City of Seattle

From: The Community Surveillance Working Group

To: Executive & Seattle City Council

Date: 07/26/2024

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

Purpose

This section shall be completed after public engagement has concluded and the department has completed the racial equity toolkit section. The Privacy and Civil Liberties Impact Assessment is completed by the Community Surveillance Working Group ("working group"), per the surveillance ordinance which states that the working group shall:

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

Executive Summary

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

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

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

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

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

Sincerely,

René Peters (Position #1, Co-Chair)

Kayleigh McNiel (Position #2, Co-Chair)

Wendy Novotne (Position #3)

John Yun-Kuang Chen (Position #4)

Carolyn Riley-Payne (Position #5)

Alex Maestretti (Position #7)

Key Concerns

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

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

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

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

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

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

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

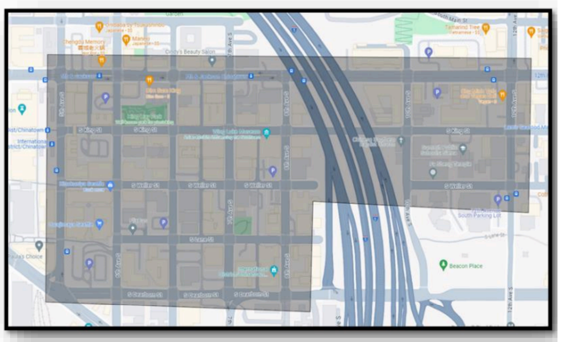
   The working group believes there may be similar concerns with SPD's deployment if the true potential and use of this technology results in the tracking of individual's movements throughout the City. Furthermore, the use of CCTV surveillance, coupled with a RTCC's enhanced license-plate readers, could be used to target protesters, deterring Seattle residents from exercising their First Amendment right to peacefully assemble and protest. Notably, the eastern edge of the proposed “Downtown & Belltown Area” surveillance zone includes Westlake Park, which is frequently utilized as a public gathering space for protests, demonstrations, and other political and cultural events.

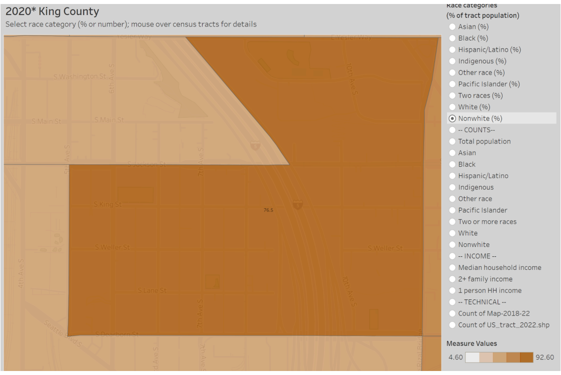
3. **Risk of disparate impact of surveillance technologies on minority communities within Seattle.**

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

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

Chinatown-International District Area

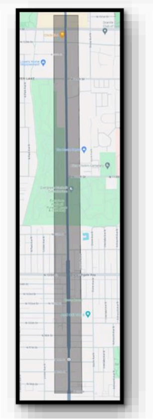


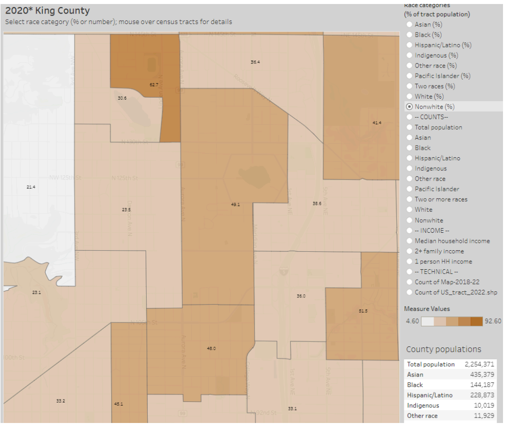


2020* King County

Select race category (% or number); mouse over census tracts for details

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





2020* King County

Select race category (% or number); mouse over census tracts for details

County populations

Total population	2,254,371
Asian	435,379
Black	144,187
Hispanic/Latino	228,873
Indigenous	10,019
Other race	11,929

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

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

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

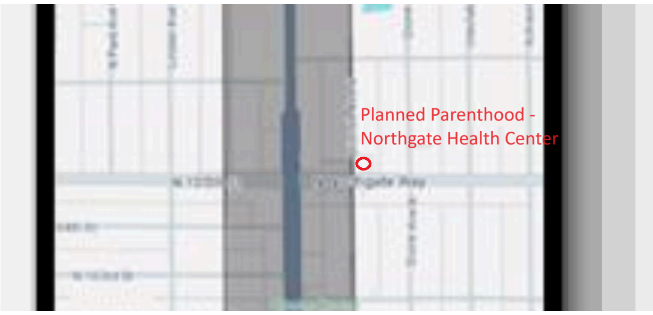
Public engagement is a key gateway leading to this working group to render a proper Privacy & Civil Liberties Assessment. It is a broad concern that the evaluation and implementation of this technology requires more public input in crucial areas, including but not limited to:

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

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

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

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



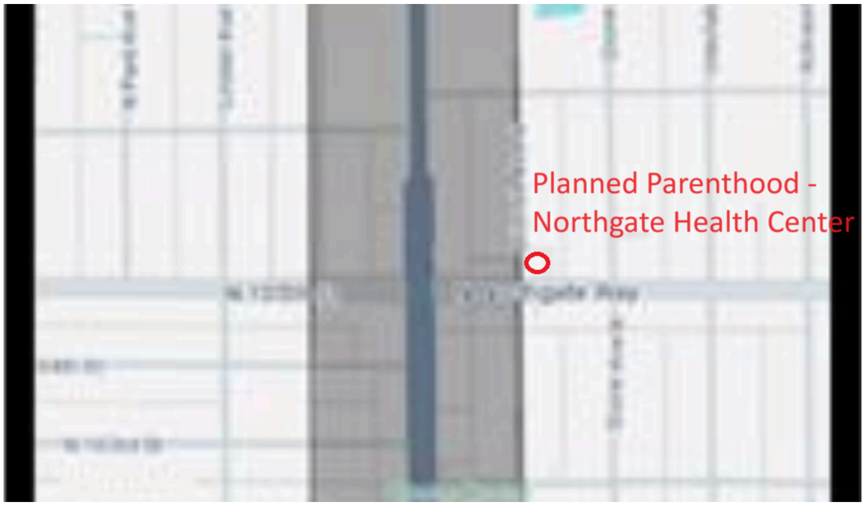
With earlier communication and review of these proposed pilot zones with the public, there may have been opportunities to flag these sensitive overlaps, and for SPD to determine coverage areas that avoided them. As it stands, this serves as another potential disparate impact to a BIPOC and marginalized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

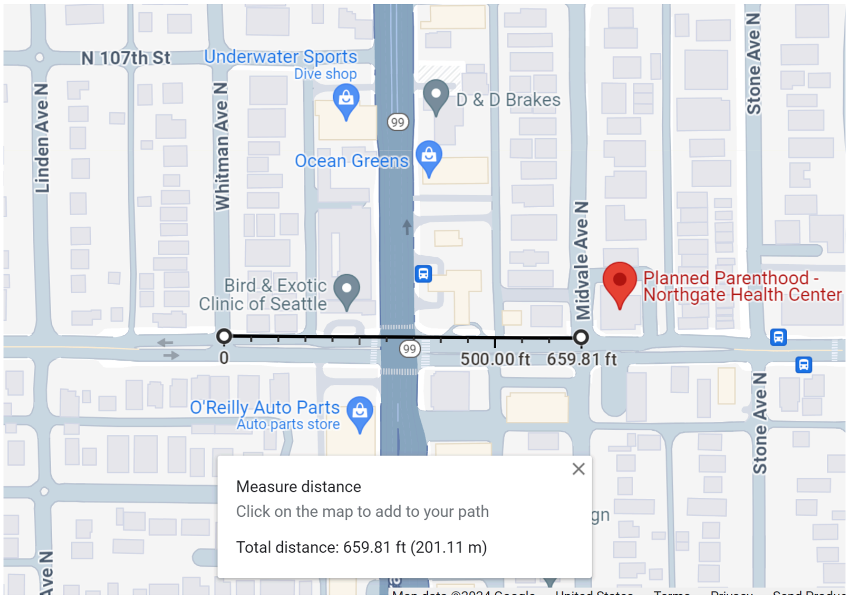
Another area of concern with this SIR is that there is not a detailed plan for reasonable notification of CCTV usage for the public. The basic requirement should be that there should be some type of signage, visual cue, or other easily-understood signal that 1) cameras are present, and 2) they are operational/being actively operated. The SIR states that “The cameras themselves will be visible to the public, and signs will be placed to alert the public to their presence and use“. Yet, this gives way to a number of other considerations. In the case of a visual/posted sign or flier, what is the correct verbiage to accurately describe the scope of the camera usage? Signs and fliers posted in English will not be sufficient to notify non-English speakers that they are in a surveillance area. This is especially concerning given the fact that the areas that have been chosen for consideration are home to a high concentration of many immigrant communities with a high amount of non-English speakers or citizens who are non-EFL. Signs may also have very low noticeability after daylight hours – understanding if the CCTV cameras themselves have lights to indicate their placement to passers by would be helpful, but the SIR doesn't contain information on any specific SKU or model. Neither signage nor lighting would be an effective notification for somebody who has a visual impairment, or is blind. As it stands, this too serves as another potential disparate risk to Seattle's BIPOC and differently-abled communities.

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

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

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

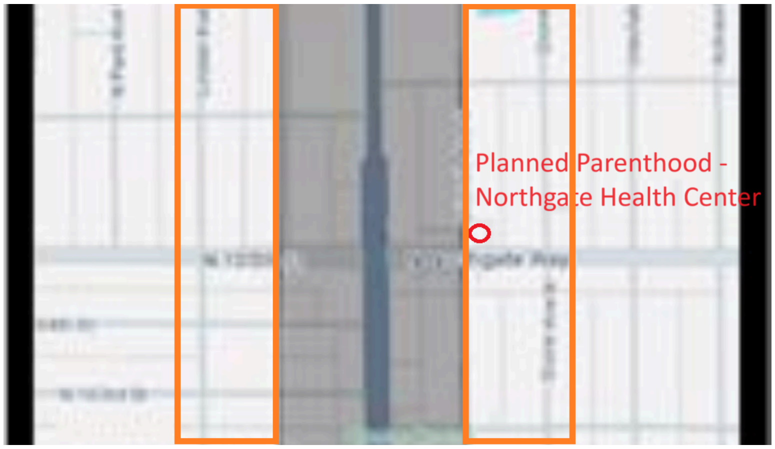




Measure distance

Click on the map to add to your path

Total distance: 659.81 ft (201.11 m)



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

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

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

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

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

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

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

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

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

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

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

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

With regard to the people reviewing the CCTV/RTCC data, there were a number of concerns surrounding privacy policies and access accountability. The SIR notes that "only authorized/trained SPD and OIG personnel will have direct access to the CCTV system" but there is a need for better understanding of what the qualifications to become authorized (if different than simply being an SPD officer or OIG member), as well as details about the training that these individuals undergo. Clarity on what types of training need to be completed, and at what frequency, would help to match areas of concern with proficiencies that the training aims to provide. The RTCC SIR notes that "The vision is for SPD to staff a real-time crime center with a combination of sworn officers and civilian staff, eventually transitioning to a more civilian-staffed model”. Thus, there is a need to understand any differences between training that sworn staff and civilian staff receive. What are the qualifications of civilian staff to gain access to information, and do they need to clear a higher bar to have access due to the fact that they do not have the ability to enforce the law? Will they need to complete background checks? It is important that standards such as SPD Policy 12.050 and Security Awareness Training (and Level 1, Level 2, etc.) be clearly explained and understood in the context of AI technology.

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

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

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

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

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

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

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

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

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

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

Timeframe is another crucial aspect to any pilot, and it appears that the SIRs may not provide a clear mechanism for the pilot to end. The CCTV SIR states that “outside academic subject matter experts will be retained to design and manage an evaluation plan with an assessment at the end of one year and another at the end of two”, but this in itself may not address any go/no-go mechanism behind the assessments. This Civil Liberties Assessment touches on the need for very clear metrics and understanding of how they will be measured. So too must there be clear actions at each checkpoint in the pilot deployment. Specifically, what are the actions that will occur if not met, such as uninstall/decommissioning of the technology? Furthermore, who will be the “outside academic experts”, what will their areas of expertise be, and how will the public be able to input on the formation of that review group? The working group flags the need to verify and ensure a clear endpoint for any pilot, such that initiating a pilot won’t allow indefinite usage and/or expansion without a built-in control.

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

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

Currently the SIR notes the following regarding governing policy:

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

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

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

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

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

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

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

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

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

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

The working group also has concerns – especially given many of the other areas such as pilot governance, AI technology risks, and community input – that the amount of deployment locations would multiply the risk presented to citizens. Multiple working group members have questioned the rollout of four CCTV locations (Aurora, Belltown, Chinatown, Downtown) given the lack of definition in key areas. Specifically, these questions center around why there is no proposed option to limit the scope of the pilot to one of these areas. A smaller rollout would limit negative impacts to the public while gaining tangible data and insights. Upon positive results (this necessitates an improved and fully developed review/assessment process as described above), the City would consider expansion and another round of proposals for said expansions. The high degree of concern in the areas above make the larger rollout proposed in the SIR a worrisome proposition.

Recommendations

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

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

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

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

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

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

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

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

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

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

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

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

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

Questions

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

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

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

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

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

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

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

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

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

Dissenting Notes (If Any)