City of Seattle

2022 Surveillance Impact Report Executive Overview

GeoTime

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

GeoTime is geospatial analysis software that allows the visual analysis of events over time. Utilizing geodata, such as latitude and longitude, procured during criminal investigations, investigators use GeoTime to create specialized 2 and 3 dimensional maps of call records and cell site locations. These maps allow investigators to see patterns in the existing data that might not be interpreted through other methods.

GeoTime is used to aid in the investigation of crime by helping detectives analyze location information over time and present patterns in the data. Analyzing observations over time and geography is a common task but typically requires multiple, separate tools. GeoTime is an application which has been developed to visualize the spatial inter-connectedness of information over time and geography. A PIA is required because some members of the public may be concerned that this software could be used to track members of the community who are not associated with the investigation.

2.0 Data Collection and Use

GeoTime does not collect information or data. It is a tool used to aggregate and analyze data manually input by investigators and exports complex geospatial maps which users save into locally stored investigation files. No information is saved inside the GeoTime tool.

3.0 Data Minimization & Limitations

GeoTime is only used during the investigation of crimes by SPD detectives. Access for personnel into the system is predicated on state and federal law governing access to Criminal Justice Information Services (CJIS). This includes pre-access background information, appropriate role-based permissions as governed by the CJIS security policy, and audit of access and transaction logs within the system. All users of GeoTime must be CJIS certified and maintain Washington State ACCESS certification.

GeoTime does not collect information or data. It is a tool used to aggregate and analyze data manually input by investigators and exports complex geospatial maps which users save into locally stored investigation files. No information is saved inside the GeoTime tool.

4.0 Access & Security

Access

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

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.

SPD Policy 12.050 defines the proper use of criminal justice information systems.

GeoTime does not collect information or data. It is a tool used to aggregate and analyze data manually input by investigators and exports complex geospatial maps which users save into locally stored investigation files. No information is saved inside the GeoTime tool.

The files created with GeoTime are stored within investigation files for the case.

Access to GeoTime requires SPD personnel to log in with password-protected login credentials which are granted to employees with business needs to access GeoTime. These employees are ACCESS and CJIS certified.

According to the CJIS security policy, “The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.”

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.

Security

GeoTime does not collect information or data. It is a tool used to aggregate and analyze data manually input by investigators and exports complex geospatial maps which users save into locally stored investigation files. No information is saved inside the GeoTime tool.

SPD’s Audit, Policy and Research Section (APRS) can conduct an audit of the any system at any time. In addition, the Office of Inspector General can access all data and audit for compliance at any time.

SPD conducts periodic reviews of audit logs and they are available for review at any time by the Seattle Intelligence Ordinance Auditor under the City of Seattle Intelligence Ordinance. The software automatically alerts users of data that must be deleted under legal deletion requirements such as 28 CFR Part 23.

5.0 Data Sharing and Accuracy

No person, outside of SPD, has direct access to GeoTime.

Data analyzed by GeoTime 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 analyzed by GeoTime 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 analyzed by this application.

Individuals may request records pursuant to the PRA, and 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.

6.0 Data Retention

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

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.

SPD policy contains multiple provisions to avoid improperly collecting data. SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a GO Report. SPD Policy 7.090 specifically governs the collection and submission of photographic evidence. Evidence is submitted to the Evidence Unit and associated with a specific GO Number and investigation. And, SPD Policy 7.110v governs the collection and submission of audio recorded statements. It requires that officers state their name, the Department name, the General Offense number, date and time of recording, the name of the interviewee, and all persons present at the beginning of the recording.

Additionally, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

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.

Per the CJIS Security Policy:

“5.8.3 Digital Media Sanitization and Disposal The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.”