Seattle Office of Inspector General

Surveillance Technology Usage Review Tracking Devices 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

Tracking Devices refers to geolocation trackers that transmit location information on a vehicle during an investigation. Deployment of Tracking Devices requires either a warrant or consent agreement. Tracking Devices contain both hardware and software elements. The physical device is fixed to a target vehicle and periodically measures GPS coordinates (longitude and latitude), temperature, the device's battery status, and alerts to any tampering, removal, or power shut off. Officers deploying Tracking Devices can remotely adjust the frequency of these periodic measurements. The software translates these data into a map showing locations and movements over time. Data generated during a deployment are encrypted and streamed to a vendor cloud server that personnel from the Technical and Electronic Support Unit (TESU) administrate.

Reporting Limitation

The efficacy of Tracking Devices and the safety of those who use them is highly dependent on confidentiality about the specific technology and the manner of use. To complete this assessment, SPD has 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 Tracking Devices, while maintaining certain information as confidential, due to safety considerations.

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.

TESU reports approving 52 deployments of tracking devices in 2023: 51 deployments for the Investigations Unit and 1 for Patrol. SPD controls the use of tracking devices in two ways:

- Requests must comply with Washington State privacy laws (RCW 9.73) and SMC 14.12, and
- TESU personnel must determine that other methods of evidence collection evidence are infeasible.

Whenever TESU personnel receive a request that satisfies these two requirements, a supervisor confirms these conditions in addition to confirming that the request includes either a warrant or a consent agreement. TESU personnel support the requesting officer to deploy Tracking Devices.

Example Cases

Dealing in Depictions of a Minor Engaged in Sexually Explicit Conduct

SPD received a cybertip about a user uploading videos containing depictions of minors engaged in sexually explicit conduct. Officers reviewed the uploaded content, established probable cause, and obtained a search warrant for the user's devices and online accounts. Officers obtained an additional search warrant to install a vehicle tracking device because they collected evidence that the subject may be physically transporting hard drives containing content depicting minors engaged in sexually explicit conduct.

Unlawful Possession of a Firearm/Robbery

A victim reported being robbed at gunpoint by multiple subjects. When the victim fled by vehicle, one of the subjects had dropped a firearm inside it. SPD officers identified the original purchaser of the firearm and established probable cause for a warrant for social media account information. With additional information, officers then established probable cause that the purchaser of the firearm was distributing/selling firearms illegally; they obtained a warrant for a Tracking Device and made an arrest.

Narcotics Investigation

Officers obtained a warrant to install a tracking device on the vehicle of a suspected narcotics dealer. Officers tracked the subject, observed a narcotics sale, and subsequently arrested the subject.

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, because there is not a centralized entity or staff member that manages data sharing of these video recordings. At the end of the deployment, TESU personnel download the tracking data from the vendor cloud server and store them on an external disc drive. Then they provide the external disc drive directly to the case officer. The case officer becomes the de facto data custodian and is manages any data sharing. SPD Policy 7.010 requires that all evidence must be sent to the Evidence Unit (EU), but the EU does not track the origin of evidence submitted to them. As a result, OIG was not able to verify that physical discs containing tracking data 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 where case officers share data generated from deployments of that technology. 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 Tracking Devices. 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 Tracking Process

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

1 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.

SECTION C — Data Management and Safeguarding of Individual Information

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

The physical inventory of Tracking Devices is secured within a Sensitive Compartmented Information Facility (SCIF), which restricts unauthorized personnel from entering. Only some personnel of TESU have access to the SCIF. Once deployed, Tracking Devices broadcast data over cellular networks with an end-to-end encryption to cloud storage administrated by and accessible to TESU personnel. Data generated during a deployment are stored directly into the vendor's cloud server. TESU personnel reported that the vendor agreement forbids the vendor from sharing these data without either authorized consent from SPD or a subpoena from another law enforcement agency. TESU personnel administrate the server: they control access to the server, manage data exports, and export/purge all data at the end of the investigation.[2] In some cases, TESU may grant live viewing access to case officers. At the end of the tracking schedule, authorized personnel (often TESU but can also be officers trained in deploying tracking devices) retrieve the device and return it to TESU. Not all Tracking Devices are recovered; in some cases, Tracking Devices may be transported over state lines or cross into Canada or Mexico.

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 (…).

Warrantless or unauthorized uses constitute the most significant risk associated with Tracking Devices. To mitigate potential misuse, TESU personnel control the physical inventory and oversee installation of tracking devices. At the time of a request to use Tracking Devices, TESU personnel

1. Confirm that the requesting officer has obtained and presented a warrant authorizing the use of Tracking Devices, and
2. Determine whether the requesting officer has had prior use training.

TESU personnel then provide either support for the deployment if the case officer has received prior training or directly manage the installation and monitoring if the case officer has not received prior training. OIG reviewed nine case files involving Tracking Devices and found that warrants authorized all nine deployments. Additionally, TESU personnel reported that they reviewed warrants authorizing all 52 deployments.

2 TESU personnel also reported that the vendor agreement states that the vendor will back up stored tracking data for one year in case of accidental deletion.

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 Tracking Devices follow multi-year cycles, depending on contract lengths. OIG estimates $13,736.87 in total costs for licensing, maintenance, and evidence-grade discs, based on purchase records provided by TESU. Personnel costs associated with use are not possible to determine since SPD does not separately track this activity in time increments.

APPENDIX A: Management Response

1. SPD should develop a process for identifying and tracking all instances where data from Tracking Devices 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.