Seattle Office of
Inspector General

Surveillance Technology Usage Review
GeoTime (2023)

As Required by Seattle Municipal Code 14.18.060

September, 2024

Purpose

Surveillance Ordinance Requirement

Per Seattle Municipal Code 14.18.060, OIG is required to annually review the Seattle Police Department's (SPD) compliance with the requirements of Chapter 14.18 in its use of surveillance technologies.
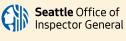
GeoTime No Longer a Surveillance Technology

In September 2024, Seattle IT removed GeoTime from the City's Master List of Surveillance Technologies.[1] While OIG is issuing this final annual report pursuant to SMC 14.18.060, the report will not include recommendations related to compliance with the relevant Surveillance Impact Report (SIR). Additionally, any outstanding recommendations from prior Annual Usage Reviews will be closed.

Table of Contents

---

1 https://clerk.seattle.gov/~CFS/CF_323176.pdf

Technology Description

GeoTime is a visual analysis and mapping software. It visually displays events over time based on geodata (longitude and latitude) procured during an investigation. GeoTime produces two- and three-dimensional maps of call records and cell site locations, which can be used in prosecutions. Examples are provided below. Personnel from the Technical and Electronic Support Unit (TESU) report that SPD owns several licenses for GeoTime, and there is one detective who is the primary user of GeoTime. Throughout this report that detective is referred to as the "subject-matter expert" or "SME." This SME is responsible for most of the departmental use of GeoTime.

Figure 1. A 2-dimensional map with time stamps placed onto each point to indicate movement
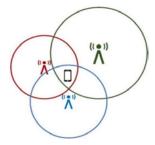

Source: Penlink's GeoTime website.

Call Data Records (CDRs): are cellular network records measuring time, signal strength, and distance between the device at the cellular tower.

Triangulation:

GeoTime Uses Call Data Records (CDRs)

Call records encode geodata using cellular triangulation, which calculates the location of a cellular device based on the intersection of signals transmitting from at least three cellular towers. Distance to each of the three cellular towers is determined by measuring the speed at which a ping from the tower travels to the cellular device and then back to the tower. Triangulation is the comparison of the three towers' distances to the device, forming a small area where the cellphone was or is located. Cellular devices automatically connect to towers, and pings typically occur on short intervals. Cellular network providers record these data and refer to them as call data records (CDRs). GeoTime is designed to easily visualize CDRs.

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.
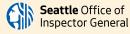
General Use Patterns

SPD personnel reported at least 73 GeoTime uses in 2023.[2] The GeoTime SME accounts for 52 of these cases. Section 2.1 of the SIR states that GeoTime is used for "complicated criminal investigations." OIG reviewed six cases where GeoTime was used. These cases involved multiple suspects and incidents, tended to be felony investigations, and involved firearms, warrants, and forensics. In all six cases, the GeoTime SME contributed to the investigation by obtaining a warrant for CDRs and analyzing those records using GeoTime.

Example Use Cases

Robbery/Burglary Case

A series of armed robberies and burglaries occurred over the course of several months with similar incident details. Detectives identified cellular devices present in multiple incidents, which provided probable cause of involvement. Search warrants for CDRs obtained data that was then analyzed in GeoTime. Other search warrants recovered mobile devices and their data, which corroborated locational data obtained from CDRs. Detectives uncovered a criminal conspiracy with multiple suspects engaging in armed robberies and burglaries throughout Seattle.

---

2 This figure – 73 – is an estimation. GeoTime does not automatically record use logs or capture information about cases. TESU personnel assisted OIG by interviewing personnel authorized to use GeoTime about how frequency they used it in 2023.

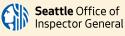|	
Hate Crime Case	A place of worship reported offensive graffiti and theft. Security footage at the place of worship captured the incident and was shared with SPD and media, which resulted in a tip about the suspect's potential identity. Detectives followed up with the person who registered the tip and established probable cause for a search warrant for CDRs. A detective analyzed the data using GeoTime and confirmed the suspect's cellphone location matched the location of the initial vandalism incident. Detectives obtained additional warrants for the suspect's cellphone and their arrest.
Robbery/Vehicle Theft/ Domestic Violence Case	A victim reported being robbed at gunpoint. One of the victim's stolen items was a cellphone. Detectives obtained private security surveillance footage of the incident, which recorded the suspects' vehicle and likeness. In another jurisdiction, a stolen vehicle was recovered with the initial victim's stolen phone in it. In yet another jurisdiction, 911 dispatch received a domestic violence-related call pertaining to the same address as the suspect in the stolen vehicle incident. Detectives established probable cause for robbery from the stolen vehicle case and obtained a warrant for CDRs for the armed robbery. GeoTime analyzed the CDRs and detectives determined the phone was present in multiple incident locations.

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.	GeoTime analyzes locational data collected during investigations, and its primary outputs are 2- and 3-dimensional maps. As outlined in Section 6.1 of the SIR, SPD may share data or maps analyzed using GeoTime with various external agencies and entities within legal guidelines or as required by law.[3] The GeoTime SME reports that any data sharing occurs in the process of discovery during a prosecution; furthermore, the SME reports that the maps are generally more likely to be shared with judicial parties than the underlying data.

---

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

SECTION C	Data Management Protocols and Security

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

Access and Transaction Logs Are Not Stored as Described in the SIR
Section 3.1 of the SIR states that "access for personnel into the system [GeoTime] is predicated on state and federal law governing access to Criminal Justice Information Services (CJIS). This includes [...] audit of access and transaction logs within the system." However, TESU personnel and the detective who is the primary user of GeoTime report that GeoTime is not capable of recording access and transaction logs. Despite this, SPD personnel were able to produce records and cases that used GeoTime from their own administrative records keeping.

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 (...).

GeoTime is a Controlled Forensic Tool
As a forensic tool, data analyzed using GeoTime are obtained through controlled processes that mitigate civil liberties impacts and do not appear to disproportionately affect disadvantaged populations. Section 3.2 of the SIR states that the data analyzed using GeoTime are obtained under the execution of court ordered warrants, "including data from cellular providers and from data extracted from mobile devices." The GeoTime SME reported that locational data used in GeoTime are most often procured through warrants to cellular network providers.[4] In a qualitative sample of six cases involving GeoTime, all data analyzed by the surveillance technology had been obtained by a warrant. Most data were CDRs but in one case GeoTime analyzed data extracted from a mobile device.

---

4   GeoTime has a feature allowing for manually entered information, but this is used in conjunction with locational data to add context or important points in time determined during the investigation. The SME reports that – while possible – they rarely use GeoTime to analyze data obtained from Computer, Cellphone, & Mobile Device Extraction Tools (CCMDE Tools). The use of extracted cellphone application data is an example in which GeoTime may be used to analyze data obtained from CCMDE Tools. Some cellphone applications record locational data, which can be used in conjunction with call records to recreate a mobile device's movement through Seattle.

| **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.
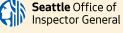
Internal Audits or Assessments
No internal audits or assessments of this surveillance technology were conducted in 2023.

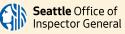| **SECTION F** | **Total Annual Costs** |

SMC 14.18.060, § F: Total annual costs for use of surveillance technology, including personnel and other ongoing costs.

According to TESU personnel, costs incurred for Tracking Devices follow multi-year cycles, depending on contract lengths. Based on purchase records provided by TESU personnel, OIG estimates $8,327.35 in total costs for GeoTime licensing and evidence-grade discs. Personnel costs associated with use were not possible to determine since SPD does not separately track this activity in time increments.

APPENDIX A: Management Response

SPD provided that it has no substantive response to this review as no matters requiring a response are raised, but SPD appreciates the opportunity to review.

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.