SEATTLE CITY COUNCIL
CENTRAL STAFF

February 6, 2023

# MEMORANDUM

**To:** Economic Development, Technology and City Light Committee
**From:** Lise Kaye, Analyst
**Subject:** Council Bill 120502 - Authorizing approval of uses and accepting the surveillance impact report for the Seattle Police Department's use of GeoTime

On Wednesday, February 8, 2023, the Economic Development, Technology and City Light Committee will discuss Council Bill (CB) 120502 This CB would approve the Seattle Police Department's (SPD's) continued use of GeoTime and accept the Surveillance Impact Report (SIR) and an Executive Overview for these technologies.

The bill is intended to meet the requirements of Seattle Municipal Code Chapter 14.18, Acquisition and Use of Surveillance Technologies, which requires City of Seattle departments intending to acquire surveillance technology to obtain advance Council approval of that acquisition and of a surveillance impact report (SIR).[1] Departments must also submit a SIR for surveillance technology in use when Ordinance 125376 was adopted in 2017 (referred to in the ordinance as "retroactive technologies"), but failure to approve an ordinance for a retroactive technology does not require SPD to discontinue its use. Councilmembers may choose to amend the ordinance to request additional information or to request that SPD develop new and/or revised operational policies, which, if implemented, could restrict or modify the application of certain technologies.

This memorandum describes SPD's use of GeoTime, summarizes recommendations from the Community Surveillance Working Group, describes whether and how each recommendation is addressed in the SIR and/or by current law, and summarizes responses by the Chief Technology Officer (CTO) and/or SPD. Finally, the memorandum identifies policy issues for Council consideration.

## GeoTime

SPD uses GeoTime software during criminal investigations to help analyze location information over time and present patterns in the data. These linkages allow users to simultaneously visualize geospatial, temporal, and linked data to see activities and events unfold over time.[2] Investigators input data into GeoTime, which then creates maps that link call records and cell site locations. Users may save the exported maps into locally stored investigation files. No information is saved in the software. According to the SIR, GeoTime increases SPD's efficiency in accessing and analyzing information obtained under execution of court ordered warrants, including data from

[1] The Executive Overview summarizes SPD's allowable uses of GeoTime. See also the memorandum summarizing process for developing a Surveillance Impact Report (SIR), consistent with Ordinances 125376 and 125679 and Ordinance 108333, Seattle's "Intelligence Ordinance," adopted in 1979 and amended in 1982 via adoption of Ordinance 100572.
[2] See https://www.esri.com/partners/uncharted-software-i-a2T70000000TNaSEAW/geotime-5-3-a2d70000000VTUWAA4

cellular providers and from data extracted from mobile devices. According to Appendix E in the SIR (Questions and Departments Responses) SPD does not use the social media analysis functionality provided in GeoTime. In September 2022, GeoTime was acquired by Ontario-based PenLink, Ltd, a developer of communications and digital evidence software for law enforcement.

SPD reports that the department mitigates potential civil liberties risks, including the risk of unlawful surveillance and the risks of racial or ethnicity-based bias from the use of these systems and associated data sharing, storage and retention through its warrant parameters, evidence procedures, and anti-bias policies. The Racial Equity Toolkit does not identify metrics to be used as part of the CTO's required annual equity assessments.

Surveillance Working Group Recommendations and CTO Response

The Community Surveillance Working Group's Impact Assessment for GeoTime makes 19 recommendations to Council. The CTO's response finds that the "policy, training and technology limitations enacted by SPD provide adequate mitigation for the potential privacy and civil liberties concerns raised by the Working Group." The CTO's response does not specifically address the Working Group's recommendations, but it identifies relevant citations from the SIR for each of the "key concerns" raised by the Working Group.

Table 1 summarizes which recommendations have been addressed in the SIR and/or are a matter of state law, and which would require a revised SPD policy and/or procedure. Attachment 1 provides additional detail on whether the SIR as drafted or current law addresses the Working Group's recommendations as well as relevant responses from the CTO and/or SPD.

*Table 1. Surveillance Working Group (SWG) Recommendations Addressed in SIR and/or State Law*

| Addressed in SIR or State Law | SWG Recommendation(s) – Abbreviated |
|---|---|
| Would require revised SPD policy and/or procedure and updated SIR | #4. Limit data input to data collected via warrant<br>#8. Analyze impacts of any GeoTime outputs<br>#9. Validate data before it is entered into GeoTime<br>#10. Analyze accuracy and analytical data generated by GeoTime<br>#11. Delete data from GeoTime after outputs are exported<br>#12. Disclose/log recipients of and the circumstances pertaining to shared GeoTime data<br>#15. Keep audit log of user actions<br>#17. Restrict vendor ownership and use of data inputs and outputs; properly store such data<br>#18. Disclose usage per year<br>#19. Prohibit SPD from signing a non-disclosure agreement with the vendor |
| Would be inconsistent with state law | #6. Disclose use of GeoTime to individual facing charges (or to their representative) |

| Addressed in SIR or State Law | SWG Recommendation(s) – Abbreviated |
|---|---|
| See citations in Attachment A | #3. Define incident types and allowed uses<br>#5. Disclose all data sources input into GeoTime<br>#7. Require strong access controls<br>#13. Securely share and properly delete shared data<br>#14. Provide adequate training, including a privacy component<br>#16. Produce publicly-available annual audit report |
| Neither is described in the SIR as an authorized use and a change would require Council approval of an updated SIR | #1. Prohibit use for predictive policing<br>#2. Prohibit use for dragnet social media analysis |

**Policy Considerations**

Central Staff has identified the following potential policy considerations and options.

1. Annual equity assessment metrics.

   SPD has not yet finalized metrics to be used in evaluating use of GeoTime as part of the CTO's annual equity assessments. These assessments are intended to play a key role in determining whether the City's surveillance legislation is meeting the goals of the Race and Social Justice Initiative.

   Options:

   A. Request a report on the proposed metrics by a date certain.

   B. Take no action.

2. Mitigation of Civil Liberties Impacts.

   The SIR provides only a boilerplate reference to SPD's general anti-bias policing policies as providing mitigation against the risk of disproportionate surveillance and/or civil liberties impacts. In the absence of data tabulating the frequency of use of GeoTime and the corresponding incident types, it is not possible to evaluate whether the technology is being used inequitably.

   Options:

   A. Request that SPD report on the deployment of GeoTime by incident type and location for the past three years and identify any disproportionate impacts.

   B. Take no action.

**Attachments:**

1. Surveillance Working Group Working Group Recommendations: SIR Citations, Current Law, and CTO and SPD Responses

cc: Esther Handy, Director
Aly Pennucci, Deputy Director
Brian Goodnight, Supervising Analyst

SEATTLE CITY COUNCIL
CENTRAL STAFF

## Attachment 1: Surveillance Working Group Working Group Recommendations: SIR Citations, Current Law, and CTO and SPD Responses

| Working Group Recommendation | Whether/How Addressed by SIR, CTO or SPD and/or Current Law |
|---|---|
| 1. Prohibit the use of GeoTime for predictive policing. | Not described in the SIR as an authorized use of camera systems and a change would require Council approval of an updated SIR |
| 2. Prohibit use of GeoTime for dragnet social media analysis. | Not described in the SIR as an authorized use of camera systems and a change would require Council approval of an updated SIR. |
| 3. Clearly define purpose and allowable uses and limit use of GeoTime to that purpose and those allowable uses. Specify incident types for which GeoTime may be used. | **SIR §1, 3 and 4 provide this information.**<br>SMC 14.12 (the "Intelligence Ordinance) governs the collection of data for a criminal investigation.<br>The SIR does not limit the use of these tools to specific incident types. |
| 4. Establish a policy that only data collected via a court-ordered search warrant can be input into GeoTime. | **SIR §3.2** The data analyzed using GeoTime is obtained by investigators under the execution of court ordered warrants, including data from cellular providers and from data extracted from mobile devices (see SIR- Computer, Cellphone, & Mobile Device Extraction Tools). |
| 5. Disclose all specific data sources inputted into GeoTime. | **SIR §3.2** The data analyzed using GeoTime … includes data from cellular providers and from data extracted from mobile devices.<br>**Appendix E.** SPD does not use the social media analysis functionality provided in GeoTime. |
| 6. Use of i2 GeoTime must be disclosed to the individual or the legal representative of an individual facing charges for which GeoTime was used in SPD's investigation. | **SPD Policy Manual 12.050.** An individual's right to access and review of their criminal history record information shall not extend to data contained in intelligence, investigative, or other related files and shall not be construed to include any information other than that defined as Criminal History Record Information by RCW 10.97.030. |
| 7. Require strong access controls for licensed workstations, internet accessible portals and GeoTime output and analyses. | **SIR §3.1** 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.<br>**CTO's Response:** As stated in the SIR, access to GeoTime requires authenticated access to SPD personnel with a business need to access GeoTime. These employees are CJIS certified to handle sensitive criminal justice information. Access and storage for information contained within GeoTime is also governed by the CJIS Security Policy. |
| 8. Impacts of any GeoTime outputs must be analyzed. | This subject is not addressed in the SIR. |
| 9. SPD must validate data before inputting it into GeoTIme. | **SIR Appendix E.** "The accuracy of the input … is independently identified by the investigator through the process of investigation." |
| 10. Analyze the accuracy and data of analyses generated by GeoTime. | This subject is not addressed in the SIR. |

| Working Group Recommendation | Whether/How Addressed by SIR, CTO or SPD and/or Current Law |
|---|---|
| 11. SPD must delete originally collected, pertinent data from GeoTime after GeoTime outputs are exported. | **CTO's Response:** Information gathered from GeoTime would be contained in an investigative file and would be governed as evidence, which is stored securely in line with SPD policy, CJIS Security Policy, and other state and federal regulations relating to handling of law enforcement data. |
| 12. Disclose/log recipients of and the circumstances pertaining to shared GeoTime data inputs and outputs. | This subject is not addressed in the SIR.<br>*Per SPD, the Department does not keep this type of log.* |
| 13. Securely share and properly delete data inputs or outputs shared with third parties. | **SIR §6.0 addresses data sharing with third parties.** |
| 14. Provide adequate training for all personnel who use these tools, including a privacy component. | **SIR §7.2** Users of GeoTime undergo training on the use of the software.<br>All authorized users of GeoTime must be CJIS certified and must maintain Washington State ACCESS certification.<br>SPD Policy 12.050 mandates that all employees receive Security Awareness Training (Level 2), and all employees also receive City Privacy Training. All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), many of which contain specific privacy requirements. 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. |
| 15. Keep an audit log of user actions within GeoTime | **CTO's Response:** SPD has existing audit functionality with the Office of Inspector General, unit supervisors, or the federal monitor. Audit, Policy & Research Section personnel can also conduct audits of all data collection software and systems. Additionally, the Surveillance Ordinance does mandate yearly auditing of these technologies by the Office of Inspector General and the IT department in some circumstances. |
| 16. Produce publicly available annual audit report about SPD's use of GeoTime | **CTO's Response:** The Surveillance Ordinance mandates yearly auditing of these technologies by the Office of Inspector General and the IT department in some circumstances. |
| 17. The software vendor does not own and may not use or retain data inputs or outputs; any data inputs and outputs should be properly stored. | **CTO's Response:** Information gathered from GeoTime would be contained in an investigative file and would be governed as evidence, which is stored securely in line with SPD policy, CJIS Security Policy, and other state and federal regulations relating to handling of law enforcement data. |
| 18. SPD must disclose the number of incidents per year for which GeoTime is used. | This subject is not addressed in the SIR. |
| 19. Prohibit SPD from signing a non-disclosure agreement with the vendor. | This subject is not addressed in the SIR. |