City of Seattle

2022 Surveillance Impact Report Executive Overview

Camera Systems – Images or Non-Auditory Video Recordings

Seattle Police Department

Overview

The Operational Policy statements in this document represent the only allowable uses of the equipment and data collected by this technology.

The purpose of this Executive Summary is to highlight policies, technology and practices regarding the surveillance technologies under Council review. This document outlines information, including policies and practices, about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. All information provided here is contained in the body of the full SIR document but is provided in a condensed format for easier access and consideration.

1.0 Purpose

The SIR covers camera systems used by the Seattle Police Department (SPD) to obtain information during criminal investigations. These covert cameras are disguised and used to record specific events related to an investigation. These camera systems are utilized in two ways: when reasonable suspicion of criminal activity exists, and in areas where no reasonable expectation of privacy exists, cameras may be placed to capture plain view events. When placed in areas where a reasonable expectation of privacy exists, use of the camera systems is pursuant to the Washington Privacy Act, Chapt.9.73 RCW, and are utilized only after obtaining appropriate consent and/or legal search warrant authority.

2.0 Data Collection and Use

Until data is extracted from the covert cameras by TESU staff, the data is temporarily stored on the device. A TESU detective extracts the data onto an SPD disc and provides the disc to the requesting Officer/Detective for inclusion in the investigation file.

SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a General Offense Report. Evidence is submitted to the Evidence Unit and associated with a specific GO Number and investigation.

3.0 Data Minimization & Limitations

When reasonable suspicion of criminal activity exists, cameras may be placed to capture plain view events in areas where no reasonable expectation of privacy exists. When placed in areas where a reasonable expectation of privacy exists, use of the camera systems is pursuant to the Washington Privacy Act, Chapt.9.73 RCW, and are utilized only after obtaining appropriate consent and/or legal search warrant authority. Any consent must be informed, documented, and given by a person with the lawful control over the private area to be surveilled.

All covert cameras are managed and maintained by the Technical and Electronic Support Unit (TESU). When an Officer/Detective has obtained appropriate consent, a court order (warrant), or has established reasonable suspicion to utilize a covert camera in areas where no reasonable expectation of privacy exists, the Officer/Detective makes a verbal request to the TESU. TESU staff completes TESU's Request Form that requires a reason for the request, a case number associated with the investigation, and court order if necessary. Each request is screened by the TESU Supervisor.

Each deployment is logged, and all request forms (including court order) are maintained within TESU.

All deployments of these devices are documented by TESU and subject to audit by the Office of Inspector General and the federal monitor at any time.

If no data was collected by the device that assists in the pursuit of the criminal investigation or falls within the scope of the appropriate consent or court order, the device or server is purged in its entirety and no data is provided to the requesting Officer/Detective for the investigation file. Data collected from covert cameras is provided to the requesting Officer/Detective for the investigation and no data is retained by TESU.

4.0 Access & Security

Access

Supervisors and commanding officers are responsible for ensuring compliance with policies.

Covert cameras may only be issued/deployed by TESU detectives. All TESU staff that deploy these cameras have received vendor training in their use.

All covert cameras are managed and maintained by the Technical and Electronic Support Unit (TESU). When an Officer/Detective has obtained appropriate consent, a court order, or has established reasonable suspicion to utilize a covert camera in areas where no reasonable expectation of privacy exists, the Officer/Detective makes a verbal request to the TESU. TESU staff completes TESU's Request Form that requires a reason for the request, a case number associated with the investigation, and court order if necessary. Each request is screened by the TESU Supervisor.

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.

Only authorized SPD users can access the covert cameras or the data while it resides in the devices. Access to the systems/technology is limited to TESU personnel via password-protected login credentials.

Data removed from the system/technology and entered into investigative files is securely input and used on SPD's password-protected network with access limited to authorized detectives and identified supervisory personnel.

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.

Security

Until data is extracted from the cameras by TESU staff, the data is temporarily stored on the device. Data is also stored on the TESU secured server when installed in a fixed location. A TESU detective extracts the data onto an SPD disc and provides the disc to the requesting Officer/Detective for inclusion in the investigation file. The device is then purged, and no data is retained by TESU.

Per the Washington Secretary of State's Law Enforcement Records Retention Schedule, investigational conversation recordings are retained "for 1 year after transcribed verbatim and verified OR until disposition of pertinent case file, whichever is sooner, then Destroy" (LE06-01-04 Rev. 1).

TESU maintains a log of deployments that are available to any auditor, including the Officer of Inspector General and federal monitor.

5.0 Data Sharing and Accuracy

SPD has no data sharing partners for covert video recording device. No person, outside of SPD, has direct access to the devices or the data while it resides in the device.

Data obtained from the technology 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.

Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

Discrete pieces of data collected by covert cameras may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by SPD Policy 12.050 and 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayoral Directive, dated February 6, 2018.

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 devices.

Covert cameras capture images as they are happening in the moment. The devices do not check for accuracy, as they are simply capturing a live exchange of images. They are not interpreting or otherwise, analyzing any data they collect.

6.0 Data Retention

Unit supervisors are responsible for ensuring compliance with data retention requirements within SPD.

SPD's Investigative Support Unit reviews the log of requests and ensures compliance with all regulations and requirements.

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.