2020 Surveillance Impact Report

Video Recording Systems

(Interview, Blood-Alcohol Collection Room, and Precinct Holding Cell Audio)

Seattle Police Department

April 13th, 2021

Version 1

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.

SPD has two camera systems used to record and/or monitor members of the public within specific, secure locations in SPD facilities.

The first is the Genetec Video Management System. It is a permanently installed, non-mobile unconcealed audio and video recording system primarily used to record in-person interactions with and interviews of crime victims, witnesses, and suspects in 7 designated interview rooms located at the SPD headquarters in the Seattle Justice Center. The system also provides a live video-only view of these interview rooms. The video-only live view is used to monitor, short term, members of the community who are in the interview rooms when no SPD detective is present. This system is used to create a video record of interviews for the purposes of use in criminal justice proceedings.

The second is Milestone Systems XProtect Video Management Software and Products. These are permanently installed in SPD's Blood Alcohol Collection (BAC) rooms and precinct holding cells. They record continuously all activity in those locations.

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

These technologies are used to record members of the public who are being interviewed or having their blood alcohol levels tested or are placed in precinct holding cells. If used out of policy, improperly, or without proper notification, this technology could potentially be used to make recordings that 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.

Though the state of Washington is not one of the 26 states that requires the recording of custodial interrogations, many law enforcement agencies and criminal justice system watchdogs, such as the Innocence Project, highly recommend the practice. Benefits include: preventing disputes about how an officer conducted the interview or treated a suspect or victim; creating a record of statements made by a suspect that may capture subtle details missed in real-time; reducing false confessions; and enhancing public confidence in the practices of SPD. Creating a visual record of activities that occur within the BAC rooms and precinct holding cells also provides a measure of accountability for both SPD and involved community members.

2.2 Provide any data or research demonstrating anticipated benefits.

According to The Justice Project, "the virtue of electronic recording of custodial interrogations… lies not only in its ability to help guard against false confessions, but also in its ability to develop the strongest evidence possible to help convict the guilty." (https://web.williams.edu/Psychology/Faculty/Kassin/files/Justice%20Project(07).pdf)

2.3 Describe the technology involved.

The Genetec Video Management System includes camera and microphone equipment that is permanently installed in the interview rooms on the 6th and 7th floors of SPD Headquarters, a physical server located at SPD HQ, two dedicated computer workstations located in the detectives' work area at SPD HQ, and video-only monitors located throughout the detectives' work area and detective supervisors' offices at SPD HQ.

The Milestone Video Management Software and Products consist of cameras located in BAC rooms and precinct holding cells throughout SPD's facilities. A dedicated server is located at each of these secure locations which stores the video and audio information from the Milestone cameras.

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. The video and audio recording of victim, witness, and suspect interviews aids investigations and prosecutions of crimes as well as enhances public confidence in the practices of SPD.

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

All SPD investigative units which include: Homicide, Robbery, Gang Unit, Intelligence, Special Assault Unit, Domestic Violence Unit, Arson-Bomb Squad, Major Crimes, Auto Theft, Vice & Human Trafficking. All SPD precinct employees tasked with the collection of blood alcohol levels and holding of subjects in precinct holding cells.

Additionally, SPD Video Unit staff, and certain backgrounded and qualified Seattle IT personnel are also involved in the support of the Video Management Systems.

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.

Genetec (Interview rooms): The detective(s) conducting the interview activates the recording system for the appropriate room with a manual switch. The detective then advises the interview subject of the audio recording acquiring implied consent, or explicitly asks for permission to record per SPD Policy 7.110 – Recorded Statements. At the conclusion of the interview or blood draw, or when the subject leaves the room, the recording is terminated by the detective or officer. The detective then exports the recording from the server on one of the two designated computer work stations and creates a copy of the recording for permanent storage on a special high-quality evidence grade DVD+R disc. This evidence grade disc is then submitted into the SPD Evidence Section as a standard item of evidence.

Milestone (BAC rooms and precinct holding cells): The Milestone systems is continuously recording in the BAC rooms and precinct holding cells. In the event that an investigator (including SPD internal investigations) needs to view the video, a request must be made to the SPD Video Unit who will locate the specific time and location video requested and provide the investigator with a DVD containing the file.

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

Signage is clearly posted in all SPD precincts indicating that audio and video surveillance is in progress. These signs are posted both at the entrances to holding cells and inside holding cells and blood alcohol collection areas.

Consent is required before these technologies may be used. **RCW 9.73.030 Intercepting, recording or divulging private communication – Consent required – Exceptions.** Also known as "All party consent". Standard procedure dictates that interview subjects are always advised of the presence of the recording or asked for their permission to record. Any recording made of an interview subject without consent would be inadmissible and could possibly subject the SPD personnel to an internal conduct assessment and possibly criminal charges.

Per SPD Policy 7.110 – Recorded Statements:

When taking an audio recorded statement, the officer/detective:

1. **States** at the beginning of the recording:

   Officer's name and includes, "of the Seattle Police Department"
   Report Number
   Date and time of the recording
   The name of the interviewee
   All persons present during the interview

2. **Asks** the person to respond to the question, "Are you aware you are being recorded?"

3. **If** the person is in custody, **gives** Miranda warning.

4. **Asks** the person to state their full name.

5. **Conducts** the interview.

6. After the interview, **if** the person is a victim, witness or complainant, **asks** the person:

   Do you declare under penalty of perjury under the laws of Washington what you have stated in this statement is true and correct?
   Do you wish to have your personal information Disclosed or Not Disclosed?

7. **Announces** the end of the recording with the date and time.

8. **Uploads** the audio statement to the Digital Evidence Management System (DEMS).

9. **Documents** the recorded statement in the appropriate report.

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.

Operators of both the Genetec and Milestone video systems are sworn SPD personnel. Training on the use of these systems is provided in-house to all SPD users of this technology. All SPD employees are required to abide by all SPD policies, including SPD Policy 7.110 – Recorded Statements which is directly related to the use of video recording equipment.

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.

These technologies record only the images and sounds that occur during an SPD interview of a witness, victim, or suspect, and activity in BAC rooms and precinct holding cells.

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

These technologies record only the images and sounds that occur during an SPD interview of a witness, victim, or suspect, and activity in BAC rooms and precinct holding cells. These technologies are permanently mounted and do not record any information outside of these parameters.

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?

Genetec (Interview rooms): The detective(s) conducting the interview activates the recording system for the appropriate room with a manual switch. The detective then advises the interview subject of the audio recording acquiring implied consent, or explicitly asks for permission to record per SPD Policy 7.110 – Recorded Statements. At the conclusion of the interview or blood draw, or when the subject leaves the room, the recording is terminated by the detective or officer. The detective then exports the recording from the server on one of the two designated computer workstations and creates a copy of the recording for permanent storage on a special high-quality evidence grade DVD+R disc. This evidence grade disc is then submitted into the SPD Evidence Section as a standard item of evidence.

Milestone (BAC rooms and precinct holding cells): The Milestone systems is continuously recording in the BAC rooms and precinct holding cells. In the event that an investigation (including SPD internal investigations) needs to view the video, a request must be made to the SPD Video Unit who will locate the specific time and location video requested and provide the investigator with a DVD containing the file.

4.4 How often will the technology be in operation?

The Genetec (interview rooms) system is used on a daily basis in the course of law enforcement activities. The Milestone system (BAC rooms and precinct holding cells) records these locations continuously.

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

Both the Genetec and Milestone systems are permanently installed.

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?

The cameras for both the Genetec and Milestone systems are overtly mounted in the interview rooms at SPD Headquarters and inside BAC rooms and precinct holding cells.

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

Genetec (interview rooms): After an interview is conducted, the detective accesses the recorded audio-video file that is stored on the Genetec server using proprietary Genetec software on one of two dedicated workstations located in the secured Detectives' Working Area and creates a copy of this file on a high-quality evidence grade DVD+R disc. This evidence-grade disc is then submitted into the SPD Evidence Section as a standard item of evidence. Standard evidence retention/disposition rules are then followed.

Milestone (BAC rooms and precinct holding cells): The recordings made by the Milestone system of BAC room use is not accessed routinely, but rather only when a specific request for that footage is needed for a criminal or internal investigation. Requests for that footage is requested by an authorized party (detective, Office of Police Accountability investigator, etc.) to the SPD Video Unit within the 90-day data retention period for those files. The Video Unit creates a copy of this file on a high-quality evidence grade DVD+R disc. This evidence grade disc is then submitted into the SPD Evidence Section as a standard item of evidence. Standard evidence retention/disposition rules are then followed.

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

This technology is not operated or used by another entity on behalf of the City.

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

The primary reason for access to the data collected by both the Genetec and Milestone systems is to investigate crimes, aid in the prosecution of criminals, and monitor subjects inside SPD facilities. Additionally, these systems are used to monitor internal SPD operations and document police activities.

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.)?

Only authorized SPD users can access the system, technology, or the data. Access to the application is limited to SPD personnel via password-protected login credentials. Logs of system activity are kept for both automatic system functions and user actions which provide an audit trail to safeguard against potential unauthorized access to stored information.

The entire system is located on the SPD network which is protected by industry standard firewalls. The Seattle IT Department performs routine monitoring of the SPD network.

All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.

SPD's Audit, Policy and Research Section (APRS) can conduct an audit of the any and all systems at any time. The Office of Inspector General and the federal monitor can also access all data and audit for compliance at any time.

ITD client services interaction with SPD systems is governed according to the terms of the 2018 Management Control Agreement between ITD and SPD, which states that:

"Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBIs Criminal Justice Information Services, (CJIS) Security Policy."

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

Genetec (interview rooms): The original recordings are stored on a proprietary Genetec server that is located in a secure server room located in SPD HQ. The long-term storage copy produced by the detective is retained at the SPD Evidence Section following standard evidence retention rules.

Milestone (BAC rooms and precinct holding cells): Individual local servers are securely located all SPD precincts.

Per the CJIS Security Policy, each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history 08/16/2018 CJISD-ITS-DOC-08140-5.7 D-3 records. Additionally, each CSO (CJIS Systems Officer, or department command personnel) must ensure that all agencies establish an information security structure that provides for an ISO and complies with the CJIS Security Policy.

Both the Genetec and Milestone systems retain recordings for 90 days before they are automatically and systematically deleted from the server.

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

SPD's Audit, Policy and Research Section (APRS) can conduct an audit of the any and all systems at any time. In addition, the Office of Inspector General and the federal monitor can access all data and audit for compliance at any time.

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

Both the Genetec and Milestone systems retain recordings for 90 days before they are automatically and systematically deleted from the server.

SPD policy contains multiple provisions to avoid improperly collecting data. SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in an incident report. SPD Policy 7.090 specifically governs the collection and submission of photographic evidence. Evidence is submitted to the Evidence Unit and associated with a specific GO Number and investigation. And, SPD Policy 7.110 governs the collection and submission of audio recorded statements. It requires that officers state their name, the Department name, the General Offense number, date and time of recording, the name of the interviewee, and all persons present at the beginning of the recording.
Additionally, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002. SPD Policy 5.001 also ensures that communication on the systems subject to collection on this system is official in nature.

Per the CJIS Security Policy:
5.8.3 Digital Media Sanitization and Disposal The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

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

Unit managers are responsible for ensuring compliance with data retention requirements within SPD. Audit, Policy & Research Section personnel can also conduct audits of all data collection software and systems. Additionally, any appropriate auditor, including the Office of Inspector General and the federal monitor can audit for compliance at any time.

6.0 Data Sharing and Accuracy

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

No person, outside of SPD and Seattle IT, has direct access to the application or the data.

Data obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law.

Data may be shared with outside entities in connection with criminal prosecutions:

• Seattle City Attorney's Office

• King County Prosecuting Attorney's Office

• King County Department of Public Defense

• Private Defense Attorneys

• Seattle Municipal Court

• King County Superior Court

• Similar entities where prosecution is in Federal or other State jurisdictions

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

SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the system.

6.2 Why is data sharing necessary?

The sharing of recorded audio-video of police interviews of victims, witnesses, and crime suspects is often needed to aid in the prosecution of cases. Recordings may be shared only within the context of the situations outlined in 6.1.

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

Yes ☒ No ☐

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

Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20, regulating criminal justice information systems. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260 (auditing and dissemination of criminal history record information systems), and RCW Chapter 10.97 (Washington State Criminal Records Privacy Act).

Once disclosed in response to PRA request, there are no restrictions on non-City data use; however, applicable exemptions will be applied prior to disclosure to any requestor who is not authorized to receive exempt content.

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

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

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

The audio and video captured by these systems are real-time recordings of the interviews and activities that take place in view of the cameras permanently mounted in the interview and BAC rooms and within precinct holding cells.

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

Individuals may request records pursuant to the PRA, and individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

7.0 Legal Obligations, Risks and Compliance

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

Though the state of Washington is not one of the 26 states that requires the recording of custodial interrogations, many law enforcement agencies and criminal justice system watchdogs, such as the Innocence Project, highly recommend the practice.

Consent is required before these technologies may be used. **RCW 9.73.030 Intercepting, recording or divulging private communication – Consent required – Exceptions.** Also known as "All party consent". Standard procedure dictates that interview subjects are always advised of the presence of the recording or asked for their permission to record.

Additionally, **RCW 9.73.090 Certain emergency response personnel exempted from RCW 9.73.030 through 9.73.080—Standards—Court authorizations—Admissibility** states:

(b) Video and/or sound recordings may be made of arrested persons by police officers responsible for making arrests or holding persons in custody before their first appearance in court. Such video and/or sound recordings shall conform strictly to the following:

(i) The arrested person shall be informed that such recording is being made and the statement so informing him or her shall be included in the recording;

(ii) The recording shall commence with an indication of the time of the beginning thereof and terminate with an indication of the time thereof;

(iii) At the commencement of the recording the arrested person shall be fully informed of his or her constitutional rights, and such statements informing him or her shall be included in the recording;

(iv) The recordings shall only be used for valid police or court activities;

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

SPD Policy 12.050 mandates that all employees receive Security Awareness Training (Level 2), and all employees also receive City Privacy Training. All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), many of which contain specific privacy requirements. Any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

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.

The nature of the Department's mission will inevitably lead it to collect and maintain information many may believe to be private and potentially embarrassing. Minimizing privacy risks revolve around disclosure of personally identifiable information.

SMC 14.12 and SPD Policy 6.060 direct all SPD personnel that "any documentation of information concerning a person's sexual preferences or practices, or their political or religious activities must be for a relevant reason and serve a legitimate law enforcement purpose."

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.

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 privacy risks outlined in 7.3 above are mitigated by legal requirements and auditing processes (i.e., maintenance of all requests, copies of consent forms/statements and warrants) that allow for any auditor, including the Office of Inspector General and the federal monitor, to inspect the collection of recorded interactions between SPD and the public.

The greatest privacy risk is the unauthorized release of interview, BAC room, and holding cell video and audio recording that may contain information deemed private or offensive. To mitigate this risk, the technologies fall under the current SPD policies around dissemination of Department data and information reflected in 6.1.

8.0 Monitoring and Enforcement

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

Per SPD Policy 12.080, the Crime Records Unit is responsible to receive and record all requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies." Any subpoenas and requests for public disclosure are logged by SPD's Legal Unit. Any action taken, and data released subsequently in response to subpoenas is then tracked through a log maintained by the Legal Unit. Public disclosure requests are tracked through the City's GovQA Public Records Response System, and responses to Public Disclosure Requests, including responsive records provided to a requestor, are retained by SPD for two years after the request is completed.

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

SPD's Audit, Policy and Research Section is authorized to conduct audits of all investigative data collection software and systems, including DEMS. In addition, the Office of Inspector General and the federal monitor can conduct audits of the software, and its use, at any time. Audit data is available to the public via Public Records Request.

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
(Genetec)6/28/2016	Aug 2016	$60,603.16			P7710
(Milestone) 6/14/2016	Aug 2016	$19,520.79			P8830

Notes:

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
(Genetec) $660.06				P7715
(Milestone) $3,698.91				P3348

Notes:

1.3 Cost savings potential through use of the technology

These are not quantified; however, potential cost savings may result from better evidence for crime prosecution and mitigating liability for complaints of misconduct of SPD personnel in BAC rooms and precinct holding cells.

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
"Preventing police torture and other forms of ill-treatment – reflections on good practices and emerging approaches"	28th General Report of the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT), published in 2019	https://rm.coe.int/1680942329
"Electronic Recording of Custodial Interrogations"	TheJusticeProject.org	https://web.williams.edu/Psychology/Faculty/Kassin/files/Justice%20Project(07).pdf

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

Purpose

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

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

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?

Inherent with any video or audio recording obtained and stored by SPD, personally identifiable and potentially sensitive personal information is collected about community members, including information about 3rd parties not present during the recordings.

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. A potential civil liberties concern is that the SPD would over-surveil vulnerable or 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. The video systems described in this report are permanently installed inside SPD facilities and record individuals who are interacting with SPD personnel or are being held in precinct holding cells.

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.

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 Genetec system (Interview rooms) is located at SPD Headquarters. The Milestone system (BAC rooms and precinct holding cells) is located at all SPD precincts throughout the City of Seattle.

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.

Video and audio collected by the Genetec and Milestone systems, is shared only with outside entities in connection with criminal prosecutions or in compliance with public records requests pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester.

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 most important unintended possible consequence related to the continued utilization of the Genetec and Milestone camera systems by SPD is the potential that members of the public will be recorded without their consent. SPD Policy 7.110 – Recorded Statements forbids SPD personnel from making such recordings without consent, except in specific exigent circumstances without proper warrant. Additionally, SPD policies, including SPD Policy 6.060 - Collection of Information for Law Enforcement Purposes also define the way information will be gathered by SPD 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).

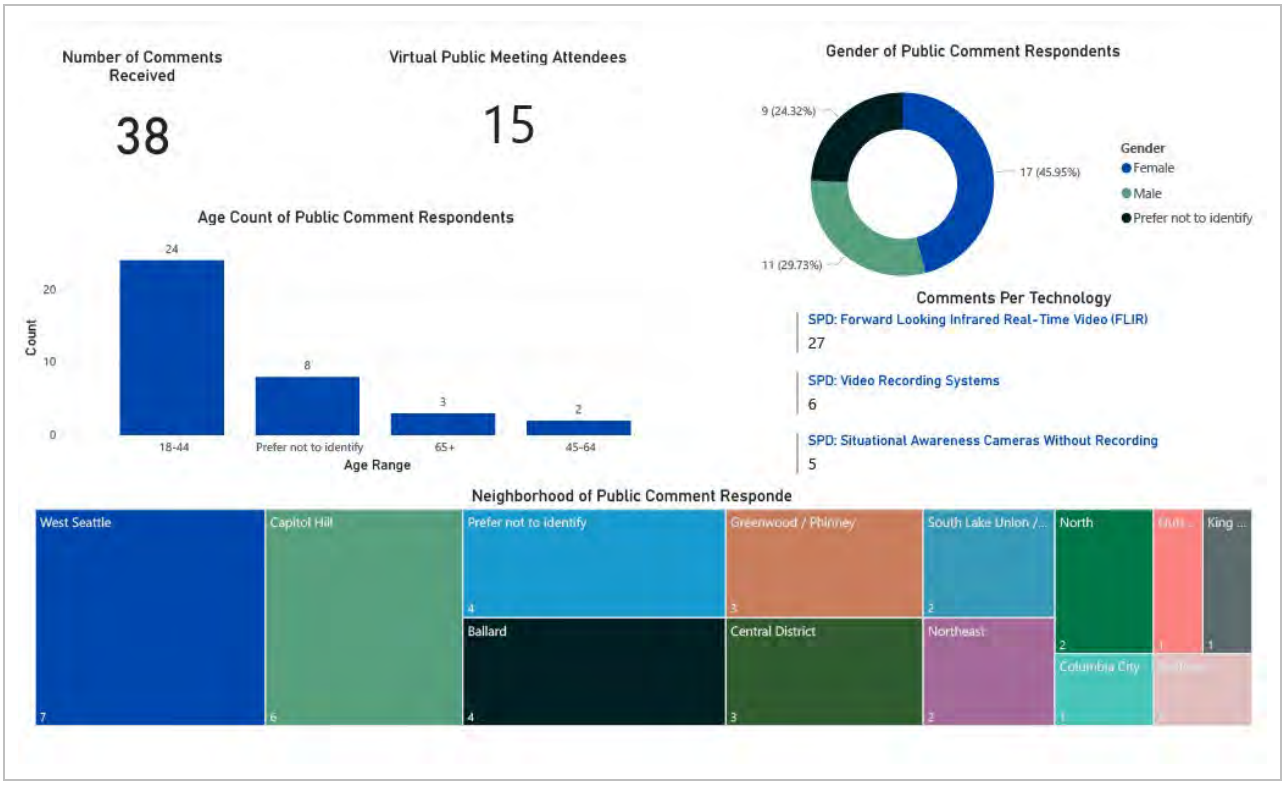
Meeting notes, sign-in sheets, all comments received, and questions from the public will be included in Appendix A-C. Comment analysis will be summarized in section 3.0 Public Comment Analysis.

Meeting 1

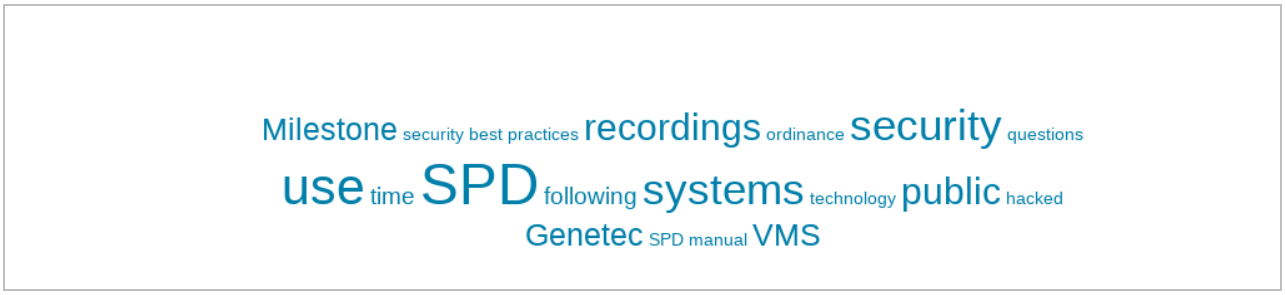
Location	Webex Online Event
Date	October 28th, 2020
Time	12 pm – 1 pm

3.0 Public Comment Analysis

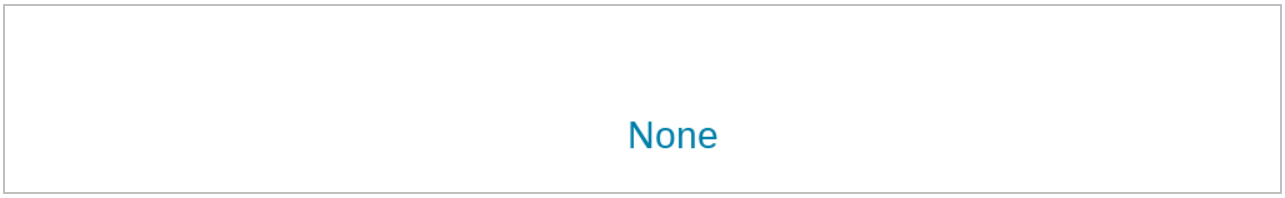
3.1 Demographics of the public who submitted comments.



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?



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?

The OIG has audit responsibilities for determining legality of the system and deployment. SPD follows case law and city ordinance and requires a legal foundation to deploy the cameras.

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

From: Seattle Community Surveillance Working Group (CSWG)

To: Seattle City Council

Date: Dec 15, 2020

Re: Privacy and Civil Liberties Impact Assessment for Video Recording Systems

Executive Summary

The CSWG has completed its review of the Surveillance Impact Reports (SIRs) for the three surveillance technologies included in Group 3 of the Seattle Surveillance Ordinance technology review process. These technologies are Forward Looking Infrared, Video Recording Systems, and Situational Awareness Cameras Without Recording. This document is the CSWG's Privacy and Civil Liberties Impact Assessment for Video Recording Systems as set forth in SMC 14.18.080(B)(1), which we provide for inclusion in the final SIRs submitted to the City Councils.

This document first provides our recommendations to Council, then provides background information, key concerns, and outstanding questions regarding Video Recording Systems.

Our assessment of Video Recording Systems as used by Seattle Police Department (SPD) focuses on three major issues:

1. The capabilities of the Genetec and Milestone systems are unclear.
2. It is unclear how data are collected, stored, and protected; additional policy language is necessary to define valid purposes of use

Recommendations:

We recommend that the Council adopt, at a minimum, clear and enforceable rules that ensure the following:

1. **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.
2. **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.

Outstanding Questions

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

City of Seattle

CTO Response

Memo

To: Seattle City Council

From: Saad Bashir, Chief Technology Officer

Subject: CTO Response to the Surveillance Working Group Video Recording Systems SIR Review

---

Purpose

As provided in the Surveillance Ordinance, SMC 14.18.080, this memo outlines the Chief Technology Officer's (CTO's) response to the Surveillance Working Group assessment on the Surveillance Impact Report for Seattle Police Department's Video Recording Systems.

Background

The Information Technology Department (ITD) is dedicated to the Privacy Principles and Surveillance Ordinance objectives to provide oversight and transparency about the use and acquisition of specialized technologies with potential privacy and civil liberties impacts. All City departments have a shared mission to protect lives and property while balancing technology use and data collection with negative impacts to individuals. This requires ensuring the appropriate use of privacy invasive technologies through technology limitations, policy, training and departmental oversight.

The CTO's role in the SIR process has been to ensure that all City departments are compliant with the Surveillance Ordinance requirements. As part of the review work for surveillance technologies, ITD's Privacy Office has facilitated the creation of the Surveillance Impact Report documentation, including collecting comments and suggestions from the Working Group and members of the public about these technologies. IT and City departments have also worked collaboratively with the Working Group to answer additional questions that came up during their review process. We believe that policy, training and technology limitations enacted by SPD and Council oversight through the surveillance technology review process provide adequate mitigation for the potential privacy and civil liberties concerns raised by the Working Group about the use of this important operational technology.

Technology Purpose

SPD has two camera systems used to record and/or monitor members of the public within specific, secure locations in SPD facilities. The first is the Genetec Video Management System. Itis a permanently installed, non-mobile unconcealed audio and video recording system primarily used to record in-person interactions with and interviews of crime victims, witnesses, and suspects in 7 designated interview rooms located at the SPD headquarters in the Seattle Justice Center. The system also provides a live video-only view of these interview rooms. The video-only live view is used to monitor, short term, members of the community who are in the interview rooms when no SPD detective is present. This system is used to create a video record of interviews for the purposes of use in criminal justice proceedings. The second is Milestone Systems XProtect Video Management Software and Products. These are permanently installed in SPD's Blood Alcohol Collection (BAC) rooms and precinct holding cells. They record continuously all activity in those locations.

Working Group Concerns

In their review, the Working Group has raised concerns about these devices being used in a privacy impacting way. Their focus was on providing details about specification and restriction of use, and concerns about additional capabilities of the systems reviewed.

Recommended Next Steps

I look forward to working together with Council and City departments to ensure continued transparency about the use of these technologies and finding a mutually agreeable means to use technology to improve City services while protecting the privacy and civil rights of the residents we serve. Specific concerns in the Working Group comments about cameras are addressed in the attached document.

Response to Specific Concerns: Video Recording Systems

Concern: Inadequate policies defining specific and restricted purpose of use

CTO Assessment: The specific and intended use of the technologies under review is governed by SPD Policy 7.110 –Recorded Statements. The process for how the technology is used and the treatment of the collected video is also outlined in the SIR. While this SIR covers two technologies with similar purpose, the capabilities and clear purpose for each system is outlined and distinguished in the review process.

SIR Response:
Section 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. The video and audio recording of victim, witness, and suspect interviews aids investigations and prosecutions of crimes as well as enhances public confidence in the practices of SPD.

Section 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.
Genetec (Interview rooms): The detective(s) conducting the interview activates the recording system for the appropriate room with a manual switch. The detective then advises the interview subject of the audio recording acquiring implied consent, or explicitly asks for permission to record per SPD Policy 7.110 –Recorded Statements. At the conclusion of the interview or blood draw, or when the subject leaves the room, the recording is terminated by the detective or officer. The detective then exports the recording from the server on one of the two designated computer workstations and creates a copy of the recording for permanent storage on a special high-quality evidence grade DVD+R disc. This evidence grade disc is then submitted into the SPD Evidence Section as a standard item of evidence.

Milestone (BAC rooms and precinct holding cells): The Milestone systems is continuously recording in the BAC rooms and precinct holding cells. In the event that an investigator (including SPD internal investigations) needs to view the video, a request must be made to the SPD Video Unit who will locate the specific time and location video requested and provide the investigator with a DVD containing the file.

Section 3.2 List the legal standards or conditions, if any, that must be met before the project / technology is used.
Signage is clearly posted in all SPD precincts indicating that audio and video surveillance is in progress. These signs are posted both at the entrances to holding cells and inside holding cells and blood alcohol collection areas.

Consent is required before these technologies may be used. RCW 9.73.030 Intercepting, recording or divulging private communication–Consent required –Exceptions. Also known as "All party consent". Standard procedure dictates that interview subjects are always advised of the presence of the recording or asked for their permission to record. Any recording made of an interview subject without consent

would be inadmissible and could possibly subject the SPD personnel to an internal conduct assessment and possibly criminal charges. Per SPD Policy 7.110 –Recorded Statements:

When taking an audio recorded statement, the officer/detective:

1. States at the beginning of the recording:

- Officer's name and includes, "of the Seattle Police Department"
- Incident or Report Number
- Date and time of the recording
- The name of the interviewee
- All persons present during the interview

2. Asks the person to respond to the question, "Are you aware you are being recorded?"

3. If the person is in custody, gives Miranda warning.

4. Asks the person to state their full name.

5. Conducts the interview.

6. After the interview, if the person is a victim, witness or complainant, asks the person:

- Do you declare under penalty of perjury under the laws of Washington what you have stated in this statement is true and correct?
- Do you wish to have your personal information Disclosed or Not Disclosed?

7. Announces the end of the recording with the date and time.

8. Uploads the audio statement to the Digital Evidence Management System (DEMS).

9. Documents the recorded statement in the appropriate report

Section 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?

Genetec (Interview rooms): The detective(s) conducting the interview activates the recording system for the appropriate room with a manual switch. The detective then advises the interview subject of the audio recording acquiring implied consent, or explicitly asks for permission to record per SPD Policy 7.110 –Recorded Statements. At the conclusion of the interview or blood draw, or when the subject leaves the room, the recording is terminated by the detective or officer. The detective then exports the recording from the server on one of the two designated computer workstations and creates a copy of the recording for permanent storage on a special high-quality evidence grade DVD+R disc. This evidence grade disc is then submitted into the SPD Evidence Section as a standard item of evidence.

Milestone (BAC rooms and precinct holding cells): The Milestone systems is continuously recording in the BAC rooms and precinct holding cells. In the event that an investigator (including SPD internal investigations) needs to view the video, a request must be made to the SPD Video Unit who will locate the specific time and location video requested and provide the investigator with a DVD containing the file.

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

The primary reason for access to the data collected by both the Genetec and Milestone systems is to investigate crimes, aid in the prosecution of criminals, and monitor subjects inside SPD facilities. Additionally, these systems are used to monitor internal SPD operations and document police activities.

Concern: Capabilities of the Genetec and Milestone systems beyond specified purpose (facial recognition)

CTO Assessment: The capabilities of both the Genetec and Milestone systems are outlined in the SIR as well as the circumstances under which they are used. There are concerns regarding additional functionality that could be added to these systems or other systems with similar advanced functionality but features such as facial recognition are not in use by any system in SPD. Any material change to the functionality of these technologies would be covered under the scope of the SIR review process. Additionally, going into effect July of 2021, Washington has passed the first state law that provides regulation and oversight over facial recognition technologies (RCW 43.386). This law regulates the development, procurement, and use of a facial recognition service, and provides a similar level of transparency and review to the Seattle Surveillance Ordinance.

SIR Response:
Section 2.3 Describe the technology involved.

The Genetec Video Management System includes camera and microphone equipment that is permanently installed in the interview rooms on the 6th and 7th floors of SPD Headquarters, a physical server located at SPD HQ, two dedicated computer workstations located in the detectives' work area at SPD HQ, and video-only monitors located throughout the detectives' work area and detective supervisors' offices at SPD HQ. The Milestone Video Management Software and Products consist of cameras located in BAC rooms and precinct holding cells throughout SPD's facilities. A dedicated server is located at each of these secure locations which stores the video and audio information from the Milestone cameras.

Section 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.
These technologies record only the images and sounds that occur during an SPD interview of a witness, victim, or suspect, and activity in BAC rooms and precinct holding cells.

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.

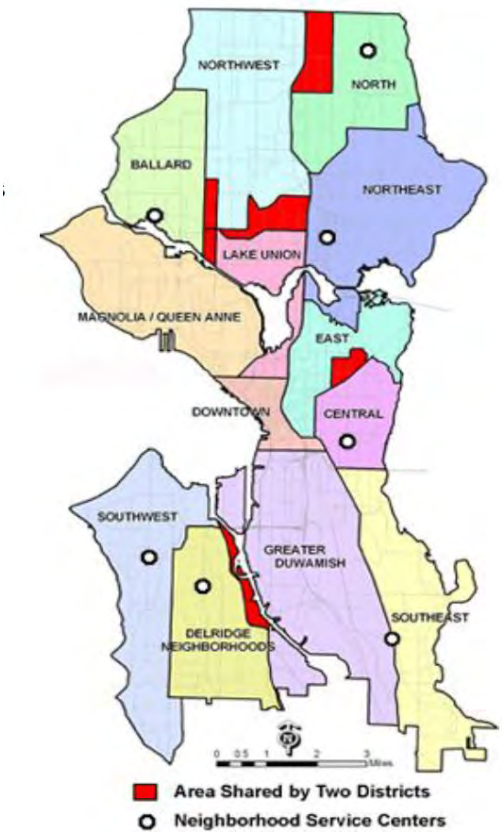
Racial inequity: (taken from the racial equity toolkit.) When a person's race can predict their social, economic, and political opportunities and outcomes.

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: 12165158184

Submitted Through: Online Comment

Date: 11/12/2020 4:05:03 PM

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

SPD: Video Recording Systems

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

I have concerns that SPD will not be transparent in the use of this technology. I worry in particular about its use in low income and minority neighborhoods.

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

I do not believe any value of this technology outweighs my major concerns.

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

I do not think the City should allow this technology.

Do you have any other comments?

ID: 12164796504

Submitted Through: Online Comment

Date: 11/12/2020 1:58:34 PM

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

SPD: Video Recording Systems

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) Does SPD use a Genetec or Milestone partner add-on that enables facial recognition or other biometric data collection/identification? (2) How are firmware/software updates applied to the Genetec systems? (3) Genetec Omnicast was the VMS used by Washington D.C. MPD CCTVs that had nearly 70% of them hacked with ransomware in 2017. It is generally understood that not following the security best practices provided by Genetec is what led to them being hacked (https://ipvm.com/reports/genetec-mpd). Keep in mind that if SPD's Genetec VMS was hacked and had the recordings leaked, then that could jeopardize publicly-anonymous witnesses (though the security of the Milestone system is also important). At the public engagement meeting, SPD's stated their understanding of the security of their VMS was based on an assumption of the contracted installer. Security should never be based on assumption; and moreover, security best practices and available security features in VMS change over time, so relying on a (possible) one-time installation as the only time security has been done on these devices would not be considered sufficient and would not meet the current industry standards for security best practices. SPD should definitively validate what security measures have been applied their VMS and communicate that to the public. Specifically: (3a) Has SPD followed all the security configuration recommendations provided by Genetec in their Best Practices document ? (3b) Similarly, has SPD followed Milestone's XProtect Hardening Checklist? (4a) Where does the SPD Evidence Section store the Genetec-generated recordings they receive via DVD+R (in DEMS, and/or Evidence.com, or something else)? (4b) Same question for the Milestone recordings (where do they go after snippets are exported on DVD)? (5) For both the Genetec and Milestone systems, who has permission to modify the pan, tilt, and/or zoom of the cameras? 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) The SPD manual doesn't limit the purpose of these recordings. (2) The ordinance that approves this tech should specifically prohibit installing/incorporating additional services that collect/assess/identify biometric information.

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. Moreover, the weak security posture puts witnesses and others at risk of having their interview leaked (and/or having the weak VMS security simply lead to the VMS being hacked as stepping stone to further attack other parts of SPD digital infrastructure). 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) Does SPD use a Genetec or Milestone partner add-on that enables facial recognition or other biometric data collection/identification? (2) How are firmware/software updates applied to the Genetec systems? (3) Genetec Omnicast was the VMS used by Washington D.C. MPD CCTVs that had nearly 70% of them hacked with ransomware in 2017. It is generally understood that not following the security best practices provided by Genetec is what led to them being hacked (https://ipvm.com/reports/genetec-mpd). Keep in mind that if SPD's Genetec VMS was hacked and had the recordings leaked, then that could jeopardize publicly-anonymous witnesses (though the security of the Milestone system is also important). At the public engagement meeting, SPD's stated their understanding of the security of their VMS was based on an assumption of the contracted installer. Security should never be based on assumption; and moreover, security best practices and available security features in VMS change over time, so relying on a (possible) one-time installation as the only time security has been done on these devices would not be considered sufficient and would not meet the current industry standards for security best practices. SPD should definitively validate what security measures have been applied their VMS and communicate that to the public. Specifically: (3a) Has SPD followed all the security configuration recommendations provided by Genetec in their Best Practices document ? (3b) Similarly, has SPD followed Milestone's XProtect Hardening Checklist? (4a) Where does the SPD Evidence Section store the Genetec-generated recordings they receive via DVD+R (in DEMS, and/or Evidence.com, or something else)? (4b) Same question for the Milestone recordings (where do they go after snippets are exported on DVD)? (5) For both the Genetec and Milestone systems, who has permission to modify the pan, tilt, and/or zoom of the cameras? 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) The SPD manual doesn't limit the purpose of these recordings. (2) The ordinance that approves this tech should specifically prohibit installing/incorporating additional services that collect/assess/identify biometric information.

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) Public comment via SurveyMonkey was configured by IT such that a single user (browser session) could only submit public comment on 1 technology. The only way to submit public comment on all the technologies would be use a different browser or clear you browser's cookies/session data, which many less technical people wouldn't know to do. This actively impedes public comment. It is ensuring there is the least public comment possible. (2) 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). (3) 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. (4) 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). (5) 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. (6) SPD has not provided answers before the public comment period closes. (7) SPD further dodged valid questions from the public by requiring PRA requests, which have zero hope of being addressed within the public comment period. (8) 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: 12111900892

Submitted Through: Online Comment

Date: 10/26/2020 8:27:30 PM

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

SPD: Video Recording Systems

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

Increased surveillance is the action of a police state, and should not be tolerated by a free society.

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

None.

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

It is antithetical to freedom.

Do you have any other comments?

This comment applies to all three systems under review.

ID: 12101381803

Submitted Through: Online Comment

Date: 10/22/2020 2:59:30 PM

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

SPD: Video Recording Systems

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

SPD has already weaponized video recording systems to limit the first amendment rights of people who politically oppose them. SPD is incredibly reckless with their use of body worn video and has demonstrated that they are not capable of following a standa

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

None

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

SPD is reckless, SPD is irresponsible, SPD is unreformable. You must take any and all surveillance tools from their control and transfer to civilian oversight boards.

Do you have any other comments?

ID: 12101189956

Submitted Through: Online Comment

Date: 10/22/2020 1:49:35 PM

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

SPD: Video Recording Systems

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

I do not trust the Seattle Police Department to handle this technology properly or within the framework of constitutional rights. The Seattle Police consistently abuse existing camera technology, such as SDOT cameras, despite existing city ordinances.

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

None. The police should not have it.

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

The astonishingly long record of human rights abuses the Seattle Police continue to mete out without the right to trial.

Do you have any other comments?

Defund SPD.

ID: 12100938026

Submitted Through: Online Comment

Date: 10/22/2020 12:24:25 PM

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

SPD: Video Recording Systems

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

None

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

Catching illegal activity and being able to quickly assess and respond to crime is a benefit to society.

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

Increase usage in problematic areas.

Do you have any other comments?

None

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