2020 Surveillance Impact Report

Situational Awareness Cameras Without Recording

Seattle Police Department

Seattle Information Technology

Surveillance Impact Report ("SIR") Overview

About the Surveillance Ordinance

The Seattle City Council passed ordinance 125376, also referred to as the "Surveillance Ordinance", on September 1, 2017. This ordinance has implications for the acquisition of new technologies by the City, and technologies that are already in use that may fall under the new, broader definition of surveillance.

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

Surveillance Ordinance Review Process

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

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

Privacy Impact Assessment

Purpose

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

When is a Privacy Impact Assessment Required?

A PIA may be required in two circumstances.

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

1.0 Abstract

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

The Seattle Police Department utilizes four types of situational awareness cameras to monitor an identified subject or watch an area of concern while positioned from a safe distance away. SPD operates these cameras in a variety of different ways to serve specific purposes depending on the situational need. The cameras fall broadly into four categories:

- mounted on remote controlled robots,
- mounted to poles or extenders,
- strategically placed, and
- cameras that are thrown.

The images transmitted from these cameras are secured and viewed on proprietary monitors. SPD does not record, store, or retain any of the images captured by these camera technologies.

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

This technology is specifically used to covertly observe subjects, in real time, from a safe position. If used out of policy or improperly, this technology could potentially be used to inappropriately infringe on public privacy.

2.0 Project / Technology Overview

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

2.1 Describe the benefits of the project/technology.

SPD's tactical units use situational awareness cameras to assess potentially dangerous situations from a safe location. The use of these cameras allows SPD to view surroundings and gain additional information prior to entering a location, which provides additional safety and security to SPD personnel, the subjects of the observation, and other members of the community.

2.2 Provide any data or research demonstrating anticipated benefits.

The National Institute of Justice asserts that situational awareness in a potentially threatening situation is an essential key variable in determining when the use of force is necessary[1]. Situational awareness may also be to as "tactical awareness;" safety for both the officer and the subject is increased when the responding officers have visual information about the event and its surroundings.

2.3 Describe the technology involved.

There are 4 types of situational awareness cameras used by SPD's SWAT Unit:

Robot Mounted Cameras – The Avatar Robot by RoboteX incorporates a 360-degree optical camera and is remote controlled by officers from a safe position on scene. The remote range of the Avatar Robot is approximately 200 meters.

Pole Cameras – Pole camera models are made by Tactical Electronics and Smith and Wesson. These are small, portable cameras that can be extended in height (to approximately 20'). They are typically handheld during their use and send secure images to the user's handheld remote monitor.

Placeable Cameras – Camera models are made by Remington and Tactical Electronics. They are small portable cameras designed to be placed in specific strategic locations and situations. These models also send secure images to the user's handheld remote monitor.

Throwable Cameras – Camera models are made by Remington and Tactical Electronics. These small, rugged cameras are designed to be thrown into situations where access by SPD personnel is not possible. Like the pole and placeable cameras, the secure images are transmitted to the user's handheld remote monitor.

None of the images transmitted by these cameras are stored or recorded by the camera equipment or the handheld monitor.

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

The mission of the Seattle Police Department is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional, and dependable police services. SPD's SWAT unit utilizes this technology to assess potentially dangerous situations and obtain as much information about the situation as possible. By doing so, SPD personnel and the subjects involved are safer.

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

Only members of the SPD SWAT Unit are authorized to use this equipment.

3.0 Use Governance

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities contracting with the City are bound by restrictions specified in the surveillance ordinance and privacy principles and must provide written procedures for how the entity will comply with any restrictions identified.

3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

All members of SWAT are given training in the use and appropriate application of these cameras. Any SWAT personnel may elect to use one of the cameras if the situation calls for its use.

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

There is no legal standard or condition for the use of these cameras in non-protected public areas, such as a hotel hallway. However, if SPD plans to use the camera inside a protected area, such as in a person's home or property, SPD will obtain a signed search warrant from a judge, absent exigent circumstances.

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

Only members of SWAT are authorized to use this equipment and are specifically trained in their use. The SWAT commanders are responsible to ensure usage of the technology falls within appropriate usage.

[1] https://www.nij.gov/topics/law-enforcement/officer-safety/use-of-force/pages/welcome.aspx

4.0 Data Collection and Use

Provide information about the policies and practices around the collection and use of the data collected.

4.1 Provide details about what information is being collected from sources other than an individual, including other IT systems, systems of record, commercial data aggregators, publicly available data and/or other City departments.

No images or data are collected, stored, or retained by any situational awareness camera used by SPD.

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

Risk of inadvertent or improper collection is low, as no images or data are collected, stored, or retained by any situational awareness camera used by SPD.

4.3 How and when will the project / technology be deployed or used? By whom? Who will determine when the project / technology is deployed and used?

This technology is used only by the SPD SWAT Unit to assess potentially dangerous situations.

4.4 How often will the technology be in operation?

The different types of cameras are used with varying frequency depending on the circumstances. Pole-mounted cameras are used frequently to assess situations around corners and above or below officer positions.

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

These cameras are portable and do not remain in fixed locations.

4.6 Is a physical object collecting data or images visible to the public? What are the markings to indicate that it is in use? What signage is used to determine department ownership and contact information?

These cameras are covert by design. They are used to assess potentially dangerous situations from a safe distance.

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

No images or data are collected, stored, or retained by any situational awareness camera used by SPD.

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

This technology is used only by the SPD SWAT Unit and no images or data are collected, stored, or retained by any situational awareness camera used by SPD.

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

These cameras are covert by design. They are used to assess potentially dangerous situations from a safe distance. No images or data are collected, stored, or retained by any situational awareness camera used by SPD.

The decision to use situational awareness cameras is made on a case-by-case basis. These devices allow officers to monitor a subject or watch situation from a position of safety and distance. Absent exigent circumstances, a signed warrant is obtained prior to the use of this technology in any protected area.

4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

This equipment is securely stored and accessible only to the SWAT Unit for use in their operations. No images or data are collected, stored, or retained by any situational awareness camera used by SPD.

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

The following questions on data storage are not applicable to these technologies, as no images or data are collected, stored, or retained by any situational awareness camera used by SPD.

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

n/a

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

n/a

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

n/a

6.0 Data Sharing and Accuracy

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

The following questions on data sharing are not applicable to these technologies, as no images or data are collected, stored, or retained by any situational awareness camera used by SPD.

6.2 Why is data sharing necessary?

n/a

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

Yes ☒ No ☐

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

This technology is used only by the SPD SWAT Unit and no images or data are collected, stored, or retained by any situational awareness camera used by SPD.

6.4 how does the project/technology review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?

n/a

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

n/a

6.6 describe any procedures that allow individuals to access their information and correct inaccurate or erroneous information.

n/a

7.0 Legal Obligations, Risks and Compliance

7.1 What specific legal authorities and/or agreements permit and define the collection of information by the project/technology?

No images or data are collected, stored, or retained by any situational awareness camera used by SPD. When situational awareness camera equipment will be utilized in protected areas, such as inside a home, the SWAT Unit obtains a signed warrant.

7.2 Describe what privacy training is provided to users either generally or specifically relevant to the project/technology.

The SWAT Unit is trained on the appropriate usage of situational awareness cameras.

7.3 Given the specific data elements collected, describe the privacy risks identified and for each risk, explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Because the SWAT Unit requires a signed warrant before utilizing this technology in protected areas, they have mitigated the risk of improper viewing of the protected areas.

7.4 Is there any aspect of the project/technology that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?

The nature of this type of technology may cause concern by giving the appearance of privacy intrusion or misuse. These cameras are specifically designed to be covert and they allow officers to view viewing into sensitive areas. While these cameras have the capability to observe the public, they are not utilized by SPD in this manner. No information, images, or audio are recorded by any of these situational awareness cameras.

8.0 Monitoring and Enforcement

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

No images or data are collected, stored, or retained by any situational awareness camera used by SPD. When situational awareness camera equipment will be utilized in protected areas, such as inside a home, the SWAT Unit obtains a signed warrant.

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

No images or data are collected, stored, or retained by any situational awareness camera used by SPD. When situational awareness camera equipment will be utilized in protected areas, such as inside a home, the SWAT Unit obtains a signed warrant.

Financial Information

Purpose

This section provides a description of the fiscal impact of the surveillance technology, as required by the surveillance ordinance.

1.0 Fiscal Impact

Provide a description of the fiscal impact of the project/technology by answering the questions below.

1.1 Current or potential sources of funding: initial acquisition costs.

Current ☒ potential ☐

Date of initial acquisition	Date of go live	Direct initial acquisition cost	Professional services for acquisition	Other acquisition costs	Initial acquisition funding source
	6/30/2016	$67,704.86		Pole Camera w/Wrist Mounted Monitor	UASI Grant Funded
02/04/2013		$5,000		Avatar 1 Base package, Pre-owned	Org Charged: P1941

Notes:

Respond here.

1.2 Current or potential sources of funding: on-going operating costs, including maintenance, licensing, personnel, legal/compliance use auditing, data retention and security costs.

Current ☐ potential ☐

Annual maintenance and licensing	Legal/compliance, audit, data retention and other security costs	Department overhead	IT overhead	Annual funding source

Notes:

1.3 Cost savings potential through use of the technology

Respond to question 1.3 here

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

N/A

Expertise and References

Purpose

The following information is provided to ensure that Council has a group of experts to reference while reviewing the completed surveillance impact report ("SIR"). Any individuals or agencies referenced must be made aware ahead of publication that their information has been included. All materials must be available for Council to access or review, without requiring additional purchase or contract.

1.0 Other Government References

1.1 Please list any other government bodies that have implemented this technology and can speak to the implementation of this technology.

Agency, municipality, etc.	Primary contact	Description of current use

2.0 Academics, Consultants, and Other Experts

2.1 Please list any experts in the technology under consideration, or in the technical completion of the service or function the technology is responsible for.

Agency, municipality, etc.	Primary contact	Description of current use

3.0 White Papers or Other Documents

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

Title	Publication	Link
"Video for SWAT Operations"	Law and Order, The Magazine for Police Management	http://www.hendonpub.com/resources/article_archive/results/details?id=3589

Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet

Purpose

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

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

Adaption of the RET for Surveillance Impact Reports

The RET was adapted for the specific use by the Seattle Information Technology Departments' ("Seattle IT") privacy team, the Office of Civil Rights ("OCR"), and change team members from Seattle IT, Seattle City Light, Seattle Fire Department, Seattle Police Department, and Seattle Department of Transportation.

Racial Equity Toolkit Overview

The vision of the Seattle Race and Social Justice Initiative is to eliminate racial inequity in the community. To do this requires ending individual racism, institutional racism and structural racism. The racial equity toolkit lays out a process and a set of questions to guide the development, implementation and evaluation of policies, initiatives, programs, and budget issues to address the impacts on racial equity.

1.0 Set Outcomes

1.1. Seattle City Council has defined the following inclusion criteria in the surveillance ordinance, and they serve as important touchstones for the risks departments are being asked to resolve and/or mitigate. Which of the following inclusion criteria apply to this technology?

☐ The technology disparately impacts disadvantaged groups.

☐ There is a high likelihood that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service.

☐ The technology collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection.

☒ The technology raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice.

1.2 What are the potential impacts on civil liberties through the implementation of this technology? How is the department mitigating these risks?

The potential that innocent members of the community would fall under surveillance by covert use of situational awareness cameras by the SPD SWAT Unit is mitigated in two ways. First, the usage of this equipment is situational, and the cameras are used during events in which the SWAT Unit responds to calls for police service. Where the cameras are utilized in non-public areas a signed warrant is obtained prior to their use. Second, no images, data, or audio is recorded by the situational awareness cameras.

1.3 What are the risks for racial or ethnicity-based bias through each use or deployment of this technology? How is the department mitigating these risks?

The mission of the Seattle Police Department is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional and dependable police services. SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures. The use of this technology does not enhance the risks of racial or ethnicity-based bias.

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

☒ all Seattle neighborhoods

☐ Ballard	☐ Southeast
☐ North	☐ Delridge
☐ Northeast	☐ Greater Duwamish
☐ Central	☐ East district
☐ Lake union	☐ King county (outside Seattle)
☐ Southwest	☐ Outside King County.

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

N/A

1.4.1 What are the racial demographics of those living in this area or impacted by these issues?

City of Seattle demographics: White - 69.5%; Black or African American - 7.9%; Amer. Indian & Alaska Native - 0.8%; Asian - 13.8%; Native Hawaiian & Pacific Islander - 0.4; Other race - 2.4%; Two or more races - 5.1%; Hispanic or Latino ethnicity (of any race): 6.6%; Persons of color: 33.7%.

King County demographics: White – 70.1%; Black or African American – 6.7%; American Indian & Alaskan Native – 1.1%; Asian, Native Hawaiian, Pacific Islander – 17.2%; Hispanic or Latino (of any race) – 9.4%

1.4.2 How are decisions made where the technology is used or deployed? How does the Department work to ensure diverse neighborhoods are not specifically targeted?

The decision to use situational awareness cameras is made on a case-by-case basis. These devices allow officers to monitor a subject or watch situation from a position of safety and distance. Absent exigent circumstances, a signed warrant is obtained prior to the use of this technology in any protected area.

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

The Aspen Institute on Community Change defines structural racism as "…public policies, institutional practices, cultural representations and other norms [which] work in various, often reinforcing ways to perpetuate racial group inequity." Data sharing has the potential to be a contributing factor to structural racism and thus creating a disparate impact on historically targeted communities. In an effort to mitigate this possibility, SPD has established policies regarding the dissemination of data in connection with criminal prosecutions, Washington Public Records Act (Chapter 42.56 RCW), and other authorized researchers.

Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

The situational awareness cameras utilized by the SPD SWAT Unit do not record any information and therefore no information from this technology is stores or shared.

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

Like decisions around data sharing, data storage and retention have similar potential for disparate impact on historically targeted communities. SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

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

The unintended consequences related to the continued utilization of situational awareness cameras by SPD is the out of policy misuse of the technology to improperly surveil the public. SPD policies, including SPD Policy 6.060 - Collection of Information for Law Enforcement Purposes also define the way information will be gathered by SPD and states, "information will be gathered and recorded in a manner that does not unreasonably infringe upon: individual rights, liberties, and freedoms guaranteed by the Constitution of the United States and the State of Washington, including freedom of speech, press, association, and assembly; liberty of conscience; the exercise of religion…"

2.0 Public **Outreach**

2.1 Scheduled public meeting(s).

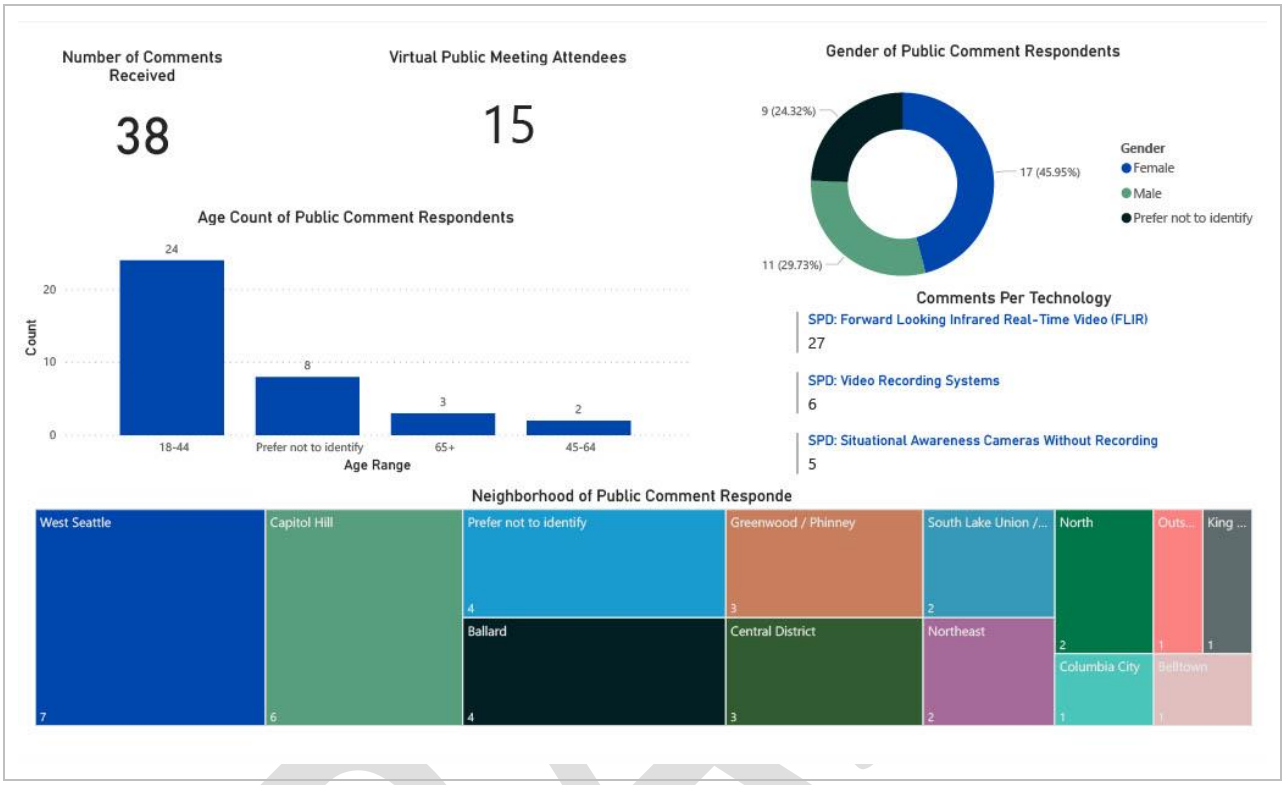
Meeting notes, sign-in sheets, all comments received, and questions from the public will be included in Appendix A-C. Comment analysis will be summarized in section 3.0 Public Comment Analysis.

Meeting 1

Location	Webex Online Event
Date	October 28th, 2020
Time	12 pm – 1 pm

3.0 Public Comment Analysis

3.1 Demographics of the public who submitted comments.



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

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

N/A

3.4 What do you want City leadership to consider about the use of this technology?

3.5 Do you have any other comments?

N/A

4.0 Response to Public Comments

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

What program, policy and partnership strategies will you implement? What strategies address immediate impacts? Long-term impacts? What strategies address root causes of inequity listed above? How will you partner with stakeholders for long-term positive change?

5.0 Equity Annual Reporting

5.1 What metrics for this technology be reported to the CTO for the annual equity assessments? Departments will be responsible for sharing their own evaluations with department leadership, change team leads, and community leaders identified in the public outreach plan.

Respond here.

Privacy and Civil Liberties Assessment

Purpose

This section shall be completed after public engagement has concluded and the department has completed the racial equity toolkit section above. The privacy and civil liberties assessment is completed by the community surveillance working group ("working group"), per the surveillance ordinance which states that the working group shall:

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

Working Group Privacy and Civil Liberties Assessment

Respond here.

Appendix A: Glossary

Accountable: (taken from the racial equity toolkit.) Responsive to the needs and concerns of those most impacted by the issues you are working on, particularly to communities of color and those historically underrepresented in the civic process.

Community outcomes: (taken from the racial equity toolkit.) The specific result you are seeking to achieve that advances racial equity.

Contracting equity: (taken from the racial equity toolkit.) Efforts to achieve equitable racial outcomes in the way the City spends resources, including goods and services, consultants and contracting.

DON: "Department of Neighborhoods."

Immigrant and refugee access to services: (taken from the racial equity toolkit.) Government services and resources are easily available and understandable to all Seattle residents, including non-native English speakers. Full and active participation of immigrant and refugee communities exists in Seattle's civic, economic and cultural life.

Inclusive outreach and public engagement: (taken from the racial equity toolkit.) Processes inclusive of people of diverse races, cultures, gender identities, sexual orientations and socio-economic status. Access to information, resources and civic processes so community members can effectively engage in the design and delivery of public services.

Individual racism: (taken from the racial equity toolkit.) Pre-judgment, bias, stereotypes about an individual or group based on race. The impacts of racism on individuals including white people internalizing privilege, and people of color internalizing oppression.

Institutional racism: (taken from the racial equity toolkit.) Organizational programs, policies or procedures that work to the benefit of white people and to the detriment of people of color, usually unintentionally or inadvertently.

OCR: "Office of Civil Rights."

Opportunity areas: (taken from the racial equity toolkit.) One of seven issue areas the City of Seattle is working on in partnership with the community to eliminate racial disparities and create racial equity. They include: education, health, community development, criminal justice, jobs, housing, and the environment.

Racial equity: (taken from the racial equity toolkit.) When social, economic and political opportunities are not predicted based upon a person's race.

Racial inequity: (taken from the racial equity toolkit.) When a person's race can predict their social, economic, and political opportunities and outcomes.

RET: "Racial Equity Toolkit"

Seattle neighborhoods: (taken from the racial equity toolkit neighborhood.) Boundaries defined for the purpose of understanding geographic areas in Seattle.

Stakeholders: (taken from the racial equity toolkit.) Those impacted by proposed policy, program, or budget issue who have potential concerns or issue expertise. Examples might include: specific racial/ethnic groups, other institutions like Seattle housing authority, schools, community-based organizations, change teams, City employees, unions, etc.

Structural racism: (taken from the racial equity toolkit.) The interplay of policies, practices and programs of multiple institutions which leads to adverse outcomes and conditions for communities of color compared to white communities that occurs within the context of racialized historical and cultural conditions.

Surveillance Ordinance: Seattle City Council passed ordinance 125376, also referred to as the "Surveillance Ordinance."

SIR: "Surveillance Impact Report", a document which captures the fulfillment of the Council-defined surveillance technology review process, as required by ordinance 125376.

Workforce equity: (taken from the racial equity toolkit.) Ensure the City's workforce diversity reflects the diversity of Seattle.

Appendix B: Meeting Notice(s)

Appendix C: All Comments Received from Members of the Public

ID: 12165161116

Submitted Through: Online Comment

Date: 11/12/2020 4:06:10 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Situational Awareness Cameras Without Recording

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

I am concerned about SPD using this technology in a transparent and fair way.

What value, if any, do you see in the use of this technology?

What do you want City leadership to consider about the use of this technology?

I do not want SPD to have access to this technology.

Do you have any other comments?

ID: 12165002568

Submitted Through: Online Comment

Date: 11/12/2020 3:06:58 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Situational Awareness Cameras Without Recording

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

test

What value, if any, do you see in the use of this technology?

test

What do you want City leadership to consider about the use of this technology?

test

Do you have any other comments?

test

ID: 12164756754

Submitted Through: Online Comment

Date: 11/12/2020 1:46:26 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Situational Awareness Cameras Without Recording

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

As of Nov. 12th, numerous questions from the public have not been answered by SPD and thus greatly hinder the ability for informed public comment. These questions include: (1) What are the complete model names/numbers for each of the equipment in scope for the Situational Awareness Cameras? (2) What technical safeguards are in place to prevent the storage/retention of images? (3) How specifically has SPD mitigated the risk of improper viewing of protected areas? (4) What (if any) sections of the SPD Manual specifically cover the use of these technologies by SWAT? SPD did not provide the manuals for this equipment in their SIR, so the public is left guessing. While it seems that SPD has an Avatar 1 Robot by RoboteX, the Avatar II robot does support audio/video recording from the remote controller and from the Audio/Video Receiver: https://robotex.com/wp-content/uploads/2019/04/RoboteX-Avatar-II-User-Manual.pdf & https://robotex.com/wp-content/uploads/2019/04/Avatar-II-AV-Receiver-User-Manual.pdf . I could not locate online the manual for the Avatar 1, but it seems likely that it would too would support recording, as it already is performing video livestreaming and recording would likely be consider valuable basic functionality for the robot to have (especially for Explosive Ordinance Disposal use cases). Additionally, the Tactical Electronics Core Monitor supports taking still images of live video (https://www.tacticalelectronics.com/wp-content/uploads/2019/03/CORE-Monitor_spec.pdf). The Tactical Electronics Core Pole Camera supports recording audio and video onto a 32GB micro SD card (https://www.tacticalelectronics.com/product/core-pole-camera/). The Tactical Electronics Core Under Door Camera supports recording video onto a 32GB micro SD card (https://www.tacticalelectronics.com/wp-content/uploads/2019/03/CORE-Under-Door-Camera_spec.pdf). Remington filed bankruptcy and had their divisions sold off to different entities. I don't know who currently owns the rights to their cameras, nor could I locate their manuals/specsheets. Smith and Wesson seems no longer make any cameras. However, third-party stores with old listings for Smith and Wesson cameras list models likely to be used by law enforcement as coming with a 4GB Micro SD card: https://www.amazon.com/Wesson-SWW-LC-PD99-Camera-4-Gigabyte-Memory/dp/B0047ERNZK & https://www.amazon.com/Smith-Wesson-SWW-LC-PD80-Enforcement-Camera/dp/B009KQYYBQ . With this mind, the public needs stronger reassurances and supporting evidence from SPD that none of these devices in scope for the SIR actually supports recording. The evidence seems to point to most (if not all) of them actually supporting recording. Also, there are some gaps in the SPD manual that should be addressed either by modifications to SPD's manual and/or via ordinance. These gaps include: (1) No part of the SPD manual specifically governs the use of these SWAT cameras, such as for what purposes are they allowed to be deployed or requiring a warrant signed by a judge before use in a non-public area. (2) SPD should be restricted by ordinance from using any situational awareness cameras with capabilities beyond what is defined in the SIR. (3) Even if none of the hardware supports recording, nothing in the SPD manual specifically governs police using SPD-provided or personal cell phones to record the livestream on the displays.

What value, if any, do you see in the use of this technology?

As it currently stands, this technology lacks sufficient guardrails to prevent abuse/misuse of the system. Additionally, SPD hasn't provided the manuals for any of this equipment and the publicly available evidence points to this equipment likely supporting recording. SPD hasn't provide sufficient evidence to the contrary. Hence the public can only assume that this SIR is incomplete and inaccurate. SPD/IT are withholding information from the public, which further impedes the ability for an informed consent by the public in seeing sufficient value in this technology.

What do you want City leadership to consider about the use of this technology?

City leadership should be made aware of the information SPD/IT has withheld from the public. This information missing from the public includes: (1) What are the complete model names/numbers for each of the equipment in scope for the Situational Awareness Cameras? (2) What technical safeguards are in place to prevent the storage/retention of images? (3) How specifically has SPD mitigated the risk of improper viewing of protected areas? (4) What (if any) sections of the SPD Manual specifically cover the use of these technologies by SWAT? SPD did not provide the manuals for this equipment in their SIR, so the public is left guessing. While it seems that SPD has an Avatar 1 Robot by RoboteX, the Avatar II robot does support audio/video recording from the remote controller and from the Audio/Video Receiver: https://robotex.com/wp-content/uploads/2019/04/RoboteX-Avatar-II-User-Manual.pdf & https://robotex.com/wp-content/uploads/2019/04/Avatar-II-AV-Receiver-User-Manual.pdf . I could not locate online the manual for the Avatar 1, but it seems likely that it would too would support recording, as it already is performing video livestreaming and recording would likely be consider valuable basic functionality for the robot to have (especially for Explosive Ordinance Disposal use cases). Additionally, the Tactical Electronics Core Monitor supports taking still images of live video (https://www.tacticalelectronics.com/wp-content/uploads/2019/03/CORE-Monitor_spec.pdf). The Tactical Electronics Core Pole Camera supports recording audio and video onto a 32GB micro SD card (https://www.tacticalelectronics.com/product/core-pole-camera/). The Tactical Electronics Core Under Door Camera supports recording video onto a 32GB micro SD card (https://www.tacticalelectronics.com/wp-content/uploads/2019/03/CORE-Under-Door-Camera_spec.pdf). Remington filed bankruptcy and had their divisions sold off to different entities. I don't know who currently owns the rights to their cameras, nor could I locate their manuals/specsheets. Smith and Wesson seems no longer make any cameras. However, third-party stores with old listings for Smith and Wesson cameras list models likely to be used by law enforcement as coming with a 4GB Micro SD card: https://www.amazon.com/Wesson-SWW-LC-PD99-Camera-4-Gigabyte-Memory/dp/B0047ERNZK & https://www.amazon.com/Smith-Wesson-SWW-LC-PD80-Enforcement-Camera/dp/B009KQYYBQ . With this mind, the public needs stronger reassurances and supporting evidence from SPD that none of these devices in scope for the SIR actually supports recording. The evidence seems to point to most (if not all) of them actually supporting recording. City leadership should be encouraged to mandate (via SPD manual changes and/or ordinance) to address some gaps and add appropriate guardrails to the use of this technology. The current gaps include: (1) No part of the SPD manual specifically governs the use of these SWAT cameras, such as for what purposes are they allowed to be deployed or requiring a warrant signed by a judge before use in a non-public area. (2) SPD should be restricted by ordinance from using any situational awareness cameras with capabilities beyond what is defined in the SIR. (3) Even if none of the hardware supports recording, nothing in the SPD manual specifically governs police using SPD-provided or personal cell phones to record the livestream on the displays.

Do you have any other comments?

There are many areas of improvement by IT/Privacy-dept. regarding their public engagement process on surveillance technologies. Some of the more recent issues include: (1) The Privacy dept. calendar event for the Group 3 public engagement meeting didn't include the access code for phone-only users to dial-in (one had to know of and go to the TechTalk blog to get the access code). (2) Directions at public engagement meeting for providing verbal public comment were to raise hand in webex which clearly is not possible for phone-only users. (3) Public engagement truncated. CTO told City Council it would be 45 days. Instead IT used 30 days with a 1 week extension agreed to be added (so 37 days). (4) The Group 3 public engagement meeting recording (as of Nov. 12th) has not been posted publicly, so people unable to attend don't have access to the discussion/Q&A before the public comment period closes. (5) SPD has not provided answers before the public comment period closes. (6) SPD further dodged valid questions from the public by requiring PRA requests, which have zero hope of being addressed within the public comment period. (7) IT has repeatedly requested & attained (and in 1 case, just self-granted) time extensions for the Surveillance Ordinance process. When the public needs time for SPD to provide answers so as to provide informed public comment, now suddenly IT is on a tight time schedule and can't extend the public comment period. Additionally, IT/Privacy-dept. has repeatedly lamented the lack of public engagement, but have also taken no additional steps to rectify this for Group 3; and did not heed prior feedback from the CSWG regarding the engagement process. There are numerous steps IT/Privacy-dept. should take to improve public engagement. The recommendations to the CTO & CPO for Group 4 include: (1) Breaking the group into smaller groups. Group 4 on deck with 13 technologies: 2 re-visits of SFD tech, 3 types of undercover technologies, & 8 other technologies. (2) Allocating more time for open public comment: minimum of 2 weeks per each in scope tech (so Group 3 would be 42 days, and Group 4 would be 154 - 182 days). (3) Hold more public engagement meetings per Group - specifically the number of public engagement meetings should at a minimum match the number of technologies being considered for public comment (otherwise the meeting will run out of time before all the questions from the public can even be asked, which did happen with Group 3). (4) Require at the public engagement meetings both a Subject Matter Expert on the use of the technology _AND_ a Subject Matter Expert on the technical management of the technology. There should be no excuse for most of the public's questions being unanswered by the City at these meetings. (5) Hold public engagement meetings that are accessible to marginalized communities most likely to have this technology used against them (such as, holding meetings at various times of day & weekends, having translators, etc). (6) Post online the recordings of all online public engagement meetings at least 1 week before the public comment period closes. (7) Require departments to provide answers to the public's questions at least 1 week before the public comment period closes. (8) Post public announcements for focus groups held by the City (9) Public engagement meetings and focus groups should have at least 1 outside civil liberties representative to present. (10) Publish to the Privacy website in a more timely manner the CSWG meeting announcements and minutes. (11) Work with more City departments (not just Dept. of Neighborhoods) to foster engagement. (12) Work with more City boards and committees to foster engagement. (13) Provide at least 2 week lead time between announcing a public engagement meeting and the timing of that meeting occurring. (14) Provide early versions of drafts SIRs to the CSWG (as they requested more than once).

ID: 12105115839

Submitted Through: Online Comment

Date: 10/23/2020 6:48:07 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Situational Awareness Cameras Without Recording

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

All video and sound feeds MUST be recorded for police accountability. Freedom of Information Act should be in place.

What value, if any, do you see in the use of this technology?

Could save lives and give SWAT a much needed new technology for public safety.

What do you want City leadership to consider about the use of this technology?

Record all video and sound files and archive properly. A transparent policy is a must.

Do you have any other comments?

ID: 12101261360

Submitted Through: Online Comment

Date: 10/22/2020 2:12:59 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Situational Awareness Cameras Without Recording

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

Typically these cameras don't have a great resolution and arent great at identifying someone. Relying on this tech to identify someone is where most of my concerns are

What value, if any, do you see in the use of this technology?

These cameras are great for seeing around corners and trying to spot folks that need pulled out of things and combined with FLIR can be real game changers when trying to locate someone in a room.

What do you want City leadership to consider about the use of this technology?

Consider using additional technology when identifying a person, but use this to help find folks.

Do you have any other comments?

Appendix D: Letters from Organizations or Commissions

November 6, 2020

Seattle Information Technology
700 5th Ave, Suite 2700
Seattle, WA 98104

RE: ACLU of Washington Comments on Group 3 Surveillance Technologies

On behalf of the ACLU of Washington, I write to offer our comments on the surveillance technologies included in Group 3 of the Seattle Surveillance Ordinance implementation process.

ACLU
AMERICAN CIVIL LIBERTIES UNION
Washington

P.O. Box 2728
Seattle, WA 98111-2728
(206) 624-2184
aclu-wa.org

Tana Lin
Board President

Michele Storms
Executive Director

The three Seattle Police Department (SPD) technologies in Group 3 are covered in the following order:

1. Forward Looking Infrared – King County Sheriff's Office Helicopters
2. Video Recording Systems
3. Situational Awareness Cameras Without Recording

These comments should be considered preliminary, given that the Surveillance Impact Reports (SIR) for each technology leave a number of important questions unanswered. Specific unanswered questions for each technology are noted in the comments relating to that technology. Answers to these questions should be included in the updated SIRs provided to the Community Surveillance Working Group and to the City Council prior to their review of the technologies.

Forward Looking Infrared - KCSO Helicopters

Background

Forward Looking Infrared (FLIR) is a powerful thermal imaging surveillance technology that raises a number of privacy and civil liberties concerns because of its ability to enable dragnet surveillance of individuals in public as well as in private spaces.

FLIR cameras sense infrared radiation to create images assembled for real-time video output. This technology detects small differences in heat, or emitted thermal energy, and displays them as shades of gray or with different colors. Because all objects emit different amounts of thermal energy, FLIR cameras are able to detect temperature differences and translate them into images.[1]

Advanced thermal imaging systems like FLIR allow governments to increase their surveillance capabilities. Like any device used for surveillance, government agents may use it inappropriately to gather information on people based on their race, religion, or political views. While thermal imaging devices cannot "see" through

[1] ACLU of Washington, *Thermal Imaging Surveillance*, THEYAREWATCHING.ORG, https://theyarewatching.org/technology/thermal-imaging-surveillance (last visited Nov. 5, 2020).

walls, pointing a thermal camera at a building can still reveal sensitive information about what is happening inside. Drug detectives often use these devices to identify possible marijuana growers by looking for heat consistent with grow lights.[2] Furthermore, privacy and civil liberties concerns with FLIR are magnified when FLIR is used in conjunction with other powerful surveillance tools such as facial recognition and drones.

The Seattle Police Department (SPD) uses three King County Sheriff's Office helicopters that are equipped with FLIR technology as well as 30-million candlepower "Night Sun" searchlights, Pro Net and LoJack radio tracking receivers, still and video cameras, and communications equipment for communicating with local, state, and federal law and firefighting agencies on their frequencies. SPD can use FLIR technology and these helicopters to monitor human beings (whose body temperatures are fairly consistent) through clouds, haze, and darkness.

There are serious concerns with SPD's use of KSCO's helicopters as described in the SIR. The policies attached in the SIR do not include purpose limitations, adequate privacy and security protections, or restrictions on use. The SIR also does not specify how long KCSO retains still images and recordings attained when assisting SPD, or whether SPD's Digital Evidence Management System (DEMS) is an on-premise or a Software-as-a-Service (SaaS) deployment.

At the public engagement meeting held on October 28, 2020,[3] SPD officers were asked if SPD had ever used KCSO helicopters or FLIR technology for the purpose of surveilling protesters and if SPD had any policies prohibiting use of these technologies for protester surveillance. The officers were also asked over which neighborhoods the helicopters had been deployed, given that the SIR states that in 2018, Guardian One was deployed 45 times to SPD events. For both questions, SPD officers declined to answer and told the public to submit public records requests. However, because SPD's Public Records Act request portal states that the minimum response timeline is in excess of 6-12 months, members of the public would not be able to receive answers to these questions in time to submit public comments on these technologies.

Given the lack of adequate policies in the SIR and the number of unanswered questions that remain, we have concerns that SPD's use of KCSO's helicopters and FLIR technology may infringe upon people's civil rights and civil liberties. KCSO's FLIR-equipped helicopters may be used to disproportionately surveil historically targeted communities, individuals exercising their constitutionally protected right to protest, or people just going about their lives.

Specific Concerns

---

[2] In the 2001 case Kyllo v. United States, the U.S. Supreme Court ruled that federal agents violated the Fourth Amendment when they used a thermal imaging device to detect marijuana plants growing inside a home.

[3] Seattle Police Department, *Surveillance Technology Public Comment Meeting*, CITY OF SEATTLE (Oct. 28, 2020), https://www.seattle.gov/Documents/Departments/Tech/Privacy/Group%203%20Presentation.pdf.

- **There are inadequate policies defining purpose of use.** The policies cited in the SIR do not impose meaningful restrictions on the purpose for which SPD may request that KSCO helicopters and FLIR technology be used. Policy 16.060 – King County Sheriff's Office Air Support Unit[4] simply states that "Guardian One offers air support for patrol and specialized missions" and that "Guardian Two offers air support for special operations such as search and rescue (SAR) and tactical missions." This policy only describes the process by which SPD may request support from KCSO's air support unit but does not state the specific purposes for which SPD may or may not request support. Section 4.9 of the SIR[5] states that SPD may request video from KCSO's Air Unit "[w]hen necessary and pertinent to a specific investigation" but does not specify the types of investigations for which SPD may request data from KSCO or how it is determined if such data is necessary and pertinent. Policy 6.060 – Collection of Information for Law Enforcement Purposes[6] states that "Information will be gathered and recorded in a manner that does not unreasonably infringe upon: individual rights, liberties, and freedoms guaranteed by the Constitution of the United States and the State of Washington" and Policy 5.140 – Bias-Free Policing states that "officers will not engage in bias-based policing."[7] However, SPD's answers at the October 28 public engagement meeting do not make clear whether and how SPD prohibits use of KCSO helicopters to engage in surveillance of protesters or biased policing. Section 1.4.2 of the Racial Equity Toolkit (RET) section of the SIR specifically asks: "How are decisions made where the technology is used or deployed? How does the Department work to ensure diverse neighborhoods are not specifically targeted?"[8] The response from SPD directs attention to SPD Policy 16.060, which does not provide adequate purpose limitations.

- **There are inadequate policies restricting data collection.** The policies cited in the SIR do not place any restrictions on the amount or types of data SPD may request from KCSO. At the October 28 public engagement meeting, SPD officers did not answer whether or how SPD places time or geographic limitations on the data it may request from KCSO.

---

[4] Seattle Police Department, *Seattle Police Department Manual: 16.060 - King County Sheriff's Office Air Support Unit*, CITY OF SEATTLE (Mar. 1, 2016), http://www.seattle.gov/police-manual/title-16---patrol-operations/16060---king-county-sheriffs-office-air-support-unit.
[5] Seattle Police Department, *2020 Surveillance Impact Report: Forward Looking Infrared Real-Time Video (FLIR) (KCSO Helicopters)*, CITY OF SEATTLE, at 12, http://www.seattle.gov/Documents/Departments/Tech/Privacy/FLIR%20-%20KCSO%20Helicopters%20Public_Engagement%20SIR.pdf (last visited Nov. 5, 2020).
[6] Seattle Police Department, *Seattle Police Department Manual: 6.060 - Collection of Information for Law Enforcement Purposes*, CITY OF SEATTLE (May 19, 2004), http://www.seattle.gov/police-manual/title-6---arrests-search-and-seizure/6060---collection-of-information-for-law-enforcement-purposes.
[7] Seattle Police Department, *Seattle Police Department Manual: 5.140 - Bias-Free Policing*, CITY OF SEATTLE (Aug. 1, 2019), http://www.seattle.gov/police-manual/title-5---employee-conduct/5140---bias-free-policing.
[8] *2020 Impact Report: Infrared Video*, supra note 5, at 23.

- **It is unclear if and how SPD protects the privacy of individuals unrelated to an investigation.** The SIR does not include any policies regarding how it redacts or deletes information. At the October 28 public engagement meeting, SPD officers did not provide an answer to the question of whether and how it redacts or deletes information collected that may compromise the privacy of individuals unrelated to an investigation.
- **It is unclear how data collected are stored and protected.** SPD stated at the October 28 public engagement meeting that it is unaware of how long KCSO retains still images and recordings obtained when assisting SPD. While SPD officers stated that SPD stores video requested from KCSO in its Digital Evidence Management System (DEMS)—not Evidence.com, this is not made clear within the SIR. Additionally, SPD officers did not answer whether SPD's DEMS is on on-premise or Software-as-a-Service (SaaS) deployment.

- **The SIR does not provide the dates and neighborhoods over which KCSO helicopters and FLIR technology have been deployed.** Though the SIR states that there have been 45 deployments of Guardian One to support SPD in 2018, the SIR does not include an analysis of the locations of those deployments.[9] Additionally, during the October 28 public engagement meeting, SPD declined to state the neighborhoods over which the helicopters had been deployed. It is important that SPD include this information in the Racial Equity Toolkit section of the final SIR in order to address the following questions in Section 1.4.2: "How are decisions made where the technology is used or deployed? How does the Department work to ensure diverse neighborhoods are not specifically targeted?"[10]

Outstanding Questions

- What are the registration and/or tail numbers for each helicopter?
- In 2019 and 2020, did the KCSO Air Support Unit have any additional helicopters aside from the three listed in the SIR?
- How long does KCSO retain still images and recordings attained when assisting SPD?
- Is SPD's Digital Evidence Management System (DEMS) an on-premise deployment or is it Software-as-a-Service?
- Has SPD ever requested KCSO ASU services or obtained data from KCSO's helicopters and/or FLIR technology to surveil protesters?
- What are the neighborhoods over which KSCO's helicopters have been deployed?

Recommendations for Regulation

At this stage, pending answers to the questions above, we can make only preliminary recommendations for the regulation of SPD's use of KCSO's helicopters and FLIR technology. We recommend that the Council adopt, via ordinance, at a minimum, clear and enforceable rules that ensure the following:

---

[9] *Id.* at 9.
[10] *Id.* at 23.

- **SPD must abide by a specific and restricted purpose of use:** The ordinance should define a specific purpose of use for KCSO's helicopters and FLIR technology, and any SPD use of KCSO's helicopters and FLIR technology and data collected with these technologies must be restricted to that specific purpose.
- **SPD must adopt processes to ensure it is not targeting diverse neighborhoods.** The ordinance should prohibit SPD from using KCSO's helicopters and FLIR technology to disproportionately surveil communities of color and other historically over-policed communities.

- **SPD must protect the privacy of individuals unrelated to a specific search or investigation.** The ordinance should require SPD to redact or delete information collected that may compromise the privacy of individuals not related to a specific search or investigation, restricted by the purpose of use.

- **SPD must produce a publicly available annual report detailing its use of KCSO helicopters and FLIR technology.** The ordinance should require that SPD produce an annual report including details on how SPD used the data collected, the amount of data collected, for how long data were retained and in what form, where the data are stored, and the neighborhoods over which KCSO helicopters and/or FLIR technology were deployed.

Video Recording Systems

Background

SPD uses two cameras systems to record and/or monitor members of the public within SPD interview rooms, Blood Alcohol Collection (BAC) rooms, and precinct holding cells: Genetec Video Management System and Milestone Systems XProtect Video Management Software and Products.

Genetec Video Management System is a permanently installed system primarily used to record in-person interactions and interviews with crime victims, witnesses, and suspects in seven designated interview rooms located at the SPD headquarters in the Seattle Justice Center. This system is used to create a video record of interviews for the purposes of use in criminal justice proceedings. Milestone Systems XProtect Video Management Software and Products is a permanently installed system in SPD's Blood Alcohol Collection (BAC) rooms and precinct holding cells. They record continuously all activity in those locations.[11]

SPD's use of these video recording systems can pose threats to people's privacy and civil liberties if used without adequate safeguards. The SIR does not provide adequate purpose limitations regarding SPD's use of these technologies, does not include full details of the capabilities of these systems, and does not adequately specify technical and procedural safeguards to prevent improper viewing,

[11] Seattle Police Department, *2020 Surveillance Impact Report: Video Recording Systems (Interview, Blood-Alcohol Collection Room, and Precinct Holding Cell Audio)*, CITY OF SEATTLE, at 4, https://www.seattle.gov/Documents/Departments/Tech/Privacy/Video%20Recording%20Systems%20Public_Engagement%20SIR.pdf (last visited Nov. 5, 2020).

collection, or storage of the images or video footage.

Specific Concerns

- **There are inadequate policies defining purpose of use.** Section 4.9 of the SIR asks, "What are acceptable reasons for access to the equipment and/or data collected?"[12] The response does not specifically detail how and for what purpose the equipment and/or data collected from the equipment may be used.

- **The capabilities of the Genetec and Milestone systems are unclear.** SPD does not provide links or attachments providing specific details about either of the systems they use. Both Genetec[13] and Milestone[14] advertise facial recognition systems that may be integrated with its video management systems.

- **It is unclear how data are collected, stored, and protected.** The SIR does not make clear whether SPD stores they data they receive in the Digital Evidence Management System or Evidence.com, a cloud-based digital evidence platform owned by Axon. The SIR simply references SPD policy 7.110 – Recorded Statements, which states that data may be uploaded to the Digital Evidence Management System (DEMS) or Evidence.com.[15] Additionally, the SIR does not include information about the security practices SPD follows to protect the privacy of members of the public who are recorded by the Genetec and Milestone video management systems. Finally, the SIR does not specify who has permission to modify the pan, tilt, and/or zoom of the cameras.

Outstanding Questions

- Does SPD use a Genetec or Milestone partner add-on that enables facial recognition or other biometric data collection/identification?
- How are firmware/software updates applied to the Genetec systems?
- What security practices does SPD follow?
- Where does the SPD Evidence Section store the Genetec-generated recordings and Milestone recordings they receive?
- For both the Genetec and Milestone systems, who has permission to modify the pan, tilt, and/or zoom of the cameras?

---

[12] *Id.* at 12.
[13] *Security Center Omnicast IP video surveillance,* GENETEC, https://resources.genetec.com/video-modules-and-add-ons/omnicast-ip-video-surveillance (last visited Nov. 5, 2020).
[14] *Dahua Face Recognition Plugin for Milestone VMS,* MILESTONE, https://www.milestonesys.com/marketplace/zhejiang-dahua-technology-co.-ltd/dahua-face-recognition-plugin-for-milestone-vms/ (last visited Nov. 5, 2020).; *Id-Guard Face Recognition Plugin,* MILESTONE, https://www.milestonesys.com/marketplace/llc-recfaces/id-guard-face-recognition-plugin/(Nov. 5, 2020).
[15] Seattle Police Department, *Seattle Police Department Manual: 7.110 - Recorded Statements,* CITY OF SEATTLE (Oct. 1, 2020), https://www.seattle.gov/police-manual/title-7---evidence-and-property/7110---recorded-statements.

Recommendations for Regulation

At this stage, pending answers to the questions above, we can make only preliminary recommendations for the regulation of SPD's use of video recording systems. We recommend that the Council adopt, via ordinance, at a minimum, clear and enforceable rules that ensure the following:

- **SPD must abide by a specific and restricted purpose of use:** The ordinance should define a specific purpose of use for any video recording systems used by SPD, and any use must be restricted to that specific purpose.

- **SPD must not use any video recording systems that have capabilities beyond what is strictly necessary to fulfill the purpose of use (e.g., recording custodial interrogations).** The ordinance should prohibit incorporating additional services such as facial recognition systems with the video recording systems.

Situational Awareness Cameras Without Recording

Background

SPD uses four types of portable cameras to observe both public and private areas during tactical operations. The four types of cameras and their vendors are:

- Robot-mounted cameras – RoboteX
- Pole-mounted cameras – Tactical Electronics & Smith and Wesson
- Placeable cameras – Remington & Tactical Electronics
- Throwable cameras – Remington & Tactical Electronics[16]

SPD's use of these situational awareness cameras can pose threats to people's privacy and civil liberties if used without adequate safeguards. The SIR does not provide adequate purpose limitations regarding SPD's use of these technologies, does not include full details of the capabilities of the cameras, and does not adequately specify technical and procedural safeguards to prevent improper viewing, collection, or storage of the images or video footage.

Specific Concerns

- **There are inadequate policies defining purpose of use.** Section 4.9 of the SIR asks, "What are acceptable reasons for access to the equipment and/or data collected?" The response states: "The decision to use situational awareness cameras is made on a case-by-case basis. These devices allow officers to monitor a subject or watch situation from a position of safety and distance. Absent exigent circumstances, a signed warrant is obtained prior to the use of this technology in any protected area."[17] This response does not

[16] Seattle Police Department, *2020 Surveillance Impact Report: Situational Awareness Cameras Without Recording*, CITY OF SEATTLE, at 5, https://www.seattle.gov/Documents/Departments/Tech/Privacy/Situational%20Awareness%20Cameras%20Public_Engagement%20SIR.pdf (last visited Nov. 5, 2020).
[17] *Id.* at 8.

provide a clear and limited purpose for which this technology may or may not be used. While SPD's response states that a warrant is obtained prior to use of the cameras in protected areas, such as inside a home, it does not state the specific purposes for which SPD may or may not use the cameras without a warrant.

- **The capabilities of the situational awareness cameras are unclear.** The SIR does not provide manuals or the complete model names and/or numbers of each of the camera technologies. During the October 28 public engagement meeting, SPD stated that their situational awareness cameras do not support recording. However, the vendor websites advertise situational awareness cameras that do support recording. For example, the Tactical Electronics Core Monitor,[18] Pole Camera,[19] and Under Door Camera[20] can either take photos, record video, and/or record audio.

- **It is unclear what technical and procedural safeguards are in place to prevent the improper viewing, collection, and storage of images.** During the October 28 public engagement meeting, SPD stated that there is no way that images, video, or audio footage could be collected and stored. In order to verify that information, SPD must provide detailed information about the technologies it uses as stated above. Additionally, even if the cameras themselves cannot record footage, it is unclear if there are policies and procedures in place to prevent live-streamed situational camera footage from being recorded via a different device.

Outstanding Questions

- What are the complete model names/numbers for each of the equipment in scope for the Situational Awareness Cameras?
- What technical safeguards are in place to prevent the storage/retention of images?
- 7.3 of Situational Awareness Cameras SIR states "[the SWAT Unit] have mitigated the risk of improper viewing of the protected areas." How specifically have they mitigated the risk?
- What (if any) sections of the SPD Manual specifically cover the use of these technologies by SWAT?

Recommendations for Regulation

At this stage, pending answers to the questions above, we can only make preliminary recommendations for the regulation of SPD's use of situational awareness cameras. We recommend that the Council adopt, via ordinance, at a minimum, clear and enforceable rules that ensure the following:

---

[18] *Core Monitor,* TACTICAL ELEC., https://www.tacticalelectronics.com/product/core-monitor/ (last visited Nov. 5, 2020).
[19] *Core Pole Camera,* TACTICAL ELEC., https://www.tacticalelectronics.com/product/core-pole-camera/ (last visited Nov. 5, 2020).
[20] *Core Under Door Camera,* TACTICAL ELEC., https://www.tacticalelectronics.com/product/core-under-door-camera/ (last visited Nov. 5, 2020).

- **SPD must abide by a specific and restricted purpose of use:** The ordinance should define a specific purpose of use for situational awareness cameras used by SPD, and any use must be restricted to that specific purpose.

- **SPD must not use any situational awareness cameras that have capabilities beyond what is strictly necessary to fulfill the purpose of use defined by the ordinance.** The ordinance should prohibit SPD from using cameras that have facial recognition or recording capabilities.

- **SPD must adopt technical and procedural safeguards to prevent misuse of the situational awareness cameras.** The ordinance should require SPD adopt safeguards that prevent use of the cameras or the footage streamed from the cameras for purposes beyond what is defined in the ordinance.

Thank you for your consideration of our comments and for facilitating this public review process.

Sincerely,

Jennifer Lee
Technology and Liberty Project Manager

Appendix E: CTO Notification of Surveillance Technology

Thank you for your department's efforts to comply with the new Surveillance Ordinance, including a review of your existing technologies to determine which may be subject to the Ordinance. I recognize this was a significant investment of time by your staff; their efforts are helping to build Council and public trust in how the City collects and uses data.

As required by the Ordinance (SMC 14.18.020.D), this is formal notice that the technologies listed below will require review and approval by City Council to remain in use. This list was determined through a process outlined in the Ordinance and was submitted at the end of last year for review to the Mayor's Office and City Council.

The first technology on the list below must be submitted for review by March 31, 2018, with one additional technology submitted for review at the end of each month after that. The City's Privacy Team has been tasked with assisting you and your staff with the completion of this process and has already begun working with your designated department team members to provide direction about the Surveillance Impact Report completion process.

Please let me know if you have any questions.

Thank you,

Michael Mattmiller

Chief Technology Officer

Technology	Description	Proposed Review Order
Automated License Plate Recognition (ALPR)	ALPRs are computer-controlled, high-speed camera systems mounted on parking enforcement or police vehicles that automatically capture an image of license plates that come into view and converts the image of the license plate into alphanumeric data that can be used to locate vehicles reported stolen or otherwise sought for public safety purposes and to enforce parking restrictions.	1
Booking Photo Comparison Software (BPCS)	BCPS is used in situations where a picture of a suspected criminal, such as a burglar or convenience store robber, is taken by a camera. The still screenshot is entered into BPCS, which runs an algorithm to compare it to King County Jail booking photos to identify the person in the picture to further investigate his or her involvement in the crime. Use of BPCS is governed by SPD Manual §12.045.	2
Forward Looking Infrared Real-time video (FLIR)	Two King County Sheriff's Office helicopters with Forward Looking Infrared (FLIR) send a real-time microwave video downlink of ongoing events to commanders and other decision-makers on the ground, facilitating specialized radio tracking equipment to locate bank robbery suspects and provides a platform for aerial photography and digital video of large outdoor locations (e.g., crime scenes and disaster damage, etc.).	3

Technology	Description	Proposed Review Order
Undercover/ Technologies	The following groups of technologies are used to conduct sensitive investigations and should be reviewed together. • **Audio recording devices**: A hidden microphone to audio record individuals without their knowledge. The microphone is either not visible to the subject being recorded or is disguised as another object. Used with search warrant or signed Authorization to Intercept (RCW 9A.73.200). • **Camera systems**: A hidden camera used to record people without their knowledge. The camera is either not visible to the subject being filmed or is disguised as another object. Used with consent, a search warrant (when the area captured by the camera is not in plain view of the public), or with specific and articulable facts that a person has or is about to be engaged in a criminal activity and the camera captures only areas in plain view of the public. • **Tracking devices**: A hidden tracking device carried by a moving vehicle or person that uses the Global Positioning System to determine and track the precise location. U.S. Supreme Court v. Jones mandated that these must have consent or a search warrant to be used.	4
Computer-Aided Dispatch (CAD)	CAD is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field.	5

Technology	Description	Proposed Review Order
CopLogic	System allowing individuals to submit police reports on-line for certain low-level crimes in non-emergency situations where there are no known suspects or information about the crime that can be followed up on. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.	6
Hostage Negotiation Throw Phone	A set of recording and tracking technologies contained in a phone that is used in hostage negotiation situations to facilitate communications.	7
Remotely Operated Vehicles (ROVs)	These are SPD non-recording ROVs/robots used by Arson/Bomb Unit to safely approach suspected explosives, by Harbor Unit to detect drowning victims, vehicles, or other submerged items, and by SWAT in tactical situations to assess dangerous situations from a safe, remote location.	8
911 Logging Recorder	System providing networked access to the logged telephony and radio voice recordings of the 911 center.	9
Computer, cellphone and mobile device extraction tools	Forensics tool used with consent of phone/device owner or pursuant to a warrant to acquire, decode, and analyze data from smartphones, tablets, portable GPS device, desktop and laptop computers.	10
Video Recording Systems	These systems are to record events that take place in a Blood Alcohol Concentration (BAC) Room, holding cells, interview, lineup, and polygraph rooms recording systems.	11
Washington State Patrol (WSP) Aircraft	Provides statewide aerial enforcement, rapid response, airborne assessments of incidents, and transportation services in support of the Patrol's public safety mission. WSP Aviation currently manages seven aircraft equipped with FLIR cameras. SPD requests support as needed from WSP aircraft.	12

Technology	Description	Proposed Review Order
Washington State Patrol (WSP) Drones	WSP has begun using drones for surveying traffic collision sites to expedite incident investigation and facilitate a return to normal traffic flow. SPD may then request assistance documenting crash sites from WSP.	13
Callyo	This software may be installed on an officer's cell phone to allow them to record the audio from phone communications between law enforcement and suspects. Callyo may be used with consent or search warrant.	14
I2 iBase	The I2 iBase crime analysis tool allows for configuring, capturing, controlling, analyzing and displaying complex information and relationships in link and entity data. iBase is both a database application, as well as a modeling and analysis tool. It uses data pulled from SPD's existing systems for modeling and analysis.	15
Parking Enforcement Systems	Several applications are linked together to comprise the enforcement system and used with ALPR for issuing parking citations. This is in support of enforcing the Scofflaw Ordinance SMC 11.35.	16
Situational Awareness Cameras Without Recording	Non-recording cameras that allow officers to observe around corners or other areas during tactical operations where officers need to see the situation before entering a building, floor or room. These may be rolled, tossed, lowered or throw into an area, attached to a hand-held pole and extended around a corner or into an area. Smaller cameras may be rolled under a doorway. The cameras contain wireless transmitters that convey images to officers.	17
Crash Data Retrieval	Tool that allows a Collision Reconstructionist investigating vehicle crashes the opportunity to image data stored in the vehicle's airbag control module. This is done for a vehicle that has been in a crash and is used with consent or search warrant.	18

Technology	Description	Proposed Review Order
Maltego	An interactive data mining tool that renders graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the internet.	19

Please let me know if you have any questions.

Thank you,

Michael