that resides in the AD Controller."); 2025 RTCC SIR, *supra* note 17, at 12 (stating that "[a]ccess to the systems/technology is limited to authorized personnel via password-protected login credentials.").

[240] *See* Policing Project Interviews with Seattle Police Dep't Personnel (May 27–28, 2026) (on file with author).

[241] *See supra,* Part IV.B.

[242] *See id.*

[243] *See* SPD Aug. 25 Responses, *supra* note 30.

[244] *See supra,* Part IV.B; *see* OGC Interview, *supra* note 119 (confirming that Washington State and local agencies must submit requests through the interagency portal).

[245] *See* SPD Aug. 25 Responses, *supra* note 30, at Q8e.

[246] *See* SPD Oct. 14 Responses; *infra*, Appendix D § C.

[247] *See* SPD Policy 12.100, at 12.100-POL-4(4); OGC Interview, *supra* note 119 (noting that most record sharing occurs through legal process, under protective orders if necessary).

[248] *See* Wash. Rev. Code § 42.56.080(2); *see also* Wash. Admin. Code § 44-14-03006; Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 38 (stating that SPD cannot require PRA requesters to identify themselves because state law permits anonymous requests).

[249] *See* Wash. Rev. Code § 42.56.240(2); *see* Does v. King County, 366 P.3d 936 (App. Ct. Wash. 2015) (holding that pixelating victims' faces in surveillance footage was adequate to comply with the "victim or witness" PRA exemption).

[250] *See* SPD Policy 12.100, at § 12.100-POL-4(3); 2025 RTCC SIR, *supra* note 17, at 12; 2025 CCTV SIR, *supra* note 17, at 12.

[251] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 22.

[252] *See* SMC § 14.18.070(A) ("The CTO shall direct any department not in compliance with the requirements of this Chapter 14.18 to cease acquisition or use of the surveillance technology or its data.").

[253] *See* SEATTLE POLICE DEP'T POL'Y MANUAL, § 5.002-POL(1)–(2) (eff. July 15, 2018).

[254] *See* SMC § 14.18.070(B).

[255] *See* Seattle, Wash., Ordinance 127110 (Oct. 8, 2024); 2024 CCTV SIR, *supra* note 142, at 10 (noting that "one or three geographic areas will be chosen for the pilot project"); SEATTLE OFF. OF THE MAYOR, *supra* note 78 (detailing the three pilot CCTV areas).

[256] *See* Seattle, Wash., Ordinance 127297 (Sept. 22, 2025) (approving three additional areas); SEATTLE OFF. OF THE MAYOR, *supra* note 78.

[257] *See* SPD Oct. 14 Responses, *supra* note 21 (listing the number of integrated cameras by type and area).

[258] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 22 ("5 cameras at each cluster. 4 [don't] move, one is PTZ"); OIG TAPS Review, *supra* note 162, at 5 (each location "includes five cameras"); SPD. Aug. 25 Responses, *supra* note 30 (explaining that two cameras near a Planned Parenthood clinic were shut off, so not every cluster operates five cameras).

[259] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 33 ("wireless cameras that … use a cellular connection").

[260] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 22.

[261] *See* Policing Project Interviews with Seattle Police Dep't Personnel (May 26–28, 2026) (on file with author) (masking done "on the chipset" by Seattle IT staff dedicated to SPD).

[262] *See* SPD Aug. 25 Responses, *supra* note 30 ("The five days of CCTV footage from SPD cameras is stored on hardware at each camera site.").

[263] *See id.*

[264] *See* SMC § 14.18.030(B)(4) (2025) (surveillance ordinance requirements do not apply to "[c]ameras installed on City property solely for security purposes"); Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 33.

[265] *See* SPD Aug. 25 Responses, *supra* note 30 (cameras at nine SPD buildings, including "All Precincts, Harbor Patrol, K9 building and SPD Evidence Building"); SPD Oct. 14 Responses, *supra* note 21 (listing 116 cameras at nine government facilities).

[266] *See* SPD Oct. 14 Responses, *supra* note 21 ("We have masked those views either digitally or physically (some do not have digital masking feature).").

[267] *See* SPD Oct. 14 Responses, *supra* note 21 (footage is stored "in two places: 1) Fusus (five-day retention) and 2) on an on-premise City server (31 days for external cameras)").

[268] *See* Seattle, Wash., Ordinance 127298 (Sept. 22, 2025) (material update "will provide the Seattle Police Department (SPD) the ability to view the Seattle Department of Transportation (SDOT) traffic monitoring cameras").

[269] *See* SPD Oct. 14 Responses, *supra* note 21 (96 SDOT cameras); Seattle, Wash., Ordinance 127298.

[270] *See Travelers Home Page*, SEATTLE DEP'T OF TRANSP. https://web.seattle.gov/travelers/ (last visited Oct. 30, 2026); SEATTLE OFF. OF CITY AUDITOR, 2024 ANNUAL SURVEILLANCE TECHNOLOGY USAGE REVIEW 6 (Sept. 30, 2025) (SDOT cameras "provide live video or updated static images 24 hours a day on the Traveler Information Map").

[271] *See* SPD Aug. 25 Responses, *supra* note 30 ("SPD cannot independently control SDOT PTZ cameras. SDOT maintains control of the PTZ and Movement of SDOT cameras. Yes, SPD can request that SDOT Pan and Tilt the camera …. RTCC must provide SPD CAD # and reason.").

[272] *See* Policing Project Interviews with Seattle Police Dep't Personnel (May 26–28, 2026) (on file with author).

[273] *See* Policing Project Interviews with Seattle Police Dep't Personnel (May 26–27, 2026) (on file with author); *see* SEATTLE OFF. OF CITY AUDITOR, *supra* note 270, at 6 (SDOT uses the cameras "to monitor traffic conditions and quickly respond to traffic issues").

[274] *See* SPD Aug. 25 Responses, *supra* note 30 ("SDOT does not retain video on their cameras. The one-day retention for SDOT cameras is retained in Fusus.").

[275] *See* SEATTLE POLICE DEP'T, *supra* note 172 ("All you need is a small CORE device that you plug into your camera system.").

[276] *See, e.g.,* 2024 RTCC SIR, *supra* note 43, at 7–8 (describing the ability to integrate private cameras feeds from businesses); *see* OIG TAPS Review, *supra* note 162, at 10 (SIRs "provide no criteria for deployment," and "citywide expansion of private cameras appears neither expressly permitted nor prohibited"); Seattle, Wash., Ordinance 127111 § 3 (Oct. 8, 2024) (requiring a report on private camera integration); 2025 CCTV SIR, *supra* note 17, at 7.

[277] *See* SPD Aug. 25 Responses, *supra* note 30 ("Axon states that in order to buy a Core for integration, they need to agree to the Terms & Conditions - Connect Seattle.").

[278] *See* SPD Oct. 14 Responses, *supra* note 21 (23 cameras at three private locations, as of Oct. 14, 2026).

[279] *See* Memorandum from Brian Maxey, *supra* note 159 ("Cameras at private single-family homes cannot use the Connected Registration option.").

[280] *See* SPD Aug. 25 Responses, *supra* note 30 ("SPD has 100 cores to allocate to businesses. At the time of writing, No decision has been made on how these will be distributed."); Policing Project Interviews with Seattle Police Dep't Personnel (May 26–28, 2026) (on file with author).

[281] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 22.

[282] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 38 (SPD "[c]an't do masking" on private cameras). *But see* OIG TAPS Review, *supra* note 162, at 22 (SPD management response: SPD has committed to "restrict ingestion of private camera feeds to only include public areas").

[283] *See* SPD Aug. 25 Responses, *supra* note 30 ("The business has discretion on setting this. SPD is not recommending any min or max….").

[284] *See* Memorandum from Brian Maxey, *supra* note 159, at 1 ("…this option gives the Department the location and owner information for private security cameras but does not allow SPD to view the cameras in real-time.").

[285] *See* 2024 RTCC SIR, *supra* note 43, at 7–8 (describing camera registries as part of an RTCC system); Seattle, Wash., Ordinance 127111, § 3 ("Should the Seattle Police Department choose to utilize the

features of the Real-Time Crime Center pilot project that allow for private camera integration, the Department shall, as part of the project, provide a report to the Public Safety Committee or its successor on the Department's implementation plan and policies for the integration of private cameras into the Real-Time Crime Center."; Memorandum from Brian Maxey, *supra* note 159 (responding to the requirement in Ordinance 127111).

[286] *See* SPD Oct. 14 Responses, *supra* note 21.

[287] *See Residential Camera Registry FAQs*, SEATTLE POLICE DEP'T, https://communityconnectseattle.org/camera-registration (last visited Oct. 30, 2026) ("Anyone whose premises are located within Seattle is welcome to register the location of their private camera(s) and aid in investigations.").

[288] *See* 2025 RTCC SIR, *supra* note 17, at 7–8; Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 22 ("Registry – this is a digital canvas"; "Registry shows on map but they can't access the cam itself"); SPD Aug. 25 Responses ("The camera registry is currently only available to RTCC staff and techs. There is no written policy for this access at this time.").

[289] *See* SEATTLE POLICE DEP'T *supra* note 287 ("You are under no obligation to provide video if requested."); 2025 RTCC SIR, *supra* note 17, at 8 ("There is no obligation to share footage if a system is registered.").

[290] *See* Policing Project Interviews with Seattle Police Dep't Personnel (May 26–27, 2026) (on file with author).

[291] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 22 (discussing integration of GIS layers, like for railroad lines, utility poles, weather, all from public sources; discussing integration of high school floor plans).

[292] *See id*.

[293] *See* SPD Aug. 25 Responses, *supra* note 30 (stating that FususVAULT "is stored on the cloud. The provider is AWS,"clips "are kept for 30 days," and that "[video] clips that get uploaded into Evidence.com are only uploaded when a case event number has been created for an incident.").

[294] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 22.

[295] *See* SPD Aug. 25 Responses, *supra* note 30.

[296] *See id.* ("the FUSUS log does not currently track this activity"); Policing Project Staff Interviews with Seattle Police Dep't Personnel (May 26–27, 2026) (on file with author) (analysts describe object detection as "a last resort" because it doesn't really work).

[297] *See* SPD Aug. 25 Responses, *supra* note 30 (head detection is "disabled by default and ha[s] not been enabled").

[298] In addition to the databases listed in the table, SPD reports that RTCC analysts can access CRIMES and CARFAX. *See* SPD Aug. 25 Responses, *supra* note 30. We did not observe RTCC personnel using these systems during our site visits.

[299] *See* SPD Oct. 22 Responses, *supra* note 56.

[300] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 22.

[301] *See id.*; SPD Policy 12.100, at § 12.100-POL-5(2).

[302] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 33.

[303] *See* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 22.

[304] *See id.* (Omnixx Force provides DMV data and photos and is managed by the State Patrol).

[305] *See id.*

[306] *See id.*; *Driver and Plate Search and Driver Information and Adjudication System*, WASH. STATE DEP'T OF LICENSING, https://dol.wa.gov/driver-and-plate-search-and-driver-information-and-adjudication-system (last visited Oct. 13, 2026).

[307] *See* WASH. STATE DEP'T OF LICENSING, *supra* note 306.

[308] *See* FBI, INTERSTATE IDENTIFICATION INDEX (III) NATIONAL FINGERPRINT FILE (NFF) 1 (July 15, 2025) (describing III as a "system that ties computerized criminal history record files of the FBI and the centralized files maintained by each III participating state into a national system. This system serves as the vehicle for data sharing and integration across the country.").

[309] *See id.;* Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 22.

[310] Policing Project Interview with Seattle Police Dep't Personnel, *supra* note 22.

[311] *See id.*

[312] *See id.*

[313] *See id.*

[314] *See id.*

[315] *See id.*; SPD Oct. 14 Responses, *supra* note 21 (LinX is "most used in non-emergency cases," such as checking whether a person "is named in another report in King County").

[316] *See* SPD Oct. 14 Responses, *supra* note 21 (when asked whether RTCC data makes its way into LinX: "No.").