SEATTLE CITY COUNCIL
CENTRAL STAFF

April 19, 2022

M E M O R A N D U M

To: Economic Development, Technology and City Light Committee
From: Lise Kaye, Analyst
Subject: Council Bill 120308 – Approves the use of and accepts the surveillance impact
           report for the Seattle Police Department's use of Maltego's Link Analysis Software

On Wednesday, April 27, 2022 the Economic Development, Technology and City Light Committee will discuss Council Bill 120308. This Council Bill would approve the Seattle Police Department's (SPD's) continued use of Maltego's Link Analysis Software and accept the Surveillance Impact Report (SIR) and an Executive Overview for this technology. 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 memo describes Maltego Link Analysis, 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 memo identifies policy issues for Council consideration.

Maltego's Link Analysis Software

SPD uses Maltego's Link Analysis Software in response to specific cybersecurity incidents, criminal investigations, and/or for training purposes. The software queries public internet data and diagrams associations between individuals, devices and networks. According to the SIR, the risk of erroneous links between individuals not related to criminal investigations constitutes the most important unintended civil liberties consequence from this technology. SPD mitigates this risk by limiting the number of detectives using the system. SPD mitigates other risks, such as acquisition of private data about individuals, potential algorithmic bias or ethnic bias, and potential racial or ethnicity-based bias in data sharing, storage and retention through its evidence procedures, anti-bias policies and warrant conditions. The Racial Equity Toolkit does not identify metrics to be used as part of the CTO's required annual equity assessments.

---

[1] The Executive Overview summarizes SPD's allowable uses of Maltego. See also the memo 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.

Surveillance Working Group Recommendations and CTO Response

The Community Surveillance Working Group's Impact Assessment for Maltego's Link Analysis Software makes 15 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** describes whether the SIR as drafted or current law would address the Working Group's recommendations, as well as relevant responses from the CTO and/or SPD.

Table 1. Working Group Recommendations

Working Group Recommendation	Whether/How Addressed by SIR, CTO or SPD
1. Prohibit use of Maltego for predictive policing	Not addressed in the SIR. *According to the CTO's Response, "The use case for Maltego identified does not allow for the use of predictive policing, and any changes to the use case would require re-approval of the SIR."*
2. Prohibit use of Maltego for dragnet social media analysis[2]	Not addressed in the SIR. *According to SPD, the department does not use Maltego for "dragnet social media analysis" apart from an official criminal investigation.*
3. Clearly define purpose and allowable uses and limit use of Maltego to that purpose and those allowable uses. Specify incident types for which Maltego may be used.	**Executive Overview.** Operational Policies represent the only allowable uses of the equipment and data collected by this technology. [SMC 14.12](#) *(the "Intelligence Ordinance) governs the collection of data for a criminal investigation.*
4. Restrict when Maltego may be used to collect data on an individual associated with an investigation, such as a regulation requiring reasonable suspicion that an individual committed a crime before their public data can be collected and assessed.	**SIR §**3.2 Maltego is only used in response to specific cybersecurity incidents, criminal investigations wherein reasonable suspicion exists that a crime has occurred, and/or for training purposes. [SMC 14.12](#) *(the "Intelligence Ordinance) governs the collection of data for a criminal investigation.*
5. SPD must disclose the specific data sources it uses via Maltego.	**SIR §**2.2 Maltego functions by parsing large amounts of publicly available information from various open source websites…[3] *The SIR provides the following link:* https://resources.infosecinstitute.com/topic/information-gathering-maltego/

---

[2] This term is not defined in the SWG's Impact Assessment. One definition of "dragnet" according to [Oxford Languages](#) is "a systematic search for someone or something, especially criminals or criminal activity."

[3] According to SPD, Maltego is capable of performing "dark web" searches including forums, torrents, beacons, and other sources.

Working Group Recommendation	Whether/How Addressed by SIR, CTO or SPD
6. Use of Maltego must be disclosed to the individual or the legal representative of the individual facing charges for which Maltego was used in SPD's investigation.	**SIR §6.6** As per RCW 10.97, individuals who are subject to a criminal investigation will not be party to the information collection process…[4]
7. Prohibit input into Maltego of internal SPD data or privately collected data by SPD officers	**SIR §4.1 …**Maltego is not used … to process or collect internal data….. **SIR §2.1** Information gathered [as authorized by a warrant] can… be manually added to the chart generated by Maltego.
8. Prohibit SPD data sharing, including via Maltego Data Partner or any similar program	**SIR §6.1** In addition to SPD Policies 12.050 and 12.110, SPD's data sharing is governed by federal and state criminal justice policies and procedures. *According to SPD, the department does not participate in Maltego Data Partner or any similar program.*
9. Analyze the impacts of any Maltego outputs.	**SIR §1.2** Search warrant authorization is required and mitigates privacy concerns if Maltego is used to collect private data of citizens. **SIR §1.4.2** … There is no distinction in the levels of service this system provides to the various and diverse neighborhoods, communities, or individuals within the city…. **SIR §1.4.2** The most important unintended possible consequence related to the continued utilization of Maltego is the possibility that erroneous links between individuals not related to criminal investigations may be considered. However, because all analysis conducted in the TESU [Technical and Electronic Support Unit] by a limited number of detectives the risk is mitigated.
10. SPD must independently validate data obtained via Maltego	**SIR §6.5** Detectives or other sworn officers may interview such subjects or conduct additional investigation to determine inaccuracies in the information, on a case by case, basis.
11. Create a process to analyze the accuracy of data and analyses generated by Maltego	**SIR §6.5** Detectives or other sworn officers may interview such subjects or conduct additional investigation to determine inaccuracies in the information, on a case by case, basis.
12. After export of Maltego data, delete that data from Maltego	**SIR §6.5** The software automatically alerts users of data that must be deleted under legal deletion requirements such as 28 CFR Part 23.

---

[4] RCW 10.97.080 – Inspection of information by subject-Challenges and corrections: All criminal justice agencies shall permit an individual who is, or who believes that he or she may be, the subject of a criminal record maintained by that agency, to appear in person during normal business hours of that criminal justice agency and request to see the criminal history record information held by that agency pertaining to the individual. *The individual's right to access and review of 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 this chapter. (italics added)

Working Group Recommendation	Whether/How Addressed by SIR, CTO or SPD
13. Execute agreement with Paterva that prevents them from storing or accessing SPD data	**SIR §4.7** …SPD utilizes the free version of Maltego and, as a result, has no control over vendor access to viewing searches that were conducted by SPD…. *According to SPD, Maltego owns the collected data; once SPD creates a copy of the data, it owns the copy of the data and any resultant analysis. Maltego does not have access to SPD's data or inputs. SPD uses the free, non-commercial use version of this technology and therefore does not have a signed agreement.*
14. Given lack of auditing and logging capabilities, create additional security measures to prevent improper use of Maltego by those with access	**SIR §2.4** Two users in SPD's Technical and Electronic Support Unit (TESU) are SPD's only trained and authorized users of Maltego. **SIR §4.10** The free version of Maltego, which SPD uses, does not have any internal logging or auditing functions. **SIR §4.10** …the Unit Supervisor or any auditor may inspect and review the investigative workstation containing the software.
15. SPD must disclose the number of incidents per year analyzed with Maltego	Not addressed in the SIR. *According to SPD, access to and use of Maltego is tracked at the login level, not at the case level. However, any information obtained from Maltego that is pertinent to a case would be added to SPD's Records Management System's case file.*

Policy Considerations

Central Staff has identified the following potential policy considerations and options (not all of which are mutually exclusive). Requests for additional reports and/or policies may require additional resources, potentially via a supplemental budget appropriation.

1. Annual equity assessment metrics. SPD has not yet finalized metrics to be used in evaluating use of Maltego 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. In the absence of such metrics, it is unclear how SPD and/or the CTO could identify disproportionate impacts from the use of Maltego, such as the frequency of specific populations appearing on Maltego diagrams.
   Options:
   A. Request a report on the proposed metrics by a date certain.
   B. Take no action.

2. Response to Public Comments. The SIR does not provide a response to question 4.1 "How will you address the concerns that have been identified by the public."
   Options:
   A. Request that SPD provide a written response to public comments associated with the SIR public engagement process by a date certain.
   B. Take no action.

3. <u>Mitigation of Civil Liberties Impacts.</u> The SIR flags the risk of erroneous links between individuals not related to criminal investigations as the most important unintended consequence from the use of this technology. The SIR also identifies data sharing, storage and retention as having the potential to contribute to structural racism and/or disparate impacts on historically targeted communities. An expanded evaluation of these risks and related concerns could reveal whether more direct policies and protocols may be needed to protect against errors, potential bias in baseline data, and/or disproportionate over-surveillance.

    <u>Options:</u>

    A. Obtain an independent evaluation of the civil liberties risks associated with the use of Maltego, which could include documentation of the types and number of incidents for which SPD has used the system, the databases used by SPD for these analyses, data input by SPD officers, data validation and accuracy of analyses, and demographic information about the individuals and groups associated with each analysis.

    B. Take no action.

4. <u>Contractual Terms – Data and Security Protection.</u> SPD reports that it uses the free version of Maltego and thus has no contractual relationship with its parent company, Paterva. The lack of a contract and/or reliance upon a vendor-provided licensing agreement may reduce the City's ability to restrict Paterva's access to sensitive and/or private information.[5]

    <u>Options:</u>

    A. Request that SPD discontinue use of the free version of Maltego and acquire a version with contractual provisions for data and security protection. This may require additional resources, potentially through a supplemental budget action.[6]

    B. Take no action.

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

---

[5] Data and security protection for the City's data is generally not included by vendors in their standard licensing agreements for off-the-shelf products or for "software as a service" products, in which an application is accessed via a cloud provider. ITD incorporates data and security protection requirements into its purchasing contracts, and Finance and Administration Department's contract template for purchasing technology has similar terms.

[6] Maltego does not appear to publish its prices online, but one site quoted licensing costs from $999 to $1,999 for two different commercial versions. Additional resources may be required for a custom contract.