City of Seattle

2022 Surveillance Impact Report Executive Overview

Tracking Devices

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

Seattle Police Department (SPD) utilizes geolocation trackers to track and locate vehicle information during criminal investigations. Geolocation trackers are devices that SPD utilizes as a tool to locate and track the movements and locations of vehicles. Trackers are utilized only after obtaining legal authority via a court order or consent, and once the consent or terms of the order have expired all data collected is maintained only in the investigation file.

Tracker technology directly tracks and collects location information of vehicles, and indirectly tracks and collects the same information about individuals. Despite the requirement that trackers be utilized only pursuant to a search warrant or with consent, this could raise potential privacy concerns, such as general surveillance or tracking of the general public.

2.0 Data Collection and Use

Tracking technology consists of interconnected hardware and software. The hardware, a real-time tracking and data logger, is a compact unit that adheres to or rides along with a targeted vehicle. These trackers are location tracking devices that report latitude and longitude coordinates on a pre-determined schedule that can be adjusted by users remotely. The hardware also logs high temperature alerts, low battery alerts, device removal, power/shut down alerts and battery level. The software consists of an online portal that collects the information captured by the hardware, and allows for graphic representation of that information, including mapping of locations and movement, alerts for established events (i.e., a vehicle has moved beyond an established boundary, etc.), and scheduling of “check-ins” (the reporting interval records the locations set in seconds, minutes or hours).

The data captured by a device is downloaded out of the online portal after the conclusion of a tracking schedule (due to the expiration of a search warrant or an investigation) and is provided to the Officer/Detective leading the investigation. The data is then purged from the software and the hardware is reset for future deployment, meaning no data captured is stored in any location other than the investigation file. This is in keeping with Washington State Retention Schedule for Records Documented as Part of More Formalized Records (GS2016-009). It requires that such records be retained "until verification of successful conversion/keying/transcription then destroy."

In the beginning of 2020, cellular providers in the USA announced that the existing 3G cell networks would be decommissioned in 2022 as the newer 5G networks were phased in. Many of the existing SPD tracking devices were tied to the older 3G network and have been or will need to be replaced with similar-functioning updated 5G versions of the same location tracking technology.

Officers/Detectives obtain search warrants or consent to deploy vehicle tracking devices. The information is gathered consistent with SPD Policy 6.060, such that it does not reasonably 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; the right to petition government for redress of grievances; and the right to privacy."

Vehicle tracking data is temporarily stored by third-party vendors (as described above), until the schedule for collection of data has expired (per the search warrant or consent authorities), at which time all data collected is downloaded and attached to the investigation file. This is in keeping with the Washington State Local Government Common Records Retention Schedule Disposition Authority Number GS2016-009 Rev. 0, governing retention of records documented as part of more formalized records, and requiring that SPD "retain until verification of successful conversion/keying/transcription, then destroy."

Physical objects involved in tracking deployments are unmarked as their purpose is in support of covert investigations.

3.0 Data Minimization & Limitations

Each application of tracking technology is screened by the TESU supervisor and held to a legal standard of consent or court issued search warrant. The process is as follows: one member of the Unit is tasked with receiving requests for deployment (including a Request Form that must be completed by the requesting Officer/Detective, which includes the active search warrant number). A TESU supervisor then approves the request before a tracking device is assigned and deployed to an investigating Officer/Detective. All requests are filed with TESU and maintained within the unit, available for audit.

Equipment deployment is constrained to the conditions stipulated by the consent or court order providing the legal authority. All deployments of tracking technology are documented and subject to audit by the Office of Inspector General and Federal Monitor at any time.

Data collected is provided to the case Detective for the investigation and no data is retained by the Technical and Electronic Support Unit.

4.0 Access & Security

Access

Only authorized SPD users can access the vehicle tracking devices or the data while it resides in the system. Access to the vehicle tracking systems/technology is specific to system and password-protected.

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

Unit supervisors are responsible for screening all deployments as well as ensuring that staff receive adequate training specific to the involved technologies.

TESU personnel are trained by the vendor in the use of the hardware and software. When an Officer/Detective requests and deploys a tracking device from TESU, TESU personnel train the Officer/Detective in the tracker's use.

If the geolocation tracking device is being utilized pursuant to a search warrant, the warrant dictates the scope and parameters of the information collected.

SPD Policy 6.060 requires 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, including freedom of speech, press, association, and assembly; liberty of conscience; the exercise of religion; the right to petition government for redress of grievances; and the right to privacy."

Security

Data is securely stored by the vehicle tracking technology vendor and will be transferred to the case investigator only via Seattle Police Department owned and authorized technology. At that time, vehicle tracking data collected by the tracking device is downloaded from the vendor software and resides only with the investigation file.

5.0 Data Sharing and Accuracy

No person, outside of SPD, has direct access to the tracking units 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.

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 these tracking devices 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 executed research and confidentiality agreements as provided by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the devices. Data sharing is necessary for SPD to fulfill its mission of contributing to crime reduction by assisting in collecting evidence related to serious and/or violent criminal activity as part of investigation, and to comply with legal requirements.

6.0 Data Retention

SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a General Offense (GO) Report.

All information must be gathered and recorded in a manner that is consistent with SPD Policy 6.060, such that it does not reasonably infringe upon "individual rights, liberties, and freedoms secured by the Constitution of the United States and of the State of Washington, including, among others, the freedom of speech, press, association and assembly; liberty of conscience; the exercise of religion; and the right to petition government for redress of grievances; or violate an individual's right to privacy."

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.

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

SPD's Intelligence and Analysis Section reviews the audit logs 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.