City of Seattle

2024 Surveillance Impact Report Executive Overview

Closed-Circuit Television Camera Systems

Seattle Police Department

Overview

This Executive Overview documents information about the collection, use, sharing, security, and access controls for data that is gathered through Seattle Police Department's (SPD) Closed-Circuit Television Camera systems (CCTV). All information provided here is contained in the body of the full Surveillance Impact Review (SIR) document but is provided in a condensed format for easier access and consideration.

1.0 Technology Description

The Seattle Police Department (SPD) proposes closed-circuit television (CCTV) camera systems to deter and detect criminal activity. CCTV camera systems contribute to averting harm to individuals and property and reducing crime by assisting in collecting evidence related to serious and/or violent criminal activity as part of investigations. The CCTV camera systems are proposed to be installed at locations where gun violence, human trafficking, and persistent felony crime is concentrated. The cameras will face toward the street, sidewalk, and other public areas. Signs acknowledging use of the cameras will be posted. Privately-owned security systems will be able to share video streams of storefronts and areas where the public has access with SPD.

2.0 Purpose

Serious felony crimes are often concentrated at specific geographic locations in Seattle and long-time efforts to prevent these crimes have not been consistently successful. Police effectiveness is further hindered due to unprecedented patrol and investigations staffing shortages in the Seattle Police Department.

The purpose of the CCTV pilot program is to mitigate unprecedented patrol and investigations staffing shortages by leveraging evidence-based and industry-standard technologies to deter and detect persistent felony criminal behavior, gun violence, and human trafficking at specific places where crime is concentrated.

CCTV camera systems contribute to averting harm to individuals and property and reducing crime by assisting in collecting evidence related to serious and/or violent criminal activity as part of investigations. For example, CCTVs could be used to review a firearms-related homicide to identify the suspect and provide information that would provide justice for the victims and remove deadly weapons from the street.

3.0 Data Collection and Use

Until data is extracted from the CCTV system's local storage, the data is temporarily stored on the device. Video may only be extracted for legitimate law enforcement purposes, as governed by SPD Policy 12.050. For most CCTV systems, the recordings are kept locally for 30 days, and not retained for a longer duration unless manually extracted by authorized personnel via the video management system software. Private, 3rd party video, if used, will be subject to the 30-day retention on SPD storage, unless used as evidence for a criminal investigation.

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

4.0 Data Minimization & Retention

In order to minimize inadvertent collection of data, the CCTV cameras will only be placed to capture events in plain view in public areas where as a matter of law no reasonable expectation of privacy exists.

CCTV video recordings are automatically purged by the system after 30 days unless the footage holds evidentiary value related to criminal activity or assists in the pursuit of a criminal investigation.

Additionally, the CCTV camera systems will maintain a complete audit log of activities (including but not limited to personnel access and video extraction logs) and would be subject to an audit by the Office of Inspector General at any time.

5.0 Access & Security

Access

Only authorized SPD and OIG users can access the CCTV camera feed or the data while it resides on the devices. Access to the systems/technology is limited to authorized personnel via password-protected login credentials.

Data extracted 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.

Access to video evidence 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.

Data collected on 3rd party systems will be accessed by SPD personnel using the above guidelines, but will be owned by the 3rd party, unless taken into evidence.

Security

The data will be encrypted at rest (where it is stored) and in transit (either through vendor encryption or through VPN on the City network side) as it's being transmitted from the camera device to the storage system, server, or cloud. Per the Washington Secretary of State's Law Enforcement Records Retention Schedule, the required records retention period for surveillance video that does not involve a specific incident is "Retain for 30 days after last recording or until determined that no security incident has occurred, whichever is sooner, then Destroy."

Audits from the Office of Inspector General or other official auditors will be allowed as needed.

6.0 Data Sharing and Accuracy

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.

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 CCTV 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.

7.0 Equity Concerns

The mission of the Seattle Police Department is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional, and dependable police services. SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior and other accountability measures. This pilot will be data-informed and guided. It will terminate if data suggests the technology is ineffective. Utilizing the abilities of the Performance Analytics and Research Unit, the Seattle Police Department has a plan to actively manage performance measures reflecting the "total cost of ownership of public safety," Equity, Accountability, and Quality ("EAQ"), which includes measures of disparate impact and over policing. In addition to a robust Continuous Intervention Assessment designed to inform, in real-time, the active development of a safer and more effective, Evidence-Based Policing (EBP) competency, the EAQ program assures just right policing is achieved with undue collateral harm.

It's worth noting that many factors can contribute to disparate impacts in policing, most of which occur early in a person's life, long before there is engagement with the police. For example, systems and policies that perpetuate poverty, the failure to provide children with the strong and fair start they deserve in the crucial birth-to-five years, inadequate public education, and a lack of economic opportunity can all contribute to disparate outcomes. In addition, family dynamics and peer pressure can also create negative outcomes. We recognize these factors and strive to do our part to mitigate

them, but we can't expect our police officers by themselves to cure these contributory factors. However, we do expect our officers to do their jobs respectfully and fairly as they interact with community members.

These technologies are location-specific, with a place-based focus, meaning they will record people who choose to be in a public place where the technologies are being used. This mitigating factor reduces, to an extent, the possible disparate impact of potential police actions.