Seattle Office of Inspector General

Surveillance Technology Usage Review Camera Systems 2023

As Required by Seattle Municipal Code 14.18.060

December, 2024

Office of Inspector General
City of Seattle
PO Box 94764
Seattle, WA 98124-7064

206.684.3663
oig@seattle.gov

Purpose

OIG's Charge Under the Surveillance Ordinance

Per Seattle Municipal Code 14.18.060, OIG is required to annually review the Seattle Police Department's (SPD) use of surveillance technology and the extent to which SPD is in compliance with the requirements of Chapter 14.18.

Table of Contents

Technology Description

Camera Systems: are covert cameras and include camera wires and fixed location cameras.

Two Types of Camera Systems

"Camera Systems" refer to two types of cameras:

1. "wires," which are covert cameras used to record specific events and identifiable individuals related to criminal investigations, and
2. "fixed location cameras," which are deployed in public spaces.[1]

Whenever wires are deployed, they may be concealed on a person or in an object. If deployed on a person, the wire must be activated by that person to commence recording, and the recording is stored locally on the device. The SIR states that if a fixed location camera is deployed, "they are most often set to record only when motion is detected. Very rarely, they may be set to record continuously in instances wherein an event may happen so quickly that motion detection may not respond in time." Fixed location cameras record and store data to SPD servers.

The SPD Technical & Electronic Support Unit (TESU) manages these devices, oversees requests to use them, and installs fixed location devices. For wires, TESU also extracts data generated after deployments. Fixed location cameras upload encrypted recordings to a server that the Seattle Information Technology Department (SITD) established. When the investigating officer needs to request video from a fixed location camera, TESU personnel assist in exporting video pertaining to a specific date range.

Washington Privacy Act, Chapter 9.73: governs the use of technologies and methods that impact privacy.

Whenever officers request to use these devices, TESU supervisors determine whether there is any reasonable expectation of privacy at the deployment location. If the deployment of a Camera System is in an area where a reasonable expectation of privacy exists, the request must be accompanied by either a consent document or a court ordered warrant to adhere to the Washington Privacy Act, Chapter 9.73. Because of the covert nature of these devices, some individuals will be unaware of the recording of visuals/images.

Reporting Limitation

The efficacy of Camera Systems and the safety of those who use them are highly dependent on the confidentiality of this technology and the manner of use. To complete this assessment, SPD provided all information and access deemed necessary by OIG for appropriate oversight. This report is intended to provide information necessary to demonstrate there is proper oversight of and knowledge about the use of Camera Systems, while maintaining certain information as confidential due to safety considerations.

1 Body wire cameras are not the same as bodycams, which are overt cameras given to Patrol officers to document interactions with members of the public. Bodycams are not classified as a surveillance technology.

SECTION A Frequency and Patterns of Use

SMC 14.18.060, § A: How surveillance technology has been used, how frequently, and whether usage patterns are changing over time.

SPD controls the use of these systems with two criteria: 1) requests must comply with local and state laws, and 2) deployments of these systems are approved only as necessary. Pursuant to RCW 9.73, TESU requires any wire request include a case number and a copy of the warrant permitting the deployment (or when applicable, third-party consent).[2] If these requirements are met, TESU further regulates use by only approving requests where: few or no other options for evidence collection exist, deployment does not pose an unreasonable risk to the requesting officers' safety, and deployment would not reveal the device.

Patterns of Use

In 2023, TESU personnel approved five deployments of body wires. In three of those instances, officers obtained warrants authorizing the collection of audio in addition to video. Officers obtained warrants for the other two deployments of camera wires and collected only video. Additionally, TESU personnel approved 110 deployments of fixed location cameras.

The nature of the criterion (community concern, SIR statement, SPD policy, etc.) or the nature of the risk

Table 1 depicts the distribution of deployments by precinct. The remaining 54 deployments pertain to mutual aid and task force uses in outside jurisdictions.

Number of Fixed Location Camera Deployments by Precinct

Search Window	Percentage of Searches
South	17
North	16
Southwest	9
West	8
East	6

Use of Biometrics or Facial Recognition Software

A concern community members expressed within the SIR was the possibility SPD may use facial recognition in conjunction with these devices. SPD personnel explained that SPD does not use or approve the use of facial recognition technology. Additionally, Seattle City Council Central Staff issued guidance on facial recognition technology in 2021, designating it a surveillance technology and subject to SMC 14.18, the Surveillance Ordinance. As of the date this report was published, SPD has not initiated the surveillance technology acquisition process for facial recognition technology.

2 In cases where a victim or other third party is involved in the creation of the video recording, a document capturing their consent must be included with the wire request. In rare cases, a warrant may not be necessary if the circumstance of the use satisfies either RCW 9.73.210 or RCW 9.73.230.

SECTION B Data Sharing with External Partners and Other Entities

SMC 14.18.060, § B: How often surveillance technology or its data are being shared with other entities, including other governments in particular.

As outlined in Section 6.1 of the SIR, SPD may share data with various external agencies and entities within legal guidelines or as required by law.1 However, OIG could not determine how often these data were shared and with whom, as there is not a centralized entity or staff member that manages data sharing of these video recordings.2 Although SPD Policy 7.010 requires these physical disks/discs containing digital recordings to be sent to the Evidence Unit (EU), the EU do not track the origin of evidence submitted to them. As a result, OIG was not able to verify that physical discs containing recordings from wires had been appropriately stored according to SPD policy.

OIG issued a recommendation in the Audio Recording Systems 2022 Annual Usage Review pertaining to the tracking of all instances of data sharing related to that technology.3 SPD concurred with that recommendation and estimated December 2024 to be the potential date of implementation. Any process developed to record instances of data sharing of that technology should also be used to record instances of data sharing from use of Camera Systems. The recommendation excludes those parties immediately involved in the criminal justice process, as there are already processes in place to track those instances of data sharing.

Recommendation 1: Create a Process to Record Data Sharing

SPD should develop a process for identifying and tracking all instances when photographs or video recordings from Camera Systems are shared with external entities excluding those immediately involved in the criminal justice process associated with the case in which the data were collected.

3 Such as prosecuting attorney's offices, insurance companies, courts, federal and state law enforcement agencies, and members of the public can access their own information pursuant to a public records request.

4 TESU controls the physical inventory of Camera Systems, oversees the extraction of recordings from wires after use, and assists in exporting recordings from fixed location cameras. Once recordings are extracted or exported, TESU stores those recordings on external disc drives and provides them directly to the case officer. For wires, TESU personnel then purge the recordings and overwrite the files on the wire multiple times to ensure complete deletion. TESU personnel do not retain copies of video files from either Camera System type; the case officer is the de facto custodian of recordings once they receive the original copy by disk or disc. As data custodians, case officers are responsible for all data sharing.

5 That report can be accessed here: https://www.seattle.gov/documents/Departments/OIG/Audits/SurveillanceTechnologyUsageReview-AudioRecordingSystems%282022%29.pdf

SECTION C Data Management and Safeguarding of Individual Information

SMC 14.18.060, § C: How well data management protocols are safeguarding individual information.

Data Retention: Body Wires

TESU personnel stated that video data from body wires are extracted by connecting the device to a dedicated workstation location in a Secure Compartmented Information Facility (SCIF). Access to the SCIF is limited to TESU personnel; only TESU personnel are authorized to extract and store recordings onto discs. The device's data are purged after each use, and no copy of the video data is stored in any manner other than on the disc. Devices are then overwritten multiple times to ensure complete deletion of the original files.

Data Retention: Fixed Location Cameras

Fixed location cameras stream directly to an encrypted server that Seattle IT created. TESU personnel administrate the server: they control access to the server, manage video exports, and purge all recordings at the end of the investigation. In some cases, TESU may grant live viewing access to case officers.

SECTION D Impact on Civil Liberties and Disproportionate Effects on Disadvantaged Populations

SMC 14.18.060, § D: How deployment of surveillance technologies impacted or could impact civil liberties or have disproportionate effects on disadvantaged populations (…).

Provided this technology is consistently deployed in compliance with state law and as described in the SIR, this technology does not appear to impact civil liberties or disproportionately affect disadvantaged populations. As stated in Section A, use of Camera Systems in protected areas is limited by Washington State law requiring either two-party consent to record or a warrant. If the Camera System would be used in an area without a reasonable expectation of privacy, then neither consent nor a warrant is necessary.

For the reviewed period, TESU reported that SPD officers included warrants authorizing all uses of their video body wires, and that none of the fixed camera deployments were deployed in protected areas. TESU personnel maintain a log of all fixed location cameras, including a snapshot of the viewing angle. OIG reviewed this log and found that all cameras did appear to be recording areas in plain view.

When used in spaces without a reasonable expectation of privacy, fixed location cameras may record bystanders with no connection to the investigation. The process for exporting relevant recordings from fixed location camera deployments lowers the likelihood of recording bystanders: officers request the exact dates and/or times pertaining to video of an incident so that the exported file excludes extraneous video.

SECTION E Complaints, Concerns and Other Assessments

SMC 14.18.060, § E: A summary of any complaints or concerns received by or known by departments about their surveillance technology and results of any internal audits or other assessments of code compliance.

Office of Police Accountability Complaints

No relevant complaints pertaining to this surveillance technology were cited in OPA complaints filed in 2023.

Customer Service Board Comments

No relevant comments pertaining to this surveillance technology were cited in Customer Service Board comments posted in 2023.

Internal Audits/Assessments

No internal audits or assessments of this surveillance technology were conducted in 2023.

SECTION F Total Annual Costs

SMC 14.18.060, § F: How surveillance technology has been used, how frequently, and whether usage patterns are changing over time.

According to TESU personnel, costs incurred for Camera Systems follow multi-year cycles, depending on contract lengths. OIG estimates $44,386.82 in total costs for licensing and maintenance of relevant cameras, based on purchase records provided by TESU.[6] Personnel costs associated with use are not possible to determine since SPD does not separately track this activity in time increments.

6 These costs include replacement materials, new computers, and evidence-grade hard drives, DVDs, and CD-Rs.

APPENDIX A: Management Response

1. SPD should develop a process for identifying and tracking all instances where data from Camera Systems are shared with external entities excluding those immediately involved in the criminal justice process associated with the case in which the data were collected.

SPD Management Response

● Concur ○ Do Not Concur

Estimated Date of Implementation: Q1 2025

Proposed Implementation Plan: SPD's TESU will implement unit procedures to document any such data sharing as a supplemental to the master case file in Mark43. Additionally, SPD's Legal Unit will track any such request made through either public disclosure or a subpoena duces tecum in any case unrelated to the case in which the data were collected.

Non-Audit Statement This review was not conducted under Generally Accepted Government Auditing Standards (GAGAS); however, OIG has followed GAGAS standards regarding the sufficiency and appropriateness of evidence.