City of Seattle

2021 Surveillance Impact Report

Link Analysis Software - Maltego

Seattle Police Department

City of Seattle

Surveillance Impact Report ("SIR") overview

About the Surveillance Ordinance

Section 14.18.020 of the Seattle Municipal Code (SMC), enacted by Ordinance 125376 and last amended by Ordinance 125679, also referred to as the "Surveillance Ordinance," charges the City's executive with developing a process to identify surveillance technologies subject to the ordinance. Seattle IT, on behalf of the executive, developed and implemented a process through which a privacy and surveillance review is completed prior to the acquisition of new technologies. This requirement, and the criteria used in the review process, are documented in Seattle IT Policy PR-02, the "Surveillance Policy".

How this Document is Completed

This document is completed by the requesting department staff, support and coordinated by the Seattle Information Technology Department ("Seattle IT"). As Seattle IT and department staff complete the document, they should keep the following in mind.

1. Responses to questions should be in the text or check boxes only; all other information (questions, descriptions, etc.) Should **not** be edited by the department staff completing this document.
2. All content in this report will be available externally to the public. With this in mind, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.

Surveillance Ordinance Review Process

The following is a high-level outline of the complete SIR review process.

Upcoming for Review	Initial Draft	Open Comment Period	Final Draft	Working Group	Council Review
The technology is upcoming for review, but the department has not begun drafting the surveillance impact report (SIR).	Work on the initial draft of the SIR is currently underway.	The initial draft of the SIR and supporting materials have been released for public review and comment. During this time, one or more public meetings will take place to solicit feedback.	During this stage the SIR, including collection of all public comments related to the specific technology, is being compiled and finalized.	The surveillance advisory working group will review each SIR's final draft and complete a civil liberties and privacy assessment, which will then be included with the SIR and submitted to Council.	City Council will decide on the use of the surveillance technology, by full Council vote.

Privacy Impact Assessment

Purpose

A Privacy Impact Assessment ("PIA") is a method for collecting and documenting detailed information collected in order to conduct an in-depth privacy review of a program or project. A PIA asks questions about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. It also requests information about policies, training and documentation that govern use of the technology. The PIA responses are used to determine privacy risks associated with a project and mitigations that may reduce some or all of those risks. In the interests of transparency about data collection and management, the City of Seattle has committed to publishing all PIAs on an outward facing website for public access.

When is a Privacy Impact Assessment Required?

A PIA may be required in two circumstances.

1. When a project, technology, or other review has been flagged as having a high privacy risk.
2. When a technology is required to complete the surveillance impact report process. This is one deliverable that comprises the report.

1.0 Abstract

1.1 Please provide a brief description (one paragraph) of the purpose and proposed use of the project/technology.

Paterva's Maltego is a cyber-security software application that is used to assist Seattle Police Department (SPD) to research publicly available data and diagram associations between individuals, devices, and networks, as part of a cybercrime investigation. Maltego allows up to two authorized users in SPD's Technical and Electronic Support Unit (TESU) to trace the origin of a specific IP address, and potentially identify a suspect, that has attacked, or attempted to infiltrate, the City's network or the network of a third party. In essence, SPD utilizes Maltego to investigate cybercrimes, primarily in determining the digital origin of attacks against cyber infrastructure.

1.2 Explain the reason the project/technology is being created or updated and why the PIA is required.

Maltego queries public information available on the internet, allowing an investigator to build a network diagram of individuals and devices (i.e., computers, cell phones, etc). Though Maltego collects only publicly available information, its use leads to privacy concerns about indiscriminate collection of internet activity by SPD on members of the general public. SPD mitigates this privacy concern by utilizing Maltego only as it relates to a specific investigation related to cybercrime and only to access publicly available information. Search warrant authorization is required, and would be obtained, to further any investigation into accessing private individual information.

2.0 Project / Technology Overview

Provide an overview of the project or technology. The overview gives the context and background necessary to understand the purpose, mission and justification for the project / technology proposed

2.1 Describe the benefits of the project/technology.

Maltego queries public data on the internet, such as domains, and displays it in a diagram showing links. This is a useful tool for SPD to use in cyber-crime investigations, as these incidents often involve interactions between individuals, devices, and networks that are otherwise unknown. This is a popular tool that is used across the information-security community for both defensive cyber-security programs and for investigating breaches and instances of cyber-crime. SPD utilizes Maltego in these capacities.

Example: The City's network is attacked with ransomware from somedomain.com. Maltego would query the internet for public information about who might own/run somedomain.com, where it might be hosted, and which company provides its internet connect. At this point, if detectives determine that further information would be beneficial in pursuit of the investigation, they would then obtain appropriate warrant authorization and subpoena information from the internet provider. Information gathered in this manner can then be manually added to the chart generated by Maltego to create a diagram showing where the ransomware originated from and how it traversed the internet to attack City of Seattle.

2.2 Provide any data or research demonstrating anticipated benefits.

Maltego functions by parsing large amounts of publicly available information from various open source websites and visualizing the results in graphs which allow detectives to piece together connections related to the investigation. Another advantage of this tool is that the relationship between various types of information can give a better picture on how they are interlinked and can also help in identifying unknown relationship.

https://resources.infosecinstitute.com/topic/information-gathering-maltego/

2.3 Describe the technology involved.

Maltego is an Open Source Intelligence (OSINT) platform which presents publicly available information in an easy to interpret visual entity-relationship model which allows investigators to analyze connections between individuals related to criminal investigations. Maltego functions similar to a web search engine but rather than returning a list of related websites, Maltego allows the user to create a visualization linking entities involved in a cybercrime incident.

A typical use would be Maltego's use in diagramming threat actors following a cyber-attack on the City's network. An investigator would need to research the IP address of domain of the attack source and work to find the individual(s) or organization(s) orchestrating the attack. Often, the source of the attack is a system belonging to a third party that has itself been compromised (i.e., bot networks) and a side benefit of an SPD investigation is mitigating the compromise of these third-party systems.

2.4 Describe how the project or use of technology relates to the department's mission.

The mission of the Seattle Police Department is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional, and dependable police services. SPD's department priorities include the use of best practices that include officer safety guidelines and performance-based accountability to provide progressive and responsive police services to crime victims, witnesses, and all members of the community, and to structure the organization to support the SPD mission and field a well-trained sworn and non-sworn workforce that uses technology, training, equipment, and research strategically and effectively.

Seattle Police Department has a responsibility to protect the City and its citizens, their data, and infrastructure from cyber-crime. Maltego is one tool that SPD uses to mitigate these crimes within Seattle.

2.5 Who will be involved with the deployment and use of the project / technology?

Two users in SPD's Technical and Electronic Support Unit (TESU) are SPD's only trained and authorized users of Maltego. TESU Detectives may share Maltego data with Seattle IT's security team in order to eliminate security vulnerabilities, assess and mitigate data compromise, and to take steps to block hostile sites from accessing City networks.

Authorized users of Maltego are Criminal Justice Information Services (CJIS) certified and maintain Washington State ACCESS (A Central Computerized Enforcement Service System) certification. More information on CJIS compliance may be found at the CJIS Security Policy website. Additional information about ACCESS may be found on the Washington State Patrol's website.

3.0 Use Governance

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities contracting with the City are bound by restrictions specified in the surveillance ordinance and privacy principles and must provide written procedures for how the entity will comply with any restrictions identified.

3.1 Describe the processes that are required prior to each use, or access to/of the project / technology, such as a notification, or check-in, check-out of equipment.

Maltego is a software only used during the investigation of cyber-crimes by SPD detectives working in TESU. 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. All users of CAD must be CJIS certified and maintain Washington State ACCESS certification. Each user must be directly granted an account in order to access the software.

3.2 List the legal standards or conditions, if any, that must be met before the project / technology is used.

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.

All use of the Maltego software must also comply with SPD Policy 12.050 – Criminal Justice Information Systems and may only be used for legitimate criminal investigative purposes.

Use of Maltego is governed by the City of Seattle Intelligence Ordinance, 28 CFR Part 23, CJIS requirements, and any future applicable requirements.

3.3 Describe the policies and training required of all personnel operating the project / technology, and who has access to ensure compliance with use and management policies.

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.

All authorized users of Maltego must be CJIS certified and must maintain Washington State ACCESS certification and trained directly in the use of the Maltego software, in addition to all standard SPD training and Directives.

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

4.0 Data Collection and Use

4.1 Provide details about what information is being collected from sources other than an individual, including other IT systems, systems of record, commercial data aggregators, publicly available data and/or other City departments.

Maltego queries publicly available data on the internet and collects information based on the parameters of the search request, much like Google returns results based on specific search terms. Maltego is not used to collect private data, nor is it used to process or collect internal data. It is specifically a tool used to query and diagram public information related to cyber-crime investigations. In this sense, it is collecting any publicly available information on the internet related to the specific parameters of the user request.

4.2 What measures are in place to minimize inadvertent or improper collection of data?

Maltego is only used by two trained TESU Detectives whose primary duties involve the investigation of cyber- and other internet-related crimes. All data collected is related to a criminal investigation and included in the investigation file. If no data is collected that assists in the pursuit of the criminal investigation, this information is not retained, and no data is provided to the investigating Officer/Detective. Data, when pertinent, is exported as a spreadsheet and/or visual diagram, at which point it is handled per department policy regarding digital evidence as part of a criminal investigation. A local copy of the data is only saved if the Detective operating Maltego manually initiates a local saved copy and that is also maintained and handled per department policy.

4.3 How and when will the project / technology be deployed or used? By whom? Who will determine when the project / technology is deployed and used?

The Maltego tool is only used by two trained SPD Detectives whose primary duties involve the investigation of cyber- and other internet-related crimes. Maltego is used when a specific incident occurs in which the network security of the City or of a private entity has been compromised, and an investigation has been instigated.

4.4 How often will the technology be in operation?

Maltego is used infrequently to investigate cybercrime incidents.

4.5 What is the permanence of the installation? Is it installed permanently, or temporarily?

The software is installed on a workstation computer located in the TESU.

4.6 Is a physical object collecting data or images visible to the public? What are the markings to indicate that it is in use? What signage is used to determine department ownership and contact information?

No physical object is collecting any data.

4.7 How will data that is collected be accessed and by whom?

Only authorized SPD users can access Maltego or the data while it resides in the specific workstation where it is installed. Access to Maltego is via a password-protected software interface and the software is stored locally rather than on the network or remote server. 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. These searches, however, would look much like any search engine responses, meaning that the parameters would return only publicly available information.

Data removed from Maltego and entered into investigative files is securely uploaded and used on SPD's password-protected network with access limited to authorized 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.

4.8 If operated or used by another entity on behalf of the City, provide details about access, and applicable protocols.

Maltego is used by two trained TESU detectives within TESU, and by no other entity.

Use of Maltego is governed by the City of Seattle Intelligence Ordinance, 28 CFR Part 23, CJIS requirements, and any future applicable requirements.

4.9 What are acceptable reasons for access to the equipment and/or data collected?

Access to Maltego is restricted to use for the related security incident and/or pertinent criminal investigations and subject to Department Policy regarding ongoing criminal investigations.

4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

SPD currently uses a free community version of Maltego that has no internal logging or auditing. A paid version includes the ability to stand up an internal SPD server that would allow for logging, but that would involve significant costs to implement and maintain.

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.

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

Data collected by Maltego is stored on an encrypted workstation within TESU.

Per the CJIS Security Policy:

"Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history 08/16/2018 CJISD-ITS-DOC-08140-5.7 D-3 records. Additionally, each CSO must ensure that all agencies establish an information security structure that provides for an ISO and complies with the CJIS Security Policy.

5.2 How will the owner allow for departmental and other entities, to audit for compliance with legal deletion requirements?

Cyber-Crime workstations are subject to audit by the supervisor of the Technical and Electronic Support Unit and 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.

5.3 What measures will be used to destroy improperly collected data?

SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a GO Report. Evidence is submitted to the Evidence Unit and associated with a specific GO Number and investigation.

All data 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 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."

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.

5.4 which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

The Technical and Electronic Support Unit Supervisor is responsible for ensuring compliance with data retention requirements for Maltego within SPD. Additionally, an auditor, including the Office of Inspector General can monitor for compliance at any time.

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.

6.0 Data Sharing and Accuracy

6.1 Which entity or entities inside and external to the City will be data sharing partners?

SPD has no data sharing partners for Maltego. No person, outside of SPD, has direct access to Maltego or the data while it resides in the system or technology.

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 without 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 Maltego 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 collected by Maltego.

6.2 Why is data sharing necessary?

Data sharing is frequently necessary during the course of a criminal investigation to follow up on leads and gather information on suspects from outside law enforcement agencies. Cooperation between law enforcement agencies is an essential part of the investigative process.

6.3 Are there any restrictions on non-City data use?

Yes ☒ No ☐

6.3.1 If you answered yes, provide a copy of the department's procedures and policies for ensuring compliance with these restrictions.

Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

Once disclosed in response to PRA request, there are no restrictions on non-City data use; however, applicable exemptions will be applied prior to disclosure to any requestor who is not authorized to receive exempt content.

6.4 How does the project/technology review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?

Research agreements must meet the standards reflected in SPD Policy 12.055. Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

6.5 Explain how the project/technology checks the accuracy of the information collected. If accuracy is not checked, please explain why.

This software simply visualizes data collected is from publicly available information on the internet.

6.6 Describe any procedures that allow individuals to access their information and correct inaccurate or erroneous information.

As per RCW 10.97, individuals who are subject to a criminal investigation will not be party to the information collection process and thus will not have an opportunity to correct their information. 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.

7.0 Legal Obligations, Risks and Compliance

7.1 What specific legal authorities and/or agreements permit and define the collection of information by the project/technology?

Maltego only accesses and collects public data and is used in response to requests for assistance with cyber-security incidents and active criminal investigations.

All use of Maltego must also comply with SPD Policy 12.050 – Criminal Justice Information Systems and may only be used for legitimate criminal investigative purposes.

Use of Maltego will be governed by the City of Seattle Intelligence Ordinance, 28 CFR Part 23, CJIS requirements, and any future applicable requirements.

7.2 Describe what privacy training is provided to users either generally or specifically relevant to the project/technology.

Users of Maltego undergo training on the use of the software, which includes privacy training.

All authorized users of Maltego must be CJIS certified and must maintain Washington State ACCESS certification.

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.

The CJIS training requirements can be found in the appendices of this document, as well as in question 3.3, above.

7.3 Given the specific data elements collected, describe the privacy risks identified and for each risk, explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy risks for Maltego revolve around the perception of mass or indiscriminate data collection of members of the public. This risk is mitigated by a number of legal and policy provisions.

SMC 14.12 and SPD Policy 6.060 direct all SPD personnel to "any documentation of information concerning a person's sexual preferences or practices, or their political or religious activities must be for a relevant reason and serve a legitimate law enforcement purpose."

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.

Finally, see 5.3 for a detailed discussion about procedures related to noncompliance.

7.4 Is there any aspect of the project/technology that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?

The privacy risks outlined in 7.3 above are mitigated by investigatory requirements and auditing processes (i.e., related to a specific criminal investigation; access logs) that allow for an auditor, including the Office of Inspector General, to inspect use and deployment of audio recording devices.

8.0 Monitoring and Enforcement

8.1 Describe how the project/technology maintains a record of any disclosures outside of the department.

The information used Maltego relates to ongoing criminal investigations. Information will be released in response to public disclosure requests as applicable under the Public Records Act and the City of Seattle Intelligence Ordinance, just as they are applicable to any other SPD investigative records.

Per SPD Policy 12.080, requests for public disclosure are logged by SPD's Legal Unit. Any action taken, and data released subsequently in response to subpoenas is then tracked through a log maintained by the Legal Unit. Public disclosure requests are tracked through the City's GovQA Public Records Response System, and responses to Public Disclosure Requests, including responsive records provided to a requestor, are retained by SPD for two years after the request is completed.

This software is not directly accessed by outside agencies. Information may be shared with outside agencies as it would with any criminal investigation and release is governed by the same rules. Any bulletins or other notifications created with information or analysis resulting from this project are kept in the SPD network file system as well as recorded in the established SPD bulletin system. In addition, the software's audit log keeps a record of all data accessed by each user.

8.2 What auditing measures are in place to safeguard the information, and policies that pertain to them, as well as who has access to the audit data? Explain whether the project/technology conducts self-audits, third party audits or reviews.

The free version of Maltego that is currently used is auditable, in that the Unit Supervisor or any auditor may inspect and review the investigative workstation containing the software. Should the City choose to invest in a Maltego paid server, there would be onsite logging which would then be available for review.

Financial Information

Purpose

This section provides a description of the fiscal impact of the surveillance technology, as required by the surveillance ordinance.

1.0 Fiscal Impact

Provide a description of the fiscal impact of the project/technology by answering the questions below.

1.1 Current or potential sources of funding: initial acquisition costs.

Current ☒ potential ☐

Date of initial acquisition	Date of go live	Direct initial acquisition cost	Professional services for acquisition	Other acquisition costs	Initial acquisition funding source

Notes:

SPD utilizes the free version of Maltego.

1.2 Current or potential sources of funding: on-going operating costs, including maintenance, licensing, personnel, legal/compliance use auditing, data retention and security costs.

Current ☒ potential ☐

Annual maintenance and licensing	Legal/compliance, audit, data retention and other security costs	Department overhead	IT overhead	Annual funding source
$0	0	0		

Notes:

1.3 Cost savings potential through use of the technology

N/A

1.4 Current or potential sources of funding including subsidies or free products offered by vendors or governmental entities

N/A

Expertise and References

Purpose

The following information is provided to ensure that Council has a group of experts to reference while reviewing the completed surveillance impact report ("SIR"). Any individuals or agencies referenced must be made aware ahead of publication that their information has been included. All materials must be available for Council to access or review, without requiring additional purchase or contract.

1.0 Other Government References

Please list any other government bodies that have implemented this technology and can speak to the implementation of this technology.

Agency, municipality, etc.	Primary contact	Description of current use

2.0 Academics, Consultants, and Other Experts

Please list any experts in the technology under consideration, or in the technical completion of the service or function the technology is responsible for.

Agency, municipality, etc.	Primary contact	Description of current use

3.0 White Papers or Other Documents

Please list any authoritative publication, report or guide that is relevant to the use of this technology or this type of technology.

Title	Publication	Link

Racial Equity Toolkit ("RET") and engagement for public comment worksheet

Purpose

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit ("RET") in order to:

- Provide a framework for the mindful completion of the SIR in a way that is sensitive to the historic exclusion of vulnerable and historically underrepresented communities. Particularly, to inform the public engagement efforts departments will complete as part of the surveillance impact report.
- Highlight and mitigate any impacts on racial equity from the adoption and the use of the technology.
- Highlight and mitigate any disparate impacts on individuals or vulnerable communities.
- Fulfill the public engagement requirements of the surveillance impact report.

Adaptation of the RET for Surveillance Impact Reports

The RET was adapted for the specific use by the Seattle Information Technology Departments' ("Seattle IT") Privacy Team, the Office of Civil Rights ("OCR"), and Change Team members from Seattle IT, Seattle City Light, Seattle Fire Department, Seattle Police Department, and Seattle Department of Transportation.

Racial Equity Toolkit Overview

The vision of the Seattle Race and Social Justice Initiative ("RSJI") is to eliminate racial inequity in the community. To do this requires ending individual racism, institutional racism and structural racism. The RET lays out a process and a set of questions to guide the development, implementation and evaluation of policies, initiatives, programs, and budget issues to address the impacts on racial equity.

1.0 Set Outcomes

1.1. Seattle City Council has defined the following inclusion criteria in the surveillance ordinance, and they serve as important touchstones for the risks departments are being asked to resolve and/or mitigate. Which of the following inclusion criteria apply to this technology?

☐ The technology disparately impacts disadvantaged groups.
☐ There is a high likelihood that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service.
☒ The technology collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection.
☒ The technology raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice.

1.2 What are the potential impacts on civil liberties through the implementation of this technology? How is the department mitigating these risks?

Some iterations of Maltego allow for collection of private data of citizens. SPD mitigates this privacy concern by utilizing Maltego only as it relates to a specific investigation related to cybercrime and only to access publicly available information. Search warrant authorization is required, and would be obtained, to further any investigation into accessing private individual information.

1.3 What are the risks for racial or ethnicity-based bias through each use or deployment of this technology? How is the department mitigating these risks?

Include a description of any issues that may arise such as algorithmic bias or the possibility for ethnic bias to emerge in people and/or system decision-making.

The mission of the Seattle Police Department is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional, and dependable police services. To mitigate against any potential algorithmic bias or ethnic bias to emerge in the use of link analysis software such as Maltego, SPD employees are responsible for gathering, creating, and disseminating information (internally or externally as defined above) and are bound by SPD Policy 5.140 which forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

1.4 Where in the City is the technology used or deployed?

☒ all Seattle neighborhoods

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County.

If possible, please include any maps or visualizations of historical deployments / use.

n/a

1.4.1 What are the racial demographics of those living in this area or impacted by these issues?

City of Seattle demographics: White - 69.5%; Black or African American - 7.9%; Amer. Indian & Alaska Native - 0.8%; Asian - 13.8%; Native Hawaiian & Pacific Islander - 0.4; Other race - 2.4%; Two or more races - 5.1%; Hispanic or Latino ethnicity (of any race): 6.6%; Persons of color: 33.7%.

King County demographics: White – 70.1%; Black or African American – 6.7%; American Indian & Alaskan Native – 1.1%; Asian, Native Hawaiian, Pacific Islander – 17.2%; Hispanic or Latino (of any race) – 9.4%

1.4.2 How does the Department to ensure diverse neighborhoods, communities, or individuals are not specifically targeted through the use or deployment of this technology?

Maltego is used during the investigation of cyber-crimes by the SPD TESU and information gathered is related to these criminal investigations. There is no distinction in the levels of service this system provides to the various and diverse neighborhoods, communities, or individuals within the city.

All use of Maltego must also comply with SPD Policy 12.050 – Criminal Justice Information Systems and may only be used for legitimate criminal investigative purposes.

Use of Maltego is be governed by the City of Seattle Intelligence Ordinance, 28 CFR Part 23, CJIS requirements, and any future applicable requirements.

1.5 How do decisions around data sharing have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

The Aspen Institute on Community Change defines *structural racism* as "…public policies, institutional practices, cultural representations and other norms [which] work in various, often reinforcing ways to perpetuate racial group inequity."[1] Data sharing has the potential to be a contributing factor to structural racism and thus creating a disparate impact on historically targeted communities. Data sharing is frequently necessary during the course of a criminal investigation to follow up on leads and gather information on suspects from outside law enforcement agencies. Cooperation between law enforcement agencies is an essential part of the investigative process.

In an effort to mitigate the possibility of disparate impact on historically targeted communities, SPD has established policies regarding the dissemination of data in connection with criminal prosecutions, Washington Public Records Act (Chapter 42.56 RCW), and other authorized researchers.

Further, 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.

1.6 How do decisions around data storage and retention have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

Like decisions around data sharing, data storage and retention have similar potential for disparate impact on historically targeted communities. The information collected by Maltego is related only to criminal investigations and its users are subject to SPD's existing policies prohibiting bias-based policing. Further, 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.

1.7 What are potential unintended consequences (both negative and positive potential impact)? What proactive steps can you can / have you taken to ensure these consequences do not occur.

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 by a limited number of detectives the risk is mitigated.

2.0 Public Outreach

2.1 Scheduled public meeting(s).

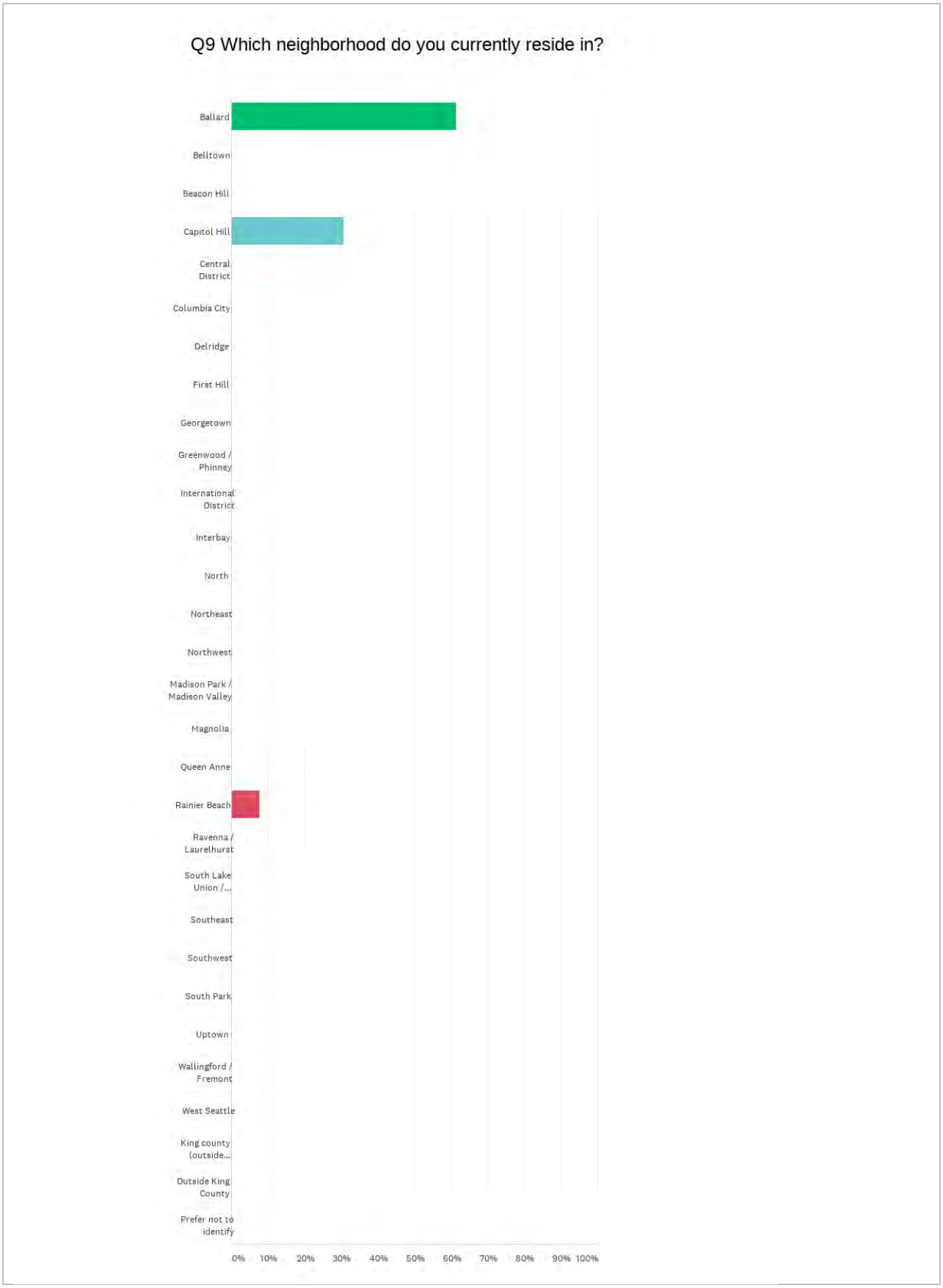
Location	Virtual Event
Time	Thursday, June 10th, 12 PM

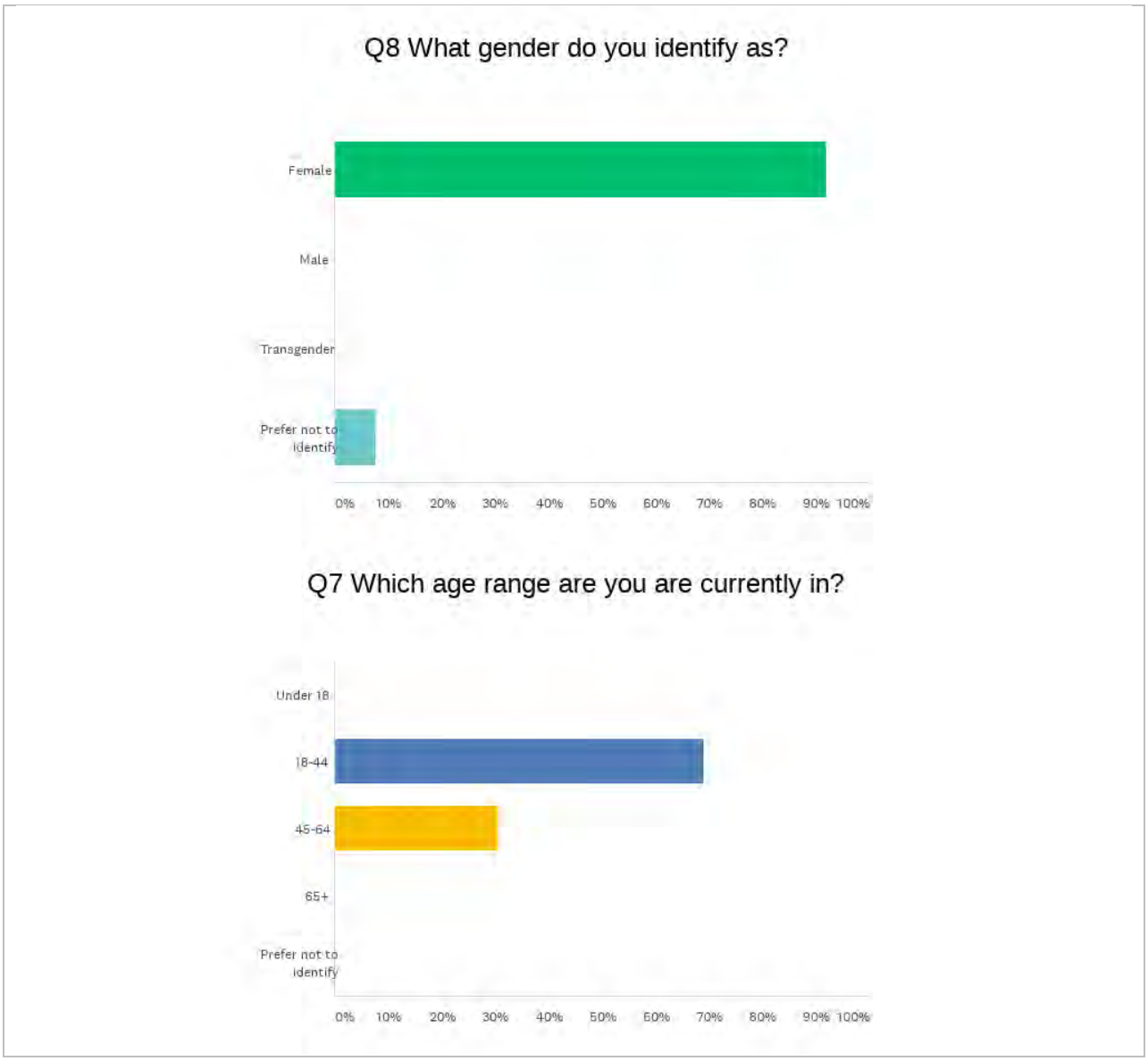
Location	Virtual Event
Time	Tuesday, June 29th, 3 PM

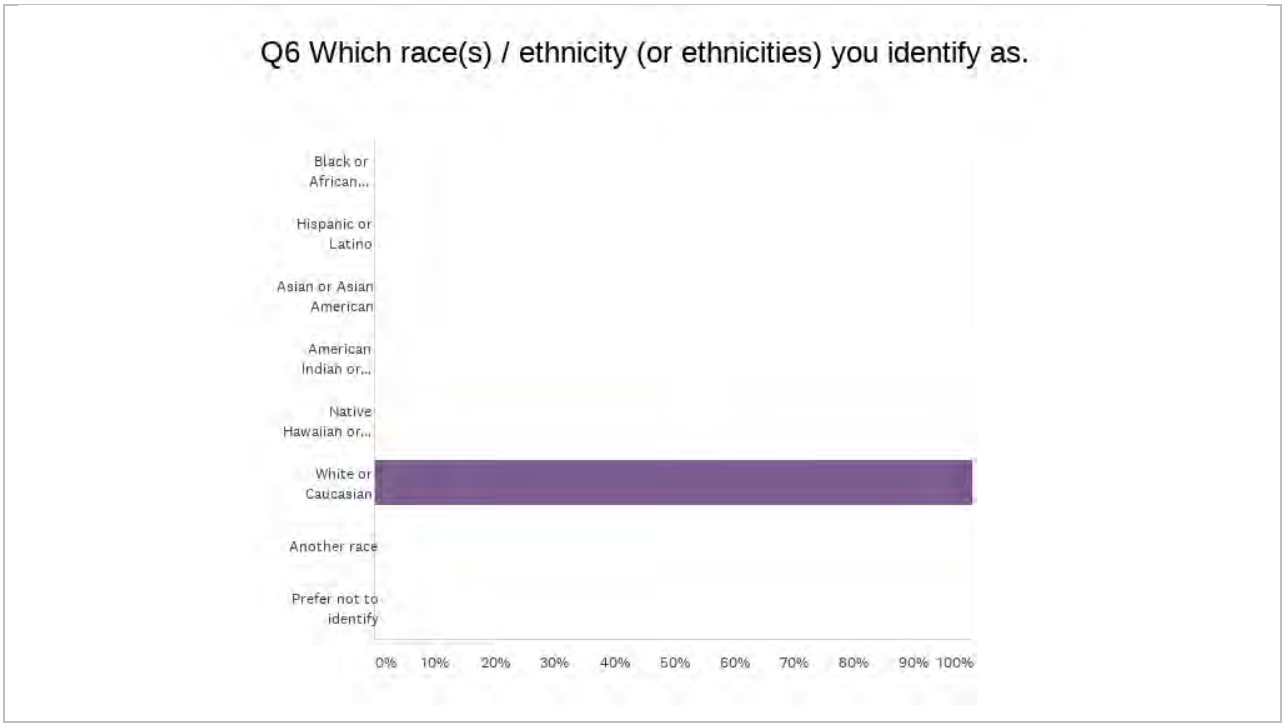
3.0 Public Comment Analysis

This section will be completed after the public comment period has been completed. Please note due to the volume of comments, analysis represents a summarization of all comments received. Technology specific comments will be included in Appendix C.

3.1 Summary of Response Volume

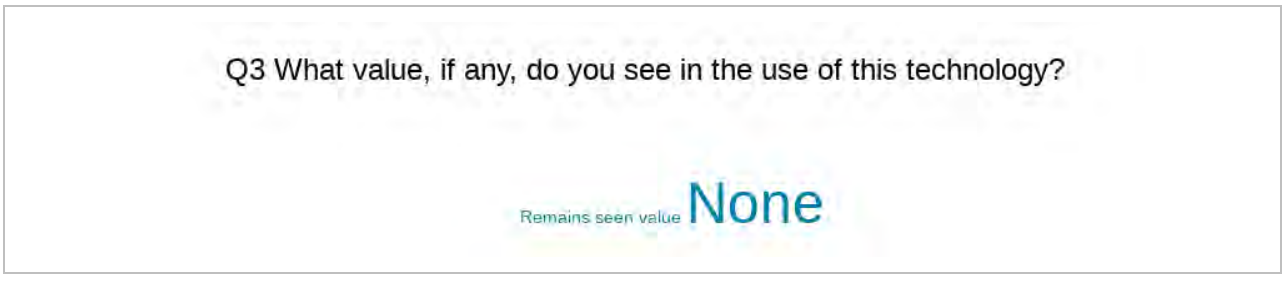

Q9 Which neighborhood do you currently reside in?
Ballard
Belltown
Beacon Hill
Capitol Hill
Central District
Columbia City
Delridge
First Hill
Georgetown
Greenwood / Phinney
International District
Interbay
North
Northeast
Northwest
Madison Park / Madison Valley
Magnolia
Queen Anne
Rainier Beach
Ravenna / Laurelhurst
South Lake Union /...
Southeast
Southwest
South Park
Uptown
Wallingford / Fremont
West Seattle
King county (outside...
Outside King County
Prefer not to identify
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%


Q8 What gender do you identify as?
Female
Male
Transgender
Prefer not to identify
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
Q7 Which age range are you are currently in?
Under 18
18-44
45-64
65+
Prefer not to identify
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%


Q6 Which race(s) / ethnicity (or ethnicities) you identify as.
Black or African...
Hispanic or Latino
Asian or Asian American
American Indian or...
Native Hawaiian or...
White or Caucasian
Another race
Prefer not to identify
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

3.2 Question One: What concerns, if any, do you have about the use of this technology?

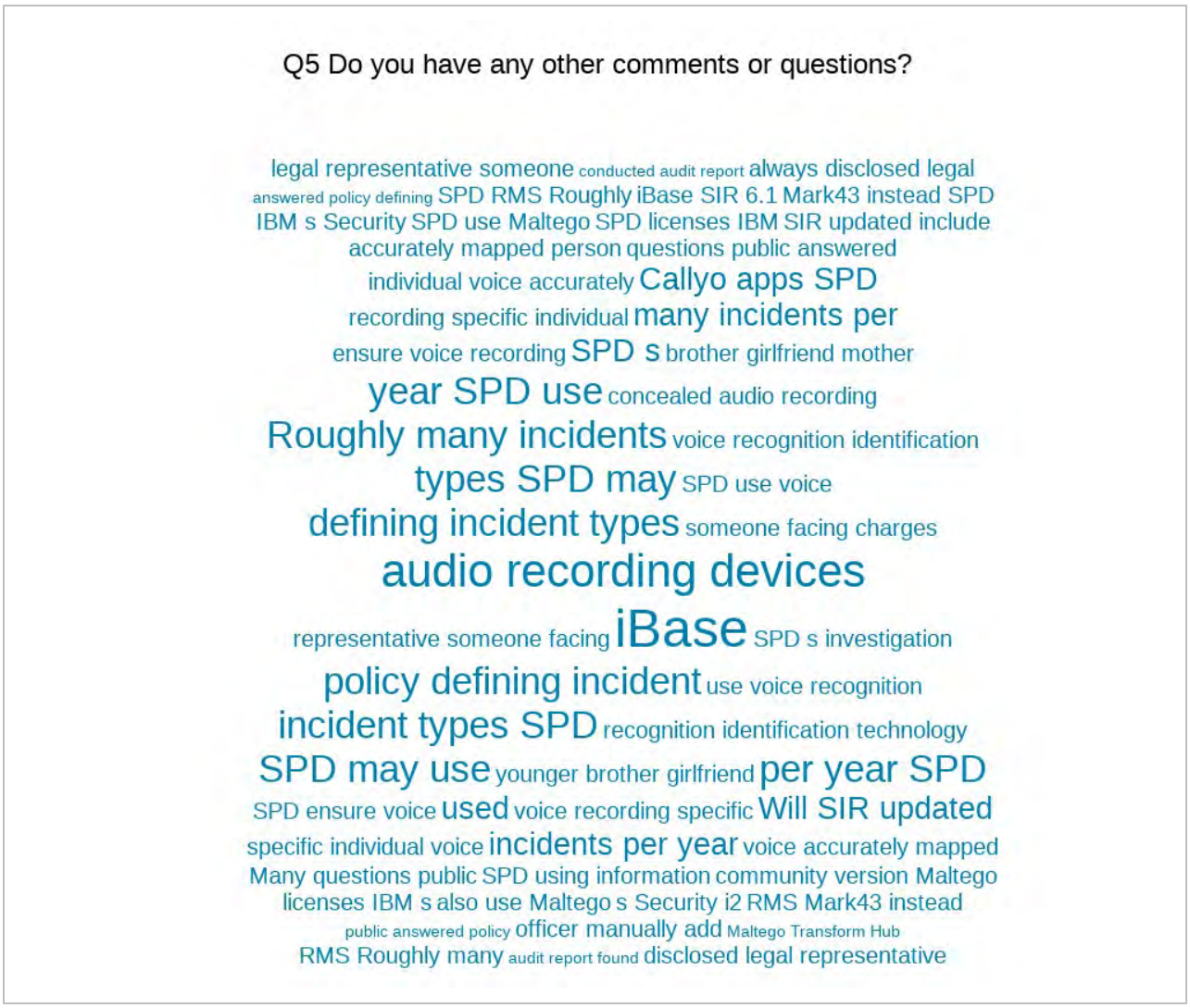
3.3 Question Two: What value, if any, do you see in the use of this technology?



3.4 Question Three: What would you want City leadership to consider when making a decision about the use of this technology?

3.5 General Surveillance Comments

These are comments received that are not particular to any technology currently under review.



4.0 Response to Public Comments

This section will be completed after the public comment period has been completed.

4.1 How will you address the concerns that have been identified by the public?

What program, policy and partnership strategies will you implement? What strategies address immediate impacts? Long-term impacts? What strategies address root causes of inequity listed above? How will you partner with stakeholders for long-term positive change?

5.0 Equity Annual Reporting

5.1 What metrics for this technology be reported to the CTO for the annual equity assessments?

Respond here.

Privacy and Civil Liberties Assessment

Purpose

This section shall be completed after public engagement has concluded and the department has completed the racial equity toolkit section above. The privacy and civil liberties assessment is completed by the community surveillance working group ("working group"), per the surveillance ordinance which states that the working group shall:

"Provide to the executive and the City Council a privacy and civil liberties impact assessment for each SIR that must be included with any departmental request for surveillance technology acquisition or in-use approval. The impact assessment shall include a description of the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities. The CTO shall share with the working group a copy of the SIR that shall also be posted during the period of public engagement. At the conclusion of the public engagement period, the CTO shall share the final proposed SIR with the working group at least six weeks prior to submittal of the SIR to Council for approval. The working group shall provide its impact assessment in writing to the executive and the City Council for inclusion in the SIR within six weeks of receiving the final proposed SIR. If the working group does not provide the impact assessment before such time, the working group must ask for a two-week extension of time to City Council in writing. If the working group fails to submit an impact statement within eight weeks of receiving the SIR, the department and City Council may proceed with ordinance approval without the impact statement."

Working Group Privacy and Civil Liberties Assessment

From: Seattle Community Surveillance Working Group (CSWG)

To: Seattle City Council

Date: Oct 25, 2021

Re: Privacy and Civil Liberties Impact Assessment for Maltego

Executive Summary

The CSWG has completed its review of the Surveillance Impact Reports (SIRs) for the three surveillance technologies included in Group 4a of the Seattle Surveillance Ordinance technology review process. These technologies are Callyo, i2 iBase, Audio Recording Systems, and Maltego. This document is the CSWG's Privacy and Civil Liberties Impact Assessment for Maltego used by Seattle Police Department (SPD) as set forth in SMC 14.18.080(B)(1), which we provide for inclusion in the final SIRs submitted to the City Councils.

This document first provides our recommendations to Council, then provides background information, key concerns, and outstanding questions regarding Maltego.

Our assessment of Maltego technology as used by Seattle Police Department (SPD) focuses on three major issues:

1. Inadequate policies defining purpose of use, data collection, assessment, retention, storage, and security.
2. Inadequate policies to assess for errors in data analysis.
3. A prohibition on use of Maltego for predictive policing is necessary.

Recommendations

The Council should adopt clear and enforceable rules that ensure, at the minimum, the following:

1. There must be a prohibition on use of Maltego for predictive policing.
2. There must be a prohibition on use of Maltego for dragnet social media analysis.
3. The purpose and allowable uses of Maltego must be clearly defined, and any SPD use of Maltego must be limited to that specific purpose and those allowable uses. The specific incident types for which Maltego may be used must be specified.
4. There must be restrictions on if 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.
5. SPD must disclose the specific data sources it uses via Maltego.
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.
7. There must be a prohibition on internal SPD data or privately collected data by SPD officers being inputted into Maltego.
8. There must be a prohibition on SPD sharing data as a Maltego Data Partner or any similar program.
9. There must be an analysis of the impacts of any Maltego outputs.

10. SPD must independently validate data obtained via Maltego.
11. There must be a process to analyze the accuracy of data and analyses generated by Maltego.
12. After Maltego data is exported, SPD must be required to delete originally collected, pertinent data from within Maltego.
13. There must be a clear agreement with Paterva for the use of the free Maltego software that prohibits Paterva from storing or accessing SPD data.
14. There must be additional security measures to prevent improper use of Maltego by those with access, given the lack of auditing and logging capabilities.
15. SPD must disclose for how many incidents per year they use Maltego.

Key Concerns

1. **Inadequate Policies Defining Purpose of Use**. The SIR suggests that Maltego is primarily used for cybercrime investigations, but does not specify any policies designating when the technology may be used. The SIR's language is also vague and implies that Maltego has been used in non-cyber contexts. During the July 20th public engagement meeting, the SPD representative also commented that Maltego could be used for non-cyber crimes, although it generally is not. It is therefore unclear how widely large-scale public data analysis is currently used in SPD criminal investigations or what would prevent widespread usage of Maltego in the future.

2. **Inadequate Policies on Data Collection and Assessment.** The SIR states that Maltego can only be used within the bounds of a specific criminal investigation or "cybersecurity incident." However, it does not specify any internal guidelines restricting what public data or whose public data may be collected and analyzed using Maltego. Under existing policies, it seems entirely possible that people tenuously or erroneously associated with potential perpetrators – including people for whom there is little or no evidence of criminal activity – could be subject to Maltego assessment and surveillance.

3. **Lack of Clarity Around Data Sources.** The SIR does not describe the specific data sources SPD utilizes via Maltego; it provides only limited examples of Maltego's usage and states that data is collected from "various open source websites." Absent further clarity, it seems possible that SPD can use Maltego for social media data analysis, raising privacy issues not addressed in the SIR. Additionally, the SIR acknowledges that "some iterations of Maltego can be used for private data collections," but does not outline procedures to prevent accidental private data collection, including of private information improperly made public through hacking.

4. **Potential for Predictive Usages.** Paterva advertises that Maltego can "[h]elp solve future investigations by pushing insights back into [a] case management system" The SIR indicates that SPD exports Maltego charts back into SPD's system and suggests that data from Maltego might be used for "defensive purposes." If Maltego is being used to anticipate future crimes, SPD must provide clarity as to a) how they guard against existing biases often replicated by predictive policing, and b) what surveillance they perform based on these predictions. Predictive policing is often referred to as "crime forecasting." Predictive policing uses computer systems to analyze large sets of data, such as historical crime data, to predict or forecast where and when the next crime or series of crimes will take place. This is a mode of policing rife with bias and inaccuracies that reproduces and compounds existing discrimination.

5. **Inadequate Policies to Assess for Errors in Data Analysis.** The SIR acknowledges that erroneous linkages are one of the "most important unintended possible consequence[s]" of Maltego. However, in describing safeguards to prevent erroneous linkages, the SIR only states, "because analysis is conducted in the TESU by a limited number of detectives the risk is

mitigated." This mechanism seems ineffective, as no data output review process is described. Perhaps the SIR means that TESU detectives perform only limited and reviewable amounts of manual analysis and diagramming, which indeed might limit inaccuracies. However, no policies are described which would enforce limits on diagramming techniques and levels of usage. To the contrary, any such limits contradict the core purpose of Maltego. SPD states that Maltego is useful precisely because it can "pars[e] large amounts of data," and thereby "help in identifying unknown relationships."

The SIR does not describe SPD tracking of Maltego's error rate. Without error tracking or safeguards, Maltego outputs likely lead police in inaccurate directions and subject random individuals to unnecessary surveillance and police interaction. Because evidence collected via Maltego can be used for search warrants, inaccurate Maltego outputs that are presented to the court as valid could lead to particularly invasive forms of improper searches.

6. **Lack of Clarity on Data Retention Policies.** The SIR states that data that is not relevant to an investigation is not retained and that "pertinent" data is exported to a spreadsheet or diagram and then handled per department policy. However, it does not make clear how and when the originally collected, pertinent data is deleted from Maltego, leaving open the possibility that such data is retained indefinitely.

7. **Lack of Clarity Around Relationship with Paterva.** The SIR states that SPD searches are stored by Paterva, as SPD is unable to stand up their own server using the free version of the software. These searches contain sensitive information that indicate the contents and direction of a criminal investigation and are being exposed to a private third-party. Additionally, the SIR states that Maltego is not "used to process or collect internal data," but elsewhere says that private information gathered via search warrant can be input into Maltego. The SIR does not describe measures to keep that private data secure nor outlines Paterva's or Maltego Technolgies's internal data security measures. The SIR also does not describe a contract between SPD and Paterva or Maltego Technologies for the use of the free Maltego software.

8. **Potential for Improper Use Without Auditing/Logging.** The free version of Maltego's software seems to include no auditing or logging capabilities. Lack of auditing or logging increases the probability that the software will be misused. Given the software's potential for invasive surveillance and monitoring that could intrude upon protected speech, more careful monitoring is essential. Notably, upgrading to the paid version of the software would not resolve the problem and would likely exacerbate the overall civil liberties concerns posed by the software; the paid version includes additional privacy risks given the far wider breadth of data available.

Outstanding Questions

- When can Maltego be used for non-cyber investigations?
- Once an investigation is opened, are there any internal guidelines restricting what public data or whose public data may be collected and analyzed using Maltego?
- Which specific data sources does SPD analyze using Maltego? Are there any limits on the kinds of data that can be assessed?
- Are Maltego outputs ever used for any predictive or "defensive" policing?
- Are errors in the data Maltego pulls systematically tracked? Are there any safeguards against errors or processes for analyzing the data?
- How often has Maltego been used, and is there research suggestive of its efficacy in resolving cybersecurity crimes?
- After data are exported, how and when are pertinent data deleted from within Maltego?

- Does SPD have any kind of written agreement or contract with Paterva/Maltego Technologies for the use of the free Maltego software? If so, what are the provisions?
- Does SPD enter private information collected via search warrant into Maltego? If so, what data security protocols are in place to protect that private information?
- Does Paterva/Maltego Technologies have access to and store data that are requested and collected by SPD, beyond requests/searches made?
- What are Paterva's policies for data security, how are data stored, and who owns the data collected and analyses generated?
- Is Maltego integrated with SPD's RMS (Mark43) or are all data inputs to Maltego entered manually?

The answers to these questions can further inform the content of any binding policy the Council chooses to include in an ordinance on this technology, as recommended above.

City of Seattle

CTO Response

MEMO

To: Seattle City Council

From: Jim Loter, Interim Chief Technology Officer

Subject: CTO Response to the Surveillance Working Group Maltego SIR Review

Purpose

As provided in the Surveillance Ordinance, SMC 14.18.080, this memo outlines the Chief Technology Officer's (CTO's) response to the Surveillance Working Group assessment on the Surveillance Impact Report for Seattle Police Department's Maltego.

Background

The Information Technology Department (ITD) is dedicated to the Privacy Principles and Surveillance Ordinance objectives to provide oversight and transparency about the use and acquisition of specialized technologies with potential privacy and civil liberties impacts. All City departments have a shared mission to protect lives and property while balancing technology use and data collection with negative impacts to individuals. This requires ensuring the appropriate use of privacy invasive technologies through technology limitations, policy, training and departmental oversight.

The CTO's role in the SIR process has been to ensure that all City departments are compliant with the Surveillance Ordinance requirements. As part of the review work for surveillance technologies, ITD's Privacy Office has facilitated the creation of the Surveillance Impact Report documentation, including collecting comments and suggestions from the Working Group and members of the public about these technologies. IT and City departments have also worked collaboratively with the Working Group to answer additional questions that came up during their review process.

Technology Purpose

Paterva's Maltego is a cyber-security software application that is used to assist Seattle Police Department (SPD) to research publicly available data and diagram associations between individuals, devices, and networks, as part of a cybercrime investigation. Maltego allows up to two authorized users in SPD's Technical and Electronic Support Unit (TESU) to trace the origin of a specific IP address, and potentially identify a suspect, that has attacked, or attempted to infiltrate, the City's network or the network of a third party. In essence, SPD utilizes Maltego to investigate cybercrimes, primarily in determining the digital origin of attacks against cyber infrastructure.

Working Group Concerns

In their review, the Working Group has raised concerns about these devices being used in a privacy impacting way, including data errors, collection, processing, and security. We believe that policy, training and technology limitations enacted by SPD provide adequate mitigation for the potential privacy and civil liberties concerns raised by the Working Group about the use of this operational technology.

Recommended Next Steps

I look forward to working together with Council and City departments to ensure continued transparency about the use of these technologies and finding a mutually agreeable means to use technology to improve City services while protecting the privacy and civil rights of the residents we serve. Specific concerns in the Working Group comments about cameras are addressed in the attached document.

Response to Specific Concerns: Maltego

Concern: Inadequate Policies Defining Purpose of Use

CTO Assessment: The SIR approval process and information provided once approved will set the defined and acceptable purposes of the specific technology. Further SPD policy sets allowed uses for data in criminal investigations.

SIR Response:

Section 1.1

"Paterva's Maltego is a cyber-security software application that is used to assist Seattle Police Department (SPD) to research publicly available data and diagram associations between individuals, devices, and networks, as part of a cybercrime investigation. Maltego allows up to two authorized users in SPD's Technical and Electronic Support Unit (TESU) to trace the origin of a specific IP address, and potentially identify a suspect, that has attacked, or attempted to infiltrate, the City's network or the network of a third party. In essence, SPD utilizes Maltego to investigate cybercrimes, primarily in determining the digital origin of attacks against cyber infrastructure"

Concern: Inadequate Policies on Data Collection and Assessment

SIR Response:
Section 4.1

"Maltego queries publicly available data on the internet and collects information based on the parameters of the search request, much like Google returns results based on specific search terms. Maltego is not used to collect private data, nor is it used to process or collect internal data. It is specifically a tool used to query and diagram public information related to cyber-crime investigations. In this sense, it is collecting any publicly available information on the internet related to the specific parameters of the user request."

Section 4.7

"Only authorized SPD users can access Maltego or the data while it resides in the specific workstation where it is installed. Access to Maltego is via a password-protected software interface and the software is stored locally rather than on the network or remote server. 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. These searches, however, would look much like any search engine responses, meaning that the parameters would return only publicly available information.

Data removed from Maltego and entered into investigative files is securely uploaded and used on SPD's password-protected network with access limited to authorized 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."

Concern: Lack of Clarity Around Data Sources

SIR Response:
Section 4.1

"Maltego queries publicly available data on the internet and collects information based on the parameters of the search request, much like Google returns results based on specific search terms. Maltego is not used to collect private data, nor is it used to process or collect internal data. It is specifically a tool used to query and diagram public information related to cyber-crime investigations. In this sense, it is collecting any publicly available information on the internet related to the specific parameters of the user request."

Concern: Potential for Predictive Usages

CTO Assessment: The SIR approval process and information provided once approved will set the defined and acceptable purposes of the specific technology. Further SPD policy sets allowed uses for data in

criminal investigations. 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.

Concern: Inadequate Policies to Assess for Errors in Data Analysis

SIR Response:
Section 4.2

"Maltego is only used by two trained TESU Detectives whose primary duties involve the investigation of cyber- and other internet-related crimes. All data collected is related to a criminal investigation and included in the investigation file. If no data is collected that assists in the pursuit of the criminal investigation, this information is not retained, and no data is provided to the investigating Officer/Detective. Data, when pertinent, is exported as a spreadsheet and/or visual diagram, at which point it is handled per department policy regarding digital evidence as part of a criminal investigation. A local copy of the data is only saved if the Detective operating Maltego manually initiates a local saved copy and that is also maintained and handled per department policy"

Concern: Lack of Clarity Around Relationship with Paterva
This concern is not addressed in the SIR.

Concern: Potential for Improper Use Without Auditing/Logging

SIR Response:
Section 4.10

"SPD currently uses a free community version of Maltego that has no internal logging or auditing. A paid version includes the ability to stand up an internal SPD server that would allow for logging, but that would involve significant costs to implement and maintain. 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."

Appendix A: Glossary

Accountable: (taken from the racial equity toolkit.) Responsive to the needs and concerns of those most impacted by the issues you are working on, particularly to communities of color and those historically underrepresented in the civic process.

Community outcomes: (taken from the racial equity toolkit.) The specific result you are seeking to achieve that advances racial equity.

Contracting equity: (taken from the racial equity toolkit.) Efforts to achieve equitable racial outcomes in the way the City spends resources, including goods and services, consultants and contracting.

DON: "department of neighborhoods."

Immigrant and refugee access to services: (taken from the racial equity toolkit.) Government services and resources are easily available and understandable to all Seattle residents, including non-native English speakers. Full and active participation of immigrant and refugee communities exists in Seattle's civic, economic and cultural life.

Inclusive outreach and public engagement: (taken from the racial equity toolkit.) Processes inclusive of people of diverse races, cultures, gender identities, sexual orientations and socio-economic status. Access to information, resources and civic processes so community members can effectively engage in the design and delivery of public services.

Individual racism: (taken from the racial equity toolkit.) Pre-judgment, bias, stereotypes about an individual or group based on race. The impacts of racism on individuals including white people internalizing privilege, and people of color internalizing oppression.

Institutional racism: (taken from the racial equity toolkit.) Organizational programs, policies or procedures that work to the benefit of white people and to the detriment of people of color, usually unintentionally or inadvertently.

OCR: "Office of Civil Rights."

Opportunity areas: (taken from the racial equity toolkit.) One of seven issue areas the City of Seattle is working on in partnership with the community to eliminate racial disparities and create racial equity. They include: education, health, community development, criminal justice, jobs, housing, and the environment.

Racial equity: (taken from the racial equity toolkit.) When social, economic and political opportunities are not predicted based upon a person's race.

Racial inequity: (taken from the racial equity toolkit.) When a person's race can predict their social, economic, and political opportunities and outcomes.

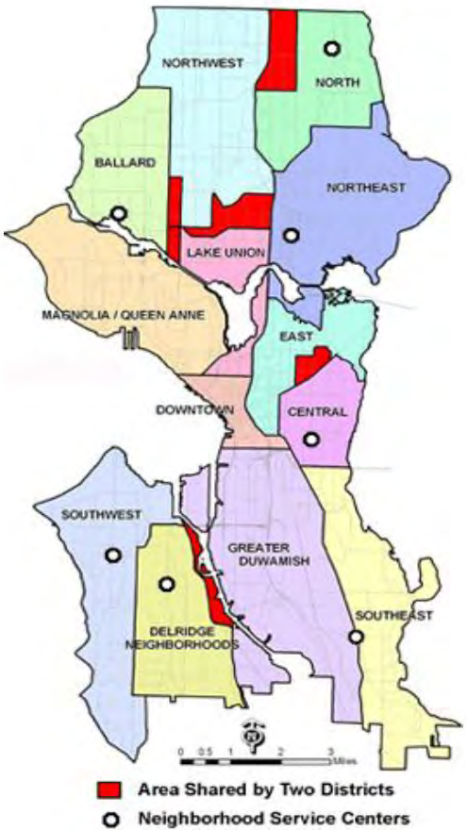
RET: "racial equity toolkit"

Seattle neighborhoods: (taken from the racial equity toolkit neighborhood.) Boundaries defined for the purpose of understanding geographic areas in Seattle.

Stakeholders: (taken from the racial equity toolkit.) Those impacted by proposed policy, program, or budget issue who have potential concerns or issue expertise. Examples might include: specific racial/ethnic groups, other institutions like Seattle housing authority, schools, community-based organizations, change teams, City employees, unions, etc.

Structural racism: (taken from the racial equity toolkit.) The interplay of policies, practices and programs of multiple institutions which leads to adverse outcomes and conditions for communities of color compared to white communities that occurs within the context of racialized historical and cultural conditions.

Surveillance ordinance: Seattle City Council passed ordinance 125376, also referred to as the "surveillance ordinance."



SIR: "surveillance impact report", a document which captures the fulfillment of the Council-defined surveillance technology review process, as required by ordinance 125376.

Workforce equity: (taken from the racial equity toolkit.) Ensure the City's workforce diversity reflects the diversity of Seattle.

Appendix B: Meeting Notice(s)

Seattle

English

Google Translate Disclaimer

Tech Talk

Seattle Information Technology

HOME TOPICS

Home / Privacy

<< Previous Next >>

Fourth Public Comment Period Opening for Technologies Subject to the City's Surveillance Ordinance

by Seattle IT on May 26, 2021

The City of Seattle has published the fourth set of draft Surveillance Impact Reports (SIRs) for four of the 26 currently existing surveillance technologies, per the Surveillance Ordinance.

The City of Seattle is looking for the public's input on the SIRs to help the provide the City Council with insight into community perspective and ensure City policies responsibly govern the use of these technologies.

The public comment period is currently open and runs through June 30, 2021. The complete list of technologies in this group for review, can be found below. We have three ways to allow residents to provide input and share their concerns:

1. Residents can submit their surveillance comments on each technology online at: City of Seattle Privacy website.
2. Seattle residents can also mail comments to Attn: Surveillance & Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124
3. City Surveillance Technology Event: The City will hold virtual events to allow attendees ask questions from department technology experts and hear from City leadership. These virtual events will take place over using Webex and participants can join via online or the phone. Links and times are as follows:

Thursday, June 10, noon to 1 p.m.
Link to join: https://seattle.webex.com/seattle/j.php?MTID=mdfa673054e3236adb179613c69692067
Phone number to call in:+1-206-207-1700
Event number (access code): 187 147 0595

Tuesday, June 29, 3-4 p.m.
Link to join: https://seattle.webex.com/seattle/j.php?MTID=me51f66a7150a8e16ca6e3220e25449fd
Phone number to call in: +1-206-207-1700
Event number (access code): 187 172 4351

More information on these technologies, as well as the City of Seattle's Privacy program, can be found online at the City of Seattle's Privacy website.

This public input period is a valuable part of our process. The City of Seattle is committed to being transparent and accountable. Hearing from residents is part of the process. We welcome your thoughts and comments and look forward to hearing them.

Seattle Police Department's Callyo

Seattle Police Department's Callyo technology is under review for public comment as a retroactive surveillance technology. This software may be installed on an officer's cell phone to allow them to record the audio from phone communications between law enforcement and suspects. Callyo may be used with consent or search warrant.

Seattle Police Department's Audio Recording Devices

Seattle Police Department's Audio Recording Device technology is under review for public comment as a retroactive surveillance technology. This technology consists of a hidden microphone to audio record individuals without their knowledge. The microphone is either not visible to the subject being recorded or is disguised as another object. Used with search warrant or signed Authorization to Intercept (RCW 9A.73.200).

Seattle Police Department's I2 iBase

Seattle Police Department's I2 iBase technology is under review for public comment as a retroactive surveillance technology. The I2 iBase crime analysis tool allows for configuring, capturing, controlling, analyzing and displaying complex information and relationships in link and entity data. iBase is both a database application, as well as a modeling and analysis tool. It uses data pulled from SPD's existing systems for modeling and analysis.

Seattle Police Department's Maltego

Seattle Police Department's Maltego technology is under review for public comment as a retroactive surveillance technology. Maltego is an interactive data mining tool that renders graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the internet.

Filed Under: Privacy
Tagged With: surveillance cameras, surveillance ordinance, Surveillance technology

20 Shares

<< Previous Next >>

Appendix C: All Comments Received from Members of the Public

ID: 12841241071

Submitted Through: Online Comment

Date: 7/23/2021 4:02:35 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Maltego

What concerns, if any, do you have about the use of this technology?

Very little time was allocated for questions from the public at the Group 4a public engagement meetings. Additionally, SPD dodged providing answers to some of the questions. As such, numerous questions from the public have not been answered and thus greatly hinder the ability for informed public comment. My open questions on SPD's use of Maltego are in the response to question #5 in this survey. Since the safest approach (security-/privacy-wise) is to assume the worst as the missing answers to these open questions, my list of concerns will do the same. Thus, these concerns include: (1) No policy defining or limiting the (CAD/etc) incident types for which SPD may enter data into or in general use Maltego. Nothing limits SPD to only use Maltego for cybercrimes. SPD could use Maltego to investigate arbitrary residents of the City. (2) SPD misleading the public via inaccurate and contradictory parts of the Maltego SIR regarding the auditability. The Maltego SIR for 8.1 says "the software's audit log keeps a record of all data accessed by each user" and 8.2 says "The free version of Maltego that is currently used is auditable"; but 4.10 says "SPD currently uses a free community version of Maltego that has no internal logging or auditing." These statements are inconsistent. 5.2 and 5.4 also fail to mention that there are no audit logs. The community version of Maltego does NOT log all the queries. It primarily seems to log errors. This technology has not been accurately or fairly described by SPD in their SIR. (3) Lack of transparency from SPD since they have not disclosed to the public which Maltego Transform Hub items are installed on SPD systems. The Transform Hub items are what dictates which types of external data is searched and pulled into Maltego. [How to list the installed transforms: Home > Maltego Transform Hub > Display = "INSTALLED"; Data Categories = none checked; Pricing = none checked; Useful for Teams = none checked.] (4) Missing information due to SPD not specifying in the SIR the data retention period for data inside Maltego. One can only safely assume that the data retention period is excessive, otherwise why hide it. (5) The potential for problematic "data fusion" of public data and non-public data, such as data obtained after a search warrant (like via digital forensics tools, etc). (6) Lack of clarity regarding whether only SPD uses Maltego or whether Seattle IT Security does as well (given the example use case provided in the SIR was investigating a ransomware attack against the City). (7) The potential for problematic "data fusion" of public data and government-owned data (given the Maltego SIR mentions SPD users having ACCESS certification, it creates ambiguity regarding whether SPD incorporates data into Maltego from any government-owned state, national, or International databases (such as DoC, DoL, WACIC, WASIS, NCIC, etc.)? (8) Lack of clarity regarding which (if any) Maltego Data Bundle(s) is SPD currently subscribed to. (9) Potential for data leakage if SPD is a Maltego Data Partner. (10) SPD naively trusting unvalidated external data. The Maltego SIR for 6.5 doesn't mention why SPD doesn't check the accuracy of the information. There can be non-unique handles, email addresses hacked, botnets running on compromised legitimate systems, etc. It's unwise to trust the results of queries without any form of validation. [For example, an IP address of www.seatle.gov (156.74.241.21) is shown in Maltego to have a fraud score of 75 (where 75 means suspicious but not necessarily fraudulent and a score of >=85 is recommended to be blocked). The fraud score of 75 seems likely incorrect (unless the City has perhaps been doing a poor job of securing their infrastructure and attackers have been leveraging the City's IP address space for malicious activity).] (11) No legal threshold must be met before Maltego-generated data is added to other SPD databases/tools (RMS/Mark43, GeoTime, etc). (12) Potential for security risk if Maltego has write access to the SPD RMS

(Mark43), as opposed to an officer manually adding data from Maltego to the RMS. (13) Lack of clarity regarding the magnitude of the use of Maltego by SPD. SPD has not specified how many incidents per year they use Maltego for. (14) SPD did not disclose to the public when the last audit of Maltego was conducted or where such an audit report might be found. (15) Lack of clarity regarding if the use of Maltego is always disclosed to the legal representative of someone facing charges for which Maltego was used in SPD's investigation.

What value, if any, do you see in the use of this technology?

It's free.

What do you want City leadership to consider about the use of this technology?

SPD shouldn't surveil residents. SPD doesn't need more tools, or more money. The community needs support so these pipelines to the criminal system are fixed. Those systemic problems aren't fixed by SPD having more tools. As such, I recommend that City leadership stop allowing use of this tool. Given City leadership's past history on prior surveillance technologies, I suspect they won't do what is fundamentally right and instead will pursue limited cosmetic changes. As such, here are some superficial changes that could be made: (1) Require SPD to answer all of the public's questions. (2) Require SPD Policy to state which specific incident types for which Meltego may be used. (3) Require SPD to accurately describe in the SIR, Maltego's Community version's auditability (specifically that it does NOT keep an audit log recording all data accessed by each user, so such information is not available to any of the entities tasked with auditing SPD). (4) Require SPD to disclose _all_ of the Maltego Transform Hub items that are installed on SPD systems. The Transform Hub items are what dictates which types of external data is searched and pulled into Maltego. [How to list the installed transforms: Home > Maltego Transform Hub > Display = “INSTALLED”; Data Categories = none checked; Pricing = none checked; Useful for Teams = none checked.] (5) Require that data that is part of an investigation be retained in Maltego for at most until the investigation is closed (if not deleted sooner). (6) Require SPD to disclose in the SIR whether they load into Maltego any non-public data obtained after a search warrant (such as via digital forensics tools, etc). (7) Require disclosure of which (if any) other City departments (besides SPD) use Maltego (such as Seattle IT Security dept). (8) Require SPD to disclose in the SIR whether they load into Maltego any non-public, government-owned data (such as from any government-owned state, national, or International databases, like DoC, DoL, WACIC, WASIS, NCIC, etc). (9) Require SPD to disclose which (if any) Maltego Data Bundle(s) SPD is currently subscribed to. (10) Ban SPD from sharing data as a Maltego Data Partner (or similar program). (11) Require SPD to independently validate data obtained via Maltego. SPD currently naively trusts unvalidated external data from Maltego. There can be non-unique handles, email addresses hacked, botnets running on compromised legitimate systems, etc. It’s unwise to trust the results of queries without any form of validation. [For example, an IP address of www.seatle.gov (156.74.241.21) is shown in Maltego to have a fraud score of 75 (where 75 means suspicious but not necessarily fraudulent and a score of >=85 is recommended to be blocked). The fraud score of 75 seems likely incorrect (unless the City has perhaps been doing a poor job of securing their infrastructure and attackers have been leveraging the City's IP address space for malicious activity).] (12) Define a minimum legal threshold that must be met before Maltego-generated data is added to other SPD databases/tools (RMS/Mark43, GeoTime, etc). (13) Improve security by requiring that SPD's Maltego system doesn't have direct read or write access to the SPD RMS (Mark43). Instead, require that an officer manually add data from Maltego to the RMS on an as needed basis. (14) Require SPD to disclose how many incidents per year they use Maltego for. (15) Require SPD to publicly provide the date and report from the most recent audit of SPD's use of Maltego. (16) Require that the use of Maltego is always disclosed to the legal representative of someone facing charges for which Maltego was used in SPD’s investigation.

Do you have any other comments or questions?

Many questions from the public have not been answered, such as: (1) Is there any policy defining the incident types for which SPD may use Maltego? (2) The Maltego SIR for 8.1 says "the software's audit log keeps a record of all data accessed by each user" and 8.2 says "The free version of Maltego that is currently used is auditable"; but 4.10 says "SPD currently uses a free community version of Maltego that has no internal logging or auditing." These statements are inconsistent. 5.2 and 5.4 also fail to mention that there are no audit logs. The community version of Maltego does NOT log all the queries. It primarily seems to log errors. Will the SIR be getting updated to accurately describe the technology? (3) What are all the installed Maltego Transform Hub items? Will the SIR be updated to include the list in an appendix? [How to list the installed transforms: Home > Maltego Transform Hub > Display = "INSTALLED"; Data Categories = none checked; Pricing = none checked; Useful for Teams = none checked.] (4) How long is Maltego-generated data retained on the TESU workstations? (5) Does SPD use only publicly available data sources for Maltego or does SPD also use Maltego with data gathered after a search warrant (such as data from forensics tools, etc)? (6) The Maltego SIR gives an example of investigating a ransomware attack against the City. Does the Seattle IT Security department not do their own incident analysis; or does IT Security also use Maltego in addition to SPD? (7) Given the Maltego SIR mentions SPD users having ACCESS certification, does SPD use Maltego to query any government-owned state, national, or International databases (such as DoC, DoL, WACIC, WASIS, NCIC, etc.)? (8) What (if any) Maltego Data Bundle(s) is SPD currently subscribed to? (9) Is SPD a Maletgo Data Partner? (10) The Maltego SIR for 6.5 doesn't mention why SPD doesn't check the accuracy of the information. There can be non-unique handles, email addresses hacked, botnets running on compromised legitimate systems, etc. It's unwise to trust the results of queries without any form of validation. Why doesn't SPD validate the accuracy of the Maltego-generated data? [For example, an IP address of www.seattle.gov (156.74.241.21) is shown in Maltego to have a fraud score of 75 (where 75 means suspicious but not necessarily fraudulent and a score of >=85 is recommended to be blocked).] (11) What legal threshold must be met before Maltego-generated data is added to other SPD databases/tools (RMS/Mark43, GeoTime, etc.)? (12) Is Maltego integrated with the SPD RMS (Mark43) or instead does an SPD officer manually add the Maltego data to the SPD RMS? (13) Roughly how many incidents per year does SPD use Maltego for? (14) SPD Policy 12.050 is referred to in multiple places in the Maltego SIR. Policy 12.050 item 12 states "The Department audits will be completed biannually and the results of these audits will be reported to the Chief Operating Officer." a) Who conducts these audits of SPD's systems (OIG, OPA)? b) Where are these reports posted (SPD website, City Clerk)? (15) Is the use of Maltego always disclosed to the legal representative of someone facing charges for which Maltego was used in SPD's investigation?

ID: 12746714616

Submitted Through: Online Comment

Date: 6/15/2021 6:31:07 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Maltego

What concerns, if any, do you have about the use of this technology?

Surveillance is always a concern.

What value, if any, do you see in the use of this technology?

Remains to be seen if there is a value.

What do you want City leadership to consider about the use of this technology?

TBD, valid considerations would depend on SPD answering the public's questions.

Do you have any other comments or questions?

1) Is there any policy defining the incident types for which SPD may use Maltego? 2) The Maltego SIR for 8.1 says "the software's audit log keeps a record of all data accessed by each user" and 8.2 says "The free version of Maltego that is currently used is auditable"; but 4.10 says "SPD currently uses a free community version of Maltego that has no internal logging or auditing." These statements are inconsistent. 5.2 and 5.4 also fail to mention that there are no audit logs. The community version of Maltego does NOT log all the queries. It primarily seems to log errors. Will the SIR be getting updated to accurately describe the technology? 3) What are all the installed Maltego Transform Hub items? Will the SIR be updated to include the list in an appendix? [How to list the installed transforms: Home > Maletgo Transform Hub > Display = "INSTALLED"; Data Categories = none checked; Pricing = none checked; Useful for Teams = none checked.] 4) How long is Maltego-generated data retained on the TESU workstations? 5) Does SPD use only publicly available data sources for Maltego or does SPD also use Maltego with data gathered after a search warrant (such as data from forensics tools, etc)? 6) The Maltego SIR gives an example of investigating a ransomware attack against the City. Does the Seattle IT Security department not do their own incident analysis; or does IT Security also use Maltego in addition to SPD? 7) Given the Maltego SIR mentions SPD users having ACCESS certification, does SPD use Maltego to query any government-owned state, national, or International databases (such as DoC, DoL, WACIC, WASIS, NCIC, etc.)? 8) What (if any) Maltego Data Bundle(s) is SPD currently subscribed to? 9) Is SPD a Maletgo Data Partner? 10) The Maltego SIR for 6.5 doesn't mention why SPD doesn't check the accuracy of the information. There can be non-unique handles, email addresses hacked, botnets running on compromised legitimate systems, etc. It's unwise to trust the results of queries without any form of validation. Why doesn't SPD validate the accuracy of the Maltego-generated data? [For example, an IP address of www.seatle.gov (156.74.241.21) is shown in Maltego to have a fraud score of 75 (where 75 means suspicious but not necessarily fraudulent and a score of >=85 is recommended to be blocked).] 11) What legal threshold must be met before Maltego-generated data is added to other SPD databases/tools (RMS/Mark43, GeoTime, etc.)? 12) Is Maltego integrated with the SPD RMS (Mark43) or instead does an SPD officer manually add the Maltego data to the SPD RMS? 13) Roughly how many incidents per year does SPD use Maltego for? 14) SPD Policy 12.050 is referred to in multiple places in the Maltego SIR. Policy 12.050 item 12 states "The Department audits will be completed biannually and the results of these audits will be reported to the Chief Operating Officer." a) Who conducts these audits of SPD's systems (OIG, OPA)? b) Where are these reports posted (SPD website, City Clerk)? 15) Is the use of Maltego always disclosed to the legal representative of someone facing charges for which Maltego was used in SPD's investigation?

ID: 12698232315

Submitted Through: Online Comment

Date: 5/28/2021 2:27:55 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Maltego

What concerns, if any, do you have about the use of this technology?

Privacy and bias

What value, if any, do you see in the use of this technology?

None

What do you want City leadership to consider about the use of this technology?

Data surveillance is just as invasive as regular surveillance. People have a right to privacy. Data models have bias built into them based on biased historical data.

Do you have any other comments or questions?

ID: 12694811517

Submitted Through: Online Comment

Date: 5/27/2021 1:26:28 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SPD: Maltego

What concerns, if any, do you have about the use of this technology?

This technology can and knowing SPD's history, almost certainly will be misused to profile individuals and groups that SPD does not like based on political affiliation, race, etc.

What value, if any, do you see in the use of this technology?

None.

What do you want City leadership to consider about the use of this technology?

Do not buy SPD more tech toys to be misused against the people of Seattle, whom they are supposed to serve and protect, not persecute and abuse.

Do you have any other comments or questions?

Defund SPD.

Appendix D: Letters from Organizations or Commissions

City of Seattle

July 23, 2021

Seattle Information Technology
700 5th Ave, Suite 2700
Seattle, WA 98104

RE: ACLU of Washington Comments on Group 4a Surveillance Technologies

On behalf of the ACLU of Washington, I write to offer our comments on the surveillance technologies included in Group 4a of the Seattle Surveillance Ordinance implementation process.

ACLU
AMERICAN CIVIL LIBERTIES UNION
Washington

P.O. Box 2728
Seattle, WA 98111-2728
(206) 624-2184
aclu-wa.org

Michele Storms
Executive Director

The four Seattle Police Department (SPD) technologies in Group 4a are covered in the following order:

1. Callyo
2. i2 iBase
3. Audio Recording Systems
4. Maltego

These comments should be considered preliminary, given that the Surveillance Impact Reports (SIR) for each technology leave a number of important questions unanswered. Specific unanswered questions for each technology are noted in the comments relating to that technology. Answers to these questions should be included in the updated SIRs provided to the Community Surveillance Working Group and to the City Council prior to their review of the technologies.

Callyo

I. *Background*

Callyo is a mobile phone identification masking and recording technology. It raises privacy and civil liberties concerns because it enables law enforcement to surreptitiously record individuals' conversations, and possibly their location data, without their knowledge or consent.

Because voice is a biometric identifier, audio data can be used to surreptitiously identify and track individuals. Any audio data collected could be used with voice recognition software that may contains inaccuracies and built-in race and gender biases.[1] Such audio could be later input into a voice recognition or biometrics database, which may further enable both corporate and government surveillance.[2]

[1] Voice recognition technologies already in use, such as Voice AI, are more likely to accurately respond to white people and men. See, for instance, Joan Bajorek, "Voice Recognition Still Has Significant Race and Gender Biases," *Harvard Business Review*, May 10, 2019, https://hbr.org/2019/05/voice-recognition-still-has-significant-race-and-gender-biases.

[2] Law enforcement agencies already use such programs and the creation of vocal recognition databases is underway. See, for instance, Michael Dumiak, "Interpol's New Software Will Recognize Criminals by Their Voices," *Spectrum.IEEE.org*, May 16, 2018, https://spectrum.ieee.org/tech-talk/consumer-electronics/audiovideo/interpols-new-automated-platform-will-recognize-criminals-by-their-voice;

SPD's possible collection of location data with Callyo raises further concerns. While an SPD representative stated that Callyo only tracks the GPS location of SPD phones and cannot collect other location data,[3] the Surveillance Impact Report (SIR) states that Callyo *is* used to GPS locate individuals.[4] The lack of clarity around SPD's collection of individuals' GPS data raises location-tracking concerns. Law enforcement can use geo-location data to conduct real-time surveillance of individuals without their knowledge or consent. Location data can reveal highly sensitive information about people's behaviors, social patterns, and personal life, including political activities in which they engage, with whom they associate, and what religion they practice. Digitally collected location data also may be improperly and inaccurately used in criminal investigations.[5] Location tracking therefore impinges upon basic privacy and due process rights and impedes individuals' abilities to enjoy their everyday lives free from fear of surveillance.

SPD's use of Callyo raises serious concerns. SPD policies described in the SIR do not include purpose limitations, adequate privacy and security protections, or clear restrictions on use. The SIR does not include a contract with the vendor, Motorola Solutions, and it is unclear whether there are contractual restrictions on data use and sharing.

Given the lack of adequate policies described by the SIR and the number of unanswered questions that remain, we have concerns that SPD's use of Callyo may infringe upon people's civil rights and civil liberties.

II. *Specific Concerns*

a. **Lack of Clarity Around Requirements for a Warrant:** The SIR states that Callyo's functions can only be used with a court order.[6] Elsewhere, the SIR states that Callyo's call recording functions may only be used with a search warrant.[7] However, the city's webpage states, "Callyo may be used with consent or search warrant."[8] Comments at the June 10th and July 20th public engagement meeting also suggested that consent might be sufficient to use Callyo. Clarity is needed as to whether current rules allow officers to use some features of Callyo based on consent alone. Such clarity is particularly important because the SIR repeatedly states that the search

---

"Speaker Identification" *GoVivace.com*, Accessed June 10, 2021, https://www.govivace.com/products/speaker-identification/; "Voice Authentication," *Aware Biometrics*, Accessed June 10, 2021, https://www.aware.com/voice-authentication/; 'Forensic Voice Analysis," *Sestek.com*, Accessed June 10, 2021, https://www.sestek.com/forensic-voice-analysis/; "Voice Inspector for Forensic Experts," *Phonexia.com*, Accessed June 10, 2021, https://www.phonexia.com/en/use-case/audio-forensics-software/.

[3] City of Seattle IT Department, "Group 4a Surveillance Technologies Public Meeting 1 20210610 1903 1," Accessed July 21, 2021, https://www.youtube.com/watch?v=I0FVEt2oyY8.

[4] Seattle Police Department, "2021 Surveillance Impact Report: Callyo," Accessed June 7, 2021, https://www.seattle.gov/Documents/Departments/Tech/Privacy/Public%20Engagement%20SIR%20-%20Callyo.pdf, 5-7.

[5] "Police Could Get Your Location Data Without a Warrant. This Has to End," *Wired*, February 2, 2017, https://www.wired.com/2017/02/police-get-location-data-without-warrant-end/.

[6] SPD, "Callyo," 5.

[7] Ibid., 7, 10, and 11.

[8] "Surveillance Technologies Under Review," *Seattle.gov*, Accessed June 6, 2021, https://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies.

warrant determines what data can be properly collected via Callyo.[9] Uses of Callyo based on consent alone would not be subject to such parameters. The SIR fails to specify when officers can request consent and what content can be recorded based on that consent. Improper data collection is probable absent clearer guidelines.

b. **Inadequate Policies Defining Purpose of Use.** The SIR does not fully describe the circumstances under which Callyo may be used. It is unclear when call-masking may be used and whether Callyo is the only recording application that SPD uses to record calls. Without clear purpose restrictions, officers may record conversations widely, amassing unnecessary sensitive data and voice biometrics. Similarly, officers may inappropriately use call-masking technologies outside of any specific criminal investigation and undermine expectations of government transparency.

c. **Lack of Clarity on How Callyo May be Used and By Whom.** The SIR primarily addresses how a non-HRVU (High-Risk Victims Unit) officer or detective would have TESU (Technical and Electronic Support Unit) record their call. Any difference in process for recording the calls of non-officers (i.e. calls made by cooperating witnesses) is not detailed. The HRVU's Callyo use parameters are also only partially explicated,[10] despite HRVU's larger share of the annual Callyo budget.[11] Without comprehensive guidelines ensuring that appropriate usage is tracked and data is properly managed, sensitive information may be improperly shared and tools like call masking may be used improperly.

d. **Lack of Clarity on Motorola Solutions' Data Collection and Retention.** The SIR does not describe a contract between SPD and Motorola Solutions, leaving it unclear whether Motorola collects or retains data. While the SIR indicates that no "sharing partners" have "direct access" to Callyo data "while it resides in the [mobile phone] device,"[12] it is unclear what access there is to data that no longer resides in the devices and may instead be stored in Callyo's cloud.[13] While SPD stores Callyo recordings on its own systems, the SIR does not make clear whether data initially recorded in Callyo's app is also uploaded to Amazon Web Service's GovCloud, which hosts Callyo's cloud and appears to store its data.[14] When asked about possible Motorola collection of Callyo data during the July 20th public engagement meeting, the SPD representative expressed uncertainty as to whether the vendor might access or store some data. If data is stored on Callyo's cloud system without contractual restrictions, Motorola Solutions may be able to review and parse private recording data, or even share or sell that data to third parties. The SIR does not mention any such

[9] SPD, "Callyo," 10, 11, 13, and 17.
[10] Ibid., 7-11.
[11] Ibid., 18.
[12] Ibid., 14.
[13] "Investigative Solutions," *Callyo.com*, Accessed June 16, 2021, https://callyo.com/investigations/investigative-solutions.
[14] "Callyo," *Amazon Web Services*, https://partners.amazonaws.com/partners/0010L00001pPHaFQAW/Callyo; "10-21 Video" *Callyo.com*, Accessed June 7, 2021, https://callyo.com/public-safety/10-21-video.

3

cloud storage or other data collection by Motorola Solutions, leaving open the possibility that Motorola has access to highly sensitive information.

e. **Inadequate Data Sharing Policies.** The SIR offers only an extremely general description of who might receive Callyo data and how such data would be shared.[15] Neither security protocols for transferring data nor for ensuring that shared data is properly deleted are explicated in the SIR. Indefinite retention of data and insecure sharing processes could lead to exposure of sensitive data, with manifold consequences for those recorded – from safety risks for witnesses to discovery of private information by employers.

f. **Inadequate Data Retention Policies.** The SIR states that devices that collect no relevant evidence, per the terms of the court order, are purged in their entirety by TESU staff and no data is provided to the investigating officer.[16] However, protocols to ensure that TESU staff properly execute these determinations are not detailed fully. Additional clarity is needed as to how deletions are determined, and how frequently supervising officers review the data that is shared with investigating officers.[17] Indefinite and improper data storage could lead sensitive data to be shared publicly or could lead SPD officers to use improperly collected data in the course of an investigation – subjecting those investigated to an overreach of police powers.

g. **Inadequate Oversight Policies.** Callyo advertises that the call masking on its 10-21 phone application "diverts millions of calls away from dispatch centers each year" by enabling officers to communicate with members of the public directly.[18] SPD does not provide data on the number of calls that might be diverted, but any such calls would no longer be subject to the systematic tracking and oversight which centralized dispatch systems provide. This arrangement makes it easier for individual officers to unilaterally control communications with members of the public and use that communication control to abuse their power.

h. **No Policies Restricting Use of Callyo's Additional Surveillance Features.** Callyo can be integrated with other law enforcement-focused Amazon Web Services technologies in ways that makes it surveillance capabilities more forceful.[19] Callyo also includes numerous additional surveillance features, such as video recording and live-streaming[20] and "10-

---

[15] SPD, "Callyo," 14-16.
[16] Ibid., 7 and 10.
[17] See "Supervisors and commanding officers are responsible for ensuring compliance with policies," at SPD, "Callyo," 9.
[18] "Spotlight: Callyo is Changing the Way Investigations Are Done," *Police 1*, March 12, 2019, https://www.police1.com/police-products/investigation/articles/spotlight-callyo-is-changing-the-way-investigations-are-done-JgCBKAD5Mmn9y27J/.
[19] AWS Public Sector Blog Team, "Harnessing the Power of the Cloud: Startups Deliver Innovative Services to Public Agencies Faster," *AWS Public Sector Blog*. Accessed June 16, 2021, https://aws.amazon.com/blogs/publicsector/harnessing-the-power-of-cloud-startups-deliver-innovative-services-to-public-safety-agencies-faster/.
[20] "Police Body Camera App," *10-21 Video.com*, Accessed June 16, 2021, https://10-21.com/; "10-21 Video," *Callyo.com*.

21 Flight," which allows officers to perform surveillance using drones.[21] The SIR describes no policy which would prevent SPD from using these Callyo features in the future. Videos captured by Callyo could be stored and later entered into facial recognition programs, which have been widely found to be racially biased.[22] Flight-based video tools can be and have been[23] used to track and observe protestors, improperly subjecting political organizers to targeted surveillance and chilling freedoms of speech and association.

III. *Outstanding Questions That Must be Addressed in the Final SIR*

- Is location data collected via Callyo? If so, how and when is location tracked and what policies govern recording and storage of location data?
- Can Callyo be used without a warrant, based on two-party consent alone? If so, when may it be used without a warrant, how is consent obtained, and what rules set the parameters for Callyo's use?
- When Callyo is used on calls between a third party (i.e. a cooperating witness) and an unknowing participant, how does the recording process differ compared to Callyo's use for recordings of officers in phone conversations?
- How and when is call masking used and what policies govern usage of that feature?
- How does the HRVU use Callyo and what guidelines govern its use? Does the HRVU ever use Callyo functions besides call masking, such as location tracking?
- Is any data collected through HRVU usage of Callyo – such as the phone numbers called – and how is that data stored and/or shared?
- Does SPD have a contract with Motorola Solutions for its use of Callyo? If so, what are the agreement's provisions?
- Where are audio recordings initially stored? Are they ever stored anywhere besides the original recording device and the thumb drive submitted to the investigating officer, such as on the Callyo cloud?
- Who owns the data collected by Callyo? Does Motorola have access to or store the collected data at any point? If so, what are Motorola's data security practices with respect to the data collected?
- How is data shared with third parties? How is shared data monitored for deletion within the appropriate time frame?

IV. *Recommendations for Regulation*

Pending answers to the questions above, we can make only preliminary recommendations for regulation of Callyo. SPD should adopt clearer and enforceable policies that ensure, at a minimum, the following:

---

[21] "10-21 Flight," *Callyo.com*, Accessed June 7, 2021, https://callyo.com/public-safety/10-21-flight.
[22] Kade Crockford, "How is Face Recognition Surveillance Technology Racist?" *ACLU.org*, Accessed June 16, 2021, https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist/.
[23] "U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance," *The New York Times*, June 19, 2020, https://www.nytimes.com/2020/06/19/us/politics/george-floyd-protests-surveillance.html.

- There is a specific and restricted purpose of use. The ordinance should define clear limits on Callyo's uses, including narrow parameters for Callyo's consent-based uses.
- All data collected through Callyo must follow the issuance of a search warrant, or a clearly delineated consent process that sets enforceable rules limiting the types of data that may be collected.
- Data is securely shared with third parties and properly deleted.
- Any data collected by Motorola is not owned by, used by, or retained by Motorola, and any data housed on the Callyo cloud is properly secured.
- There must be clear accountability processes for ensuring TESU officers delete improperly recorded data that falls outside the scope of a search warrant or consent statement and do not share it with investigating officers.
- There must be clear guidelines for securely storing and managing any data collected by Callyo outside of call recordings, such as location data, and provisions to ensure the deletion of any such data collected that does not fall within the scope of a search warrant or consent agreement.

i2 iBase

I. *Background*

IBM i2 iBase is a database application that raises serious privacy and civil liberties concerns because it can operate as a surveillance dragnet and can perform automated social network analysis (SNA), which likely exacerbates disproportionate surveillance and policing of marginalized communities.

iBase is used by law enforcement to identify and analyze network connections and patterns within input data, conduct SNA or "link analysis," and share data with other agencies.[24] SPD uses i2 iBase in partnership with a second IBM application, i2 Analyst's Notebook,[25] which is "a visual analysis tool" that includes "connected network visualizations, social network analysis, and geospatial or temporal views to help… uncover hidden connections and patterns in data."[26] Together, these tools can search massive pools of data to find similarities and connections between entities and individuals, then produce maps and charts that represent the relationships or groups identified. The "Search 360" function in iBase allows officers to perform complex queries of stored records, expanding data search capabilities beyond those offered by existing records systems.[27]

iBase also allows for new ways of viewing data, and includes features not described in the SIR. It can generate heat maps and find "hidden connections" via the "Find

[24] "IBM Security i2 iBase: FAQs," *IBM.com*, Accessed June 10, 2021, https://www.ibm.com/products/i2-ibase.
[25] Seattle Police Department, "2021 Surveillance Impact Report: Link Analysis Software – IBM i2 iBase," Accessed June 9, 2021, https://www.seattle.gov/Documents/Departments/Tech/Privacy/Public%20Engagement%20SIR_%20Link%20Analysis_IBM%20i2%20iBase.pdf, 7.
[26] "IBM Security i2 Analyst's Notebook," *IBM.com*, Accessed June 10, 2021, https://www.ibm.com/products/i2-analysts-notebook.
[27] "IBM Security i2 iBase: Details," *IBM.com*, Accessed July 23, 2021, https://www.ibm.com/products/i2-ibase.

Connected Network" tool, which identifies a network that "directly or indirectly" connects several entities of interest.[28]

The SIR suggests that iBase is generally employed in two contexts. First, SPD's Real Time Crime Center (RTCC) uses iBase to rapidly provide information to officers responding to incidents.[29] The RTCC is a "centralized data and logistics hubs" that allows analysts to provide data to officers on the street.[30] Second, investigating officers use iBase to collect and organize timeline and relationship data for cases in progress.[31]

Although SPD describes using iBase only to assess RMS and CAD data, iBase can process larger data pools and operate as a data dragnet. For instance, the Durham, NC Police Department has considered importing city utility data, recreational park logs, and daily jail visitor lists into iBase.[32] A law enforcement-focused Open Source Intelligence integration is now available for iBase Analyst's notebook. The integration allows "customers to use not only the internal data available on the platform, but also to collect and analyze a wealth of further information through open sources."[33] This "further information" is public, but still raises privacy concerns when collected en masse and utilized for policing; for instance, the information could include social media data and geolocation history.[34] The SIR does not describe any SPD policy that would prevent additional data from being added to iBase. During the July 20th public engagement meeting, the SPD representative expressed uncertainty as to whether outside information was being used in SPD's iBase.

The data analysis and matching performed by SNA tools like iBase can often be inaccurate. Data may become outdated or be entered incorrectly or in different formats.[35] Such errors are difficult to catch when data is processed at this scale. The analysis process can perpetuate these inaccuracies by integrating errors into the visualizations produced and generating linkages between people who have no relationship. For instance, a one-letter typo in an address might lead someone to be inaccurately connected to a household miles away. An outdated address might generate a connection with a location or person someone has not visited for years. These inaccuracies can compound existing police bias; those who have previously interacted with the police – who are disproportionately Black, Latinx, and

---

[28] "IBM Security i2 Analyst's Notebook: Feature Spotlights," IBM.com, Accessed June 10, 2021, https://www.ibm.com/products/i2-analysts-notebook/details.
[29] SPD, "IBM i2 iBase," 5.
[30] Seattle Police Department Public Affairs, "SPD Announces Agile Policing Strategy, Unveils Real-Time Crime Center," *spdblotter.seattle.gov*, October 7, 2015, https://spdblotter.seattle.gov/2015/10/07/spd-announces-agile-policing-strategy-unveils-real-time-crime-center/.
[31] SPD, "i2 iBase," 5-6.
[32] "Digital Dragnet: How Data Became a Cop's Best Weapon," *GCN*, November 29, 2011, https://gcn.com/Articles/2011/12/05/Predictive-policing-tech-feature.aspx?Page=2.
[33] "Social Links Brings the OSINT Solution to IBM's i2 Analyst's Notebook Platform," *SocialLinks.io*, Accessed June 10, 2021, https://blog.sociallinks.io/https-blog-sociallinks-io-social-links-brings-the-osint-solution-to-ibms-i2-analysts-notebook-platform/.
[34] "SL Pro on IBM i2 Analyst's Notebook," *SocialLinks.io*, Accessed June 11, 2021, https://blog.sociallinks.io/sl-pro-on-ibm-i2-analysts-notebook-product-launch-and-practical-application/.
[35] Timothy Crocker, "The Power of Social Network Analysis," *Police Chief Magazine*, Accessed June 11, 2021, https://www.policechiefmagazine.org/power-social-network-analysis/.

7

Indigenous[36] – are more likely to have data in RMS or CAD that could lead to a false "linkage" to a person of interest and subject that person to surveillance and unwarranted interactions with police.

The SIR acknowledges that i2 iBase and the Analytics notebook are used as tools within the field of social network analysis (SNA).[37] SNA is a problematic mode of analysis, in part because it is often used for predictive policing via "heat-mapping." iBase advertises such features.[38] Any tool potentially useful for predictive policing raises well-documented civil liberties concerns, including reproducing existing biases and compounding the surveillance of neighborhoods which return higher crime data because they are over-policed.[39]

Utilizing relationship analysis in conjunction with other more common predictive policing tools also raises new threats. For instance, rather than identifying specific locations where gun violence is likely to occur, SNA predictive policing may aim to identify *specific individuals* likely to face gun violence[40] – an entirely new level of invasive surveillance and data targeting. The SIR does not describe predictive policing uses of iBase, but such uses are also not prohibited. Given RTCC's mission, it seems entirely conceivable that iBase data could be used to predict threats and re-direct officers. Unless governed by narrowly tailored guidelines, iBase has the potential to compound issues already present in SPD's existing predictive policing apparatus.

RTCC use of SNA technology also raises freedom of association concerns. Without proper regulation, SNA tools could be used with open source data to pull up details not only on the subject of the incident, but on all of their associations – for instance, criminal records for a brother, parent, or Facebook friend. That information may influence an officer's response to the situation; after all, RTCC

---

[36] Factors including biased policing, discriminatory school discipline policies, and community over-policing mean that Latinx, Black, and Indigenous people are more likely to interact with police, be stopped by police, and be searched by police – leading to the creation of notes or an entry in a system like CAD or RMS. These differences are well-documented nationally and in Seattle. See, for instance, David Kroman, "Report Shows Seattle Policing Still Disparate Along Racial Lines," *Crosscut*, May 1, 2019, https://crosscut.com/2019/05/report-shows-seattle-police-enforcement-still-disparate-along-racial-lines; Elizabeth David, et al, "Contacts Between the Police and Public, 2015," *Bureau of Justice Statistics Special Report*, October 2018, "Findings," *Stanford Open Policing Project*, Accessed June 11, 2021, https://openpolicing.stanford.edu/findings/; Kim Eckart, "How a Police Contact by Middle School Leads to Different Outcomes for Black, White Youth," *Washington.edu*, December 3, 2020, https://www.washington.edu/news/2020/12/03/how-a-police-contact-by-middle-school-leads-to-different-outcomes-for-black-white-youth/; https://bjs.ojp.gov/content/pub/pdf/cpp15.pdf; Robert Crutchfield., et al, "Racial Disparity in Police Contacts," *Race Justice* 2, no.3 (July 1, 2012): 10, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3868476/;

[37] SPD "IBM i2 iBase," 6.

[38] "IBM Security i2 Analyst's Notebook: Feature Spotlights," *IBM.com*, Accessed June 10, 2021, https://www.ibm.com/products/i2-analysts-notebook/details; "Durham Police Department," *IBM.com*, Accessed July 23, 2021, https://www.ibm.com/case-studies/durham-police-department.

[39] Tim Lau, "Predictive Policing Explained," *The Brennan Center for Justice*, April 1, 2020, https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained; Jared Friend, "Seattle's New Crime Analytics Program Threatens to Perpetuate Racism in Policing," *ACLU-WA.org*, October 20, 2015, https://www.aclu-wa.org/blog/seattle-s-new-crime-analytics-program-threatens-perpetuate-racism-policing.

[40] Andrew Papachristos and Michael Sierra-Arevalo, "Policing the Connected World," *Department of Justice Community Oriented Policing Services*, 2018, https://www.hsdl.org/?view&did=814315; Reichart, et.al. "Focused Deterrence: A Policing Strategy to Combat Gun Violence," *ICJIA Research Hub*, Accessed July 23, 2021, https://icjia.illinois.gov/researchhub/articles/focused-deterrence-a-policing-strategy-to-combat-gun-violence.

pulls this data with the goal of informing officers' actions. Use of that data may prompt more aggressive policing on the basis of association alone, exacerbating existing biases in street policing. If additional data is imported into iBase, it is possible other kinds of associations and affiliations could also be identified and immediately sent to police, such as membership in Facebook groups or job history.

II. Concerns

a. **Bias and Inaccuracies in Computer-Automated Social Network Analysis.** As outlined above, iBase's automated relationship analyses are likely to generate data errors that compound existing biases. SPD does not indicate how often incorrect connections are identified, but they have confirmed that false connections do occur. To protect against these errors, the SIR indicates that relationship analysis will be "developed manually by analysts."[41] However, that claim conflicts with assertions that iBase's automated processing will "create[e] relevant intelligence from large amounts of data,"[42] and will create new "efficiencies" by avoiding manual data management.[43] Manual analysis also seems time-prohibitive in rapid-response scenarios. Even if SPD only analyzes relationships manually, the SIR never fully explains what safeguards are embedded into that manual analysis to ensure data is fully reviewed and erroneous connections deleted.

b. **Lack of Clarity on Purpose of Use and Usage Limits.** The SIR does not fully explain use cases for iBase and does not include policies placing limits on its uses.

   i. **Rapid Response Uses.** The SIR indicates that RTCC uses the social network analysis provided by iBase to provide "actionable information"[44] to officers in the field but does not thoroughly explain how that information is used by offices or why it is helpful. It is therefore difficult to assess the full extent of civil liberties concerns presented by the in-the-field uses of the technology and to assess SPD's need for the technology.

   ii. **Need for a Criminal Investigation.** The SIR does not specify at what point someone's data is consolidated and viewed in iBase. Based on the contemplated RTCC uses of the technology, it seems that a formal criminal investigation does not need to be opened before data can be pulled and visualized in iBase. Rather, anyone who is merely the subject of a 911 call might be analyzed using iBase.

   iii. **Visualization vs. Predictive Policing.** Without clearer usage limits, data compiled via iBase might be used for predictive policing.

[41] SPD, "IBM i2 iBase," 27.
[42] Ibid., 7.
[43] Ibid., 6, 21, and 27.
[44] Ibid., 10.

c. **Lack of Clarify Around Types of Data Stored and Processed.** In the SIR, SPD does not specify what portion of existing data is automatically imported into iBase, and what kinds of data have been manually inputted.[45] The lack of information on data currently included or potentially included in iBase raises numerous concerns.

   i. **Lack of Limits on Data Imported.** The SIR indicates that additional data can be "manually imported" into the system[46] and suggests that officers would manually input only single "piece[s] of data."[47] However, it does not specify a policy limiting the kinds of data that can be manually inputted or that would prevent automatic import of outside data. The lack of such restrictions is concerning given iBase's potential to operate as a dragnet with a disparate surveillance impact.

   ii. **Biased Data Selection.** Biases likely already exist in the data imported from RMS and CAD. Members of over-policed communities are far more likely to appear in SPD systems and are therefore more likely to appear in iBase relationships analyses and be subjected to police investigation resulting from false linkages. The SIR also states that only some portions of RMS and CAD data are automatically imported into iBase. If so, the data selection parameters used could introduce additional bias. For instance, importing data only for certain types of incidents or from certain locations could compound the racial and economic disparities already present in the data. The SIR does not indicate whether SPD has completed a disparate impact assessment of the linkages iBase generates, nor whether any policies exist which might mitigate this disparate impact. When asked what portion of data is imported into iBase, the SPD representative implied that only difficult to import data was excluded, but the inclusion parameters were not fully described.

d. **Lack of Clarity Regarding Contract with IBM.** The SIR does not indicate whether SPD has a contract with IBM and does not describe the provisions of any such contract. It is therefore difficult to assess what future uses of iBase might be possible, what kinds of data might be imported, and what data security mechanisms are in place. Although the SIR states that data is maintained on SPD servers and is entered into iBase via a one-way server transfer, the SIR does not describe enforceable provisions which could prevent future IBM use or review of data and analyses from iBase.

e. **Lack of Clarity on Data Security.** The SIR does not fully describe data security measures that would prevent third-party access to sensitive iBase relationship analyses and searches.

[45] Ibid., 7.
[46] Ibid.
[47] Ibid., 6.

i. **Data Deletion.** The SIR states that manually entered data will be automatically deleted after five years.[48] It is not clear why there is a lengthy five-year retention period. The SIR also does not specify what systems or oversight mechanisms are in place to ensure that data is deleted. This is particularly concerning given the lack of limits on manual data inputs, as outlined above.

ii. **Incidental Data Access.** The SIR specifies, "incidental data access may occur through delivery of technology client services."[49] However, it does not describe the specific scenarios in which this data access might occur, nor what kind of data would be viewed, leaving open the possibility that significant elements of analysis generated by iBase could be released to third-party entities.

III. *Outstanding Questions that Must be Addressed in the Final SIR*

- Which "portion" of SPD RMS and CAD data is automatically imported into iBase? How often does the data used generate erroneous relationship linkages?
- Has an equity assessment been performed on the portion of the data transferred? What biases exist in the data, and how does SPD ensure that the biases present in the social network analyses conducted with this software do not cause disparate impact?
- Are there any limits on the kinds of data that can be manually inputted into the system? Has there been an evaluation of what kinds of data have been manually inputted thus far?
- Are there any policies that would prevent other kinds of data from being imported into iBase in the future?
- How is manual relationship analysis performed using iBase, and what specific safeguards exist within the analysis process to prevent erroneous connections? Does SPD ever use the automatically-generated relationship maps created by iBase or Analyst's notebook, without verifying the accuracy of all the many data points involved?
- Is data compiled via iBase ever used for predictive purposes, rather than mere visualization? Are there any policies that would prevent its use for predictive purposes in the future?
- How does RTCC use the social network analysis provided by iBase to provide "actionable information"[50] to officers in the field? What kinds of actionable information would this include, and why would such data be necessary or helpful?
- At what point can someone's data be consolidated and viewed in iBase?
- What systems ensure that manually entered data is deleted automatically?
- What circumstances might lead to "incidental" data access, and what data would be viewed? Could only ITD employees potentially obtain "incidental data access?"
- Does SPD have a contract with IBM, and if so, what are its provisions?

[48] Ibid., 10.
[49] Ibid., 11.
[50] Ibid., 10.

IV. *Suggestions for Regulation*

Pending answers to the to the questions above, we can make only preliminary recommendations for regulation of IBM's i2 iBase and Analyst's Notebook. SPD should adopt clearer and enforceable policies that include, at a minimum, the following:

- A regular audit to assess for biases in the data imported into iBase and in the analyses generated by iBase.
- Limits on the kinds of data that may be inputted both manually and automatically into iBase, ensuring that additional pools of public or private information are not added in the future.
- A shortened data retention period that does not exceed the time necessary to conduct a criminal investigation.
- A clear deletion oversight process to ensure that manually added data is deleted after the specified retention period.
- A manual relationships analysis process that includes clear checkpoints designed to ensure erroneous data and inaccurate linkages generated by iBase are detected and corrected before they are actively investigated.
- Limits on the usage of potentially erroneous iBase analyses and search data in rapid response settings where manual analysis is not possible.
- Clear purpose of use limits, restricting when someone's relationship network may be assembled in iBase, such as a requirement that a criminal investigation be opened before such an analysis is begun, to prevent the widespread use of iBase analysis on all individuals encountering the police.
- A regulation banning the use of iBase for predictive policing.
- A contract with IBM that ensures IBM never possesses, uses, or accesses SPD data.

Audio Recording Systems

I. *Background*

"Wires" are concealed audio recording devices, generally used to record in-person conversations pursuant to a search warrant. This type of technology poses serious privacy and civil liberties concerns. If people do not have the knowledge and assurance that private communications are, indeed, private, habits based upon fear and insecurity will gradually replace habits of freedom, chilling people's civil rights and liberties.

"Audio recording systems" include devices hidden on a person, in an object, or in a location and used to record audio, following consent or search warrant authorization.[51] The SIR does not specify the particular audio recording technology

[51] Seattle Police Department, "2021 Surveillance Impact Report: Audio Recording Systems ('Wires')," accessed June 4, 2021, https://www.seattle.gov/Documents/Departments/Tech/Privacy/Public%20Engagement%20SIR%20-5%20Audio%20Recording%20Systems.pdf, 4.

used by the department, outside of the Callyo call recording technology discussed above. At the June 10th public engagement meeting, an SPD representative indicated that some technologies that fall under this SIR may be able to record video, though the SIR states video devices are described in a separate SIR.[52] Although the SIR is unclear about the type or model of devices used, at the July 20th public engagement meeting, SPD representatives suggested that the devices used were mostly relatively new devices – not legacy "wires" or tape recorders – and were typically small, handheld recorders or officers' cell phones.

Many new audio wire technologies are substantially similar in function to traditional recording devices but may be far smaller and have improved audio quality and storage capacity, making them easier to conceal and surveillance easier to perform. Improved audio filtering and increased wearer comfort mean devices can be used in a wider array of settings irrespective of noise, can pick up sound from much further away, and can be worn for longer periods of time. Transmissions from planted devices can also be streamed to remote computers so that law enforcement need not be near the conversation recorded.[53] Modern devices are therefore capable of widespread and complex surveillance not contemplable even 15 years ago. Increased storage capacity and ease of data deletion also make device misuse more likely; officers can now leave a device running in a public place where third-party conversations can be captured, then try to later delete excess data improperly collected.

Improved audio quality and increasingly sophisticated audio-processing software also pose new threats. Law enforcement agencies already employ software that can identify and match voices, and voice databases are being developed.[54] The use of this software, in conjunction with mass police storage of high-quality audio recordings, poses a risk of easy but possibly inaccurate or biased government identification and surveillance of those recorded. SPD acknowledges that audio recordings may be shared with other agencies, including other law enforcement departments.[55] As such, even if SPD would need to undergo a review process before acquiring voice recognition technologies, the voices of those recorded by SPD could easily become part of other agencies' voice recording databases. SPD audio recordings could therefore become a permanent biometric record, much like a fingerprint. Given these new and developing risks, it is necessary to set narrower limits on uses of audio-processing software, sharing of audio data, and uses of recorders.

---

[52] Ibid., 6.
[53] Wendy Ruderman, "Is Someone Recording This? It's Harder to Find Out," *The New York Times*, April 7, 2013, https://www.nytimes.com/2013/04/08/nyregion/secret-recording-grows-safer-as-the-wire-grows-tinier.html; Laurie Mason Schroeder, "'Wearing a Wire' in the Digital Age: Smaller, Safer, More Comfortable," *The Morning Call*, February 3, 2018, https://www.mcall.com/news/police/mc-nws-allentown-city-hall-investigation-wiretaps-20180201-story.html.
[54] Michael Dumiak, "Interpol's New Software Will Recognize Criminals by Their Voices," *Spectrum.IEEE.org*, May 16, 2018, https://spectrum.ieee.org/tech-talk/consumer-electronics/audiovideo/interpols-new-automated-platform-will-recognize-criminals-by-their-voice; "Speaker Identification" *GoVivace.com*, Accessed June 10, 2021, https://www.govivace.com/products/speaker-identification/; "Voice Authentication," *Aware Biometrics*, Accessed June 10, 2021, https://www.aware.com/voice-authentication/; "Forensic Voice Analysis," *Sestek.com*, Accessed June 10, 2021, https://www.sestek.com/forensic-voice-analysis/; "Voice Inspector for Forensic Experts," *Phonexia.com*, Accessed June 10, 2021, https://www.phonexia.com/en/use-case/audio-forensics-software/.
[55] SPD, "Audio Recording Systems ('Wires')," 12.

13

II. *Specific Concerns*

a. **Lack of Clarity Around How Devices Are Used.** The SIR does not specify the scenarios in which officers may use recording devices, saying that "[SPD] utilizes audio recording systems in a handful of ways to obtain information during a criminal investigation."[56] It is difficult to assess the necessity of audio recordings without clarity as to how devices are used and where they may be used. Although audio recordings are helpful in some scenarios, some audio recordings – particularly those authorized only by two-party consent – may be unjustified given the privacy concerns posed by audio recording. SPD never describes how frequently audio is recorded or how often improper recordings are captured, making it difficult to assess the current process's flaws.

b. **Lack of Clarity Around Warrant and Consent Procedures.** The SIR indicates that either a warrant or consent may authorize use of a recording device.[57] However, neither the SIR nor the June 10th or July 20th public engagement meetings provided a thorough description of the consent process. It is unclear whether SPD has a clear consent script or guidelines for determining what recordings are permissible. It is important that individuals know precisely what they are consenting to and how they can opt out of being recorded. Without clear processes, SPD may be capturing and retaining audio that falls neither clearly within the terms of the party's consent nor outside of them. Retaining any such audio undermines the privacy expectations embodied in Washington's two-party consent laws. Additionally, without clear guidelines, decisions about which recordings to keep are likely to be made arbitrarily or in ways informed by bias.

c. **Lack of Adequate Safeguards Against Improper Data Collection Prevention.** The SIR specifies data deletion practices that prevent improperly collected data from being retained, pursuant to the terms of a warrant or the terms of a party's consent. However, it does not outline formal usage guidelines that would prevent improper recordings from ever being collected. The additional storage capacity and audio sensitivity of today's recording make it far more likely that an officer might turn on a device early or leave it on too long and capture third-party conversations before and after any conversation of interest. Even carefully timed recordings might capture private background conversations. Although such data might eventually be deleted, those conversations will be temporarily stored, then reviewed by a member of SPD staff. The capture, review, and temporary storage of recordings of citizens who have not consented and are not subject to a warrant constitutes a serious privacy violation, particularly given the highly personal, identifiable information which might be collected.

[56] Ibid., 4.
[57] Ibid.

14

d. **Lack of Clarity on Types of Devices Used.** The SIR does not specify the manufacturer or function of devices used.[58] This is particularly concerning given that officers are using their phones to record, which may involve the use of a third-party application or software.

e. **Lack of Clarity on Specific Data Extraction Software.** The SIR states that completed recordings are "…extracted onto a thumb drive from the device using a locally stored computer application…. This application… is used solely to extract audio data from a device and stores no data."[59] The type of application and its features are never detailed. As such, we cannot analyze the security of the software. Presumably some second software is also used to delete parts of recordings that are improperly collected. That software and its features are also not specified.

f. **Inconsistencies in Deletion Policies.** The SIR states that the TESU officer is responsible for purging improperly collected data,[60] but also that the investigating officer is responsible for the purge.[61] If no one person is accountable for data deletion, some improperly collected data may never be purged. Additionally, if the investigating officer can complete the deletion, they necessarily may access and review improperly collected recordings. The review, use or retention of such unauthorized recordings constitutes a clear violation of 4th amendment rights and Washington consent laws.

g. **Security Risks Associated with Third Party Data Sharing.** The SIR describes third-party data sharing only vaguely.[62] It does not describe the sharing process, nor how data security will be maintained. The lack of data security measures increases the likelihood that third parties will improperly expose, retain, or share private data. It is also unclear whether audio recordings shared with partner law enforcement agencies or other jurisdictions – who are not subject to the same surveillance regulations – are shared permanently, or whether any protocols are in place to ensure that shared data is later deleted.

h. **Inconsistencies in Audio Device Request and Management Process.** The SIR is inconsistent in describing how TESU officers process requests for audio device usage. The SIR in one place states that the investigating officer completes the audio device request form[63] but elsewhere states that TESU does so.[64] The request form is designed to ensure that officers obtain consent or a warrant before a device is issued. Therefore, an unclear request process increases the probability of unauthorized device use and improper private data collection.

---

[58] Ibid., 5 and 16.
[59] Ibid., 8.
[60] Ibid., 6.
[61] Ibid., 11.
[62] Ibid., 12.
[63] Ibid., 10.
[64] Ibid., 7.

III. *Outstanding Questions That Must be Addressed in the Final SIR*

- What is the manufacture and functionality of audio recording devices utilized by SPD? How much storage do they have, from what distance can they transmit, and from what distance can they pick up sound?
- How are new technologies selected when replacing devices that have reached end of life? Are there any limits on the kinds of new recording devices that can be acquired? Do new technologies include features not present in older technologies?
- What application is used to extract data from the recording devices and place the audio onto a hard drive or thumb drive? Can this software or any other alter recordings? If so, how is use of the software logged?
- Are there guidelines limiting the settings in which an audio device can be used or preventing the collection of unneeded and improper recordings?
- Are there any guidelines limiting how the audio devices can be used – for instance specifying at what point the recording may be turned on and when it must be turned off?
- What is the device request process? Who fills out the request form?
- What is the process for purging data? Who purges the data, and what oversight measures are in place to ensure data is properly and fully purged?
- What protocols ensure that consent is properly and clearly obtained before a recording is initiated?
- Where there is no warrant, how do officers decide which recordings or portions of recordings to delete and which to retain? Are there guidelines for making this determination?
- How is data shared with third parties? What security practices are observed? How is shared data monitored for deletion within the appropriate time frame?

IV. *Recommendations for Regulation*

Pending answers to the to the questions above, we can make only preliminary recommendations for regulation of audio/wire technology, particularly given that both the kind of technology and the scenarios where it is used are not described. SPD should adopt clearer and enforceable policies that include, at a minimum, the following:

- Narrowly tailored guidelines for where, how, and when recording devices may be used that help to limit the collection of unauthorized data. This might include a requirement that recording devices be turned on only once a person of interest is present, or a prohibition on using particularly powerful devices in public places where other private conversations might easily be picked up.
- Clear rules for the issuance of recording devices and processing of all recordings that limit the role of the investigating officer and ensure oversight by a supervisor. These rules should include a data-deletion protocol which makes clear who is responsible for deleting improperly collected data, ensures regular oversight of deletion, and provides clarity as to what data must be deleted where no warrant is used.

16

- Limits on the kinds of audio recording technology which SPD can use as end-of-life replacements for current audio devices, with consideration for the risks posed by newer and more powerful recording devices and applications.
- Limits on the software that can be used to process and extract audio recordings. For instance, this might include a prohibition on software that involves offsite cloud storage or voice biometrics recognition.
- Clear procedures for securely sharing data with third parties, including a policy that ensures shared data is erased.

Maltego

I. *Background*

Maltego is a powerful technology used by law enforcement to search, collect, and analyze billions of open-source data points and generate charts representing connections between identified entities and individuals. This technology poses serious privacy and civil liberties concerns as it enables dragnet surveillance through mass social media monitoring.

Maltego is advertised to law enforcement and cybersecurity analysts as a tool for acquiring identifying information on individuals and entities under investigation, including through analysis of email addresses and social media data, or data from the "dark web."[65] There are multiple versions of Maltego that include different functions and data packages.[66] SPD states that they use the free, community version to asses information which is already publicly available online, primarily in the course of cybercrime investigations.[67]

Maltego advertises having more than 35 data partners.[68] Their partners include Social Links,[69] a platform which allows for the harvesting of data from more than 50 social networks including Facebook, Instagram, and YouTube.[70] Even the free version of Maltego can be used to accesses these additional data integrations. For instance, Social Links has a free plug-in, Social Links CE, which can retrieve information from Skype and Social Links' own database,[71] which includes 7 billion

[65] "Law Enforcement," *Maltego.com*, Accessed June 15, 2021, https://www.maltego.com/law-enforcement/.
[66] "Pricing," *Maltego.com*, Accessed June 15, 2021, https://www.maltego.com/pricing-plans/; "Products," *Maltego.com*, Accessed June 15, 2021, https://www.maltego.com/products/.
[67] Seattle Police Department, 2021 Surveillance Impact Report: Link Analysis Software - Maltego," Accessed June 4, 2021, https://www.seattle.gov/Documents/Departments/Tech/Privacy/Public%20Engagement%20SIR_%20Link%20Analysis-Maltego.pdf, 5 and 11.
[68] "The Five Pillars of the Maltego Officer," *Maltego.com*, Accessed June 4, 2021, https://www.maltego.com/blog/the-five-pillars-of-the-maltego-offering/.
[69] "Transform Hub," *Maltego.com*, Accessed June 15, 2021, https://www.maltego.com/transform-hub/.
[70] "Social Links Pro," *Maltego.com*, Accessed June 15, 2021, https://www.maltego.com/transform-hub/social-links-pro; "Police Tight Lipped on Trial of Social Media Surveillance Tools," *NewsHub*, June 14, 2021, https://www.newshub.co.nz/home/new-zealand/2021/06/police-tight-lipped-on-trial-of-social-media-surveillance-tools.html.
[71] "Social Links CE," *Maltego.com*, Accessed June 15, 2021, https://www.maltego.com/transform-hub/social-links-ce/.

17

pieces of data.[72] Similarly, the free Wayback Machine integration allows users to browse "hundreds of billions of websites, going back for years or even decades…" including historical snapshots of pages and data long since deleted.[73] Although the SIR identifies some types of data that SPD does collect, such as web domain ownership information,[74] it does not fully explicate what kinds of data SPD uses within Maltego.

The validity of data collected via Maltego is questionable, given the multiple source points and huge quantities of data analyzed. Although the SIR indicates that all SPD data collected via Maltego is already publicly available,[75] that guarantee is misleading. Publicly available information can include private or sensitive data improperly made public via data breaches or hacking. Indeed, law enforcement agencies are known to purchase and use such "public" hacked data.[76] Notably, Maltego includes a free integration from "Have I Been Pwned," which may be used to search for such "public" hacked data.[77] Without proper analysis and verification, outputs generated from Maltego's open source data could further expose sensitive information.

Monitoring even accurate and properly collected public data raises serious civil liberties concerns when performed at the scale promised by Maltego. Vast pools of public data, when stored and analyzed in combination, can uncover privately held information. For instance, at a public demonstration in 2012, Maltego's founder demonstrated that his software could uncover the identity of a likely NSA employee using "public" information flowing out of the agency's parking lot. Maltego identified the employee's email address, date of birth, travel history, employment and education history, and image.[78] Such invasive surveillance fundamentally impedes individual privacy rights, particularly when entrusted to a government agency and used without clear limitations.

Maltego also may be used for mass monitoring of social media. Law enforcement social media monitoring is not new; by 2016, 70% of more than 500 surveyed departments used social media for intelligence gathering.[79] Tools like Maltego, however, allow for mass analysis and complex searches of social media data, a far more potent form of surveillance than targeted investigations of specific accounts. These tools can enhance agencies' existing social media agendas, including

---

[72] Jorn Weber, "Social Links: The All-Round Tools for OSINT Intern Investigations – Part 2," *Corma*, August 13, 2020, https://corma.de/en/4-social-links-the-all-round-tool-for-osint-internet-investigations-part-2/.
[73] "Wayback Machine," *Maltego.com*, Accessed June 15, 2021, https://www.maltego.com/transform-hub/wayback-machine/.
[74] SPD, "Maltego," 6.
[75] Ibid., 5.
[76] Joseph Cox, "Police are Buying Access to Hacked Website Data," *Vice.com*, July 8, 2020, https://www.vice.com/en/article/3azvey/police-buying-hacked-data-spycloud; The Department of Justice, "Criminal Charges Filed in Los Angeles and Alaska in Connection with Seizures of 15 Websites Offering DDoS-For-Hire Services," December 20, 2018, https://www.justice.gov/usao-cdca/pr/criminal-charges-filed-los-angeles-and-alaska-connection-seizures-15-websites-offering.
[77] "Have I Been Pwned," *Maltego.com*, Accessed June 15, 2021, https://www.maltego.com/transform-hub/haveibeenpwned/.
[78] Jeremy Kirk, "Who Is Tweeting from the NSA's Parking Lot," *Computer World*, October 17, 2012, https://www.computerworld.com/article/2492504/who-is-tweeting-from-the-nsa-s-parking-lot-.html.
[79] KiDeuk Kim, et. al., "2016 Law Enforcement Use of Social Media Survey," *The Urban Institute and International Association of Chiefs of Police*, February 2017, https://www.urban.org/sites/default/files/publication/88561/2016-law-enforcement-use-of-social-media-survey_5.pdf.

monitoring of demonstrations and activists,[80] with tracking often particularly focused on Black Lives Matter organizers.[81] Such tracking chills political speech and raises safety and privacy concerns, extending decades of police surveillance and abuse of civil rights protestors.[82] Social media analysis has also been used as a form of predictive policing – a mode of policing rife with bias and inaccuracies[83] – as police surveil accounts of interest and analyze posts to anticipate future crimes.[84]

Law enforcement already misuses and misconstrues social media data to compound existing biases and feed mass incarceration. The NYPD, for instance, has a social media tracking unit devoted to monitoring youth "gangs." Data is provided to probation and parole officers and can be presented in court with devastating consequences; in one case, misinterpreted social media "likes" were used to deny pre-trial bail to a misidentified, innocent Black teenager who spent two years awaiting trial on Rikers Island.[85] Maltego's mass analysis of public data grants police expanded surveillance capabilities and can subject individuals to unwarranted police interaction or criminal consequences on the basis of inaccurate, hacked, or misinterpreted information.

II. *Concerns*

a. **Inadequate Policies Defining Purpose of Use.** The SIR suggests that Maltego is primarily used for cybercrime investigations,[86] but does not specify any policies designating when the technology may be used. The SIR's language is also vague and implies that Maltego has been used in non-cyber contexts.[87] During the July 20th public engagement meeting, the SPD representative also commented that Maltego could be used for non-cyber crimes, although it generally is not. It is therefore unclear how widely large-scale public data analysis is currently used in SPD criminal investigations or what would prevent widespread usage of Maltego in the future.

b. **Inadequate Policies on Data Collection and Assessment.** The SIR states that Maltego can only be used within the bounds of a specific criminal investigation or "cybersecurity incidents."[88] However, it does not specify any internal guidelines restricting what public data or whose public data may be collected and analyzed using Maltego. Under existing policies, it seems entirely possible that people tenuously or erroneously associated with potential perpetrators – including people for whom there is little or no

[80] Rachel Levinson-Waldman, "Government Access to and Manipulation of Social Media: Legal and Police Challenges," *Howard Law Journal* (61.3, 2018), https://www.brennancenter.org/sites/default/files/publications/images/RLW_HowardLJ_Article.pdf, 529.
[81] "Police Monitoring of Social Media Sparks Concerns in Black and Brown Communities," *NPR – All Things Considered*, August 21, 2020, https://www.npr.org/2020/08/21/904646038/police-monitoring-of-social-media-sparks-concerns-in-black-and-brown-communities.
[82] Rachel Levinson-Waldman and Angel Diaz, "How to Reform Police Monitoring of Social Media," *Brookings Institute – Tech Stream*, July 9, 2020, https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media/; Levinson-Waldman, "Government Access," 524-525.
[83] Lau, "Predictive Policing Explained;" Friend, "Seattle's New Crime Analytics Program."
[84] Levinson-Waldman, "Government Access," 530.
[85] Ibid., 528.
[86] SPD, "Maltego," 5.
[87] Ibid., 8 and 10.
[88] Ibid., 8.

evidence of criminal activity – could be subject to Maltego assessment and surveillance.

c. **Lack of Clarity Around Data Sources.** The SIR does not describe the specific data sources SPD utilizes via Maltego; it provides only limited examples of Maltego's usage and states that data is collected from "various open source websites."[89] Absent further clarity, it seems possible that SPD can use Maltego for social media data analysis, raising privacy issues not addressed in the SIR. Additionally, the SIR acknowledges that "some iterations of Maltego allows for collection of private data of citizens,"[90] but does not outline procedures to prevent accidental private data collection, including of private information improperly made public through hacking.

d. **Potential for Predictive Usages.** Paterva advertises that Maltego can "[h]elp solve future investigations by pushing insights back into [a] case management system."[91] The SIR indicates that SPD exports Maltego charts back into SPD's system[92] and suggests that data from Maltego might be used for "defensive" purposes.[93] If Maltego is being used to anticipate future crimes, SPD must provide clarity as to a) how they guard against existing biases often replicated by predictive policing, and b) what surveillance they perform based on these predictions.

e. **Inadequate Policies to Assess for Errors in Data Analysis.** The SIR acknowledges that erroneous linkages are one of the "most important unintended possible consequence[s]" of Maltego. However, in describing safeguards to prevent erroneous linkages, the SIR only states, "because all analysis [is] conducted in the TESU by a limited number of detectives the risk is mitigated."[94] This mechanism seems ineffective, as no data output review process is described. Perhaps the SIR means that TESU detectives perform only limited and reviewable amounts of manual analysis and diagramming, which indeed might limit inaccuracies. However, no policies are described which would enforce limits on diagramming techniques and levels of usage. To the contrary, any such limits contradict the core purpose of Maltego. SPD states that Maltego is useful precisely because it can "pars[e] large amounts of… information,"[95] and thereby "help in identifying unknown relationship[s]."[96]

The SIR does not describe SPD tracking of Maltego's error rate. Without error tracking or safeguards, Maltego outputs likely lead police in inaccurate directions and subject random individuals to unnecessary surveillance and police interaction. Because evidence collected via Maltego can be used for search warrants, inaccurate Maltego outputs that are presented to the court as valid could lead to particularly invasive forms of improper searches.[97]

[89] Ibid., 6.
[90] SPD, "Maltego," 20.
[91] Law Enforcement," *Maltego.com.*
[92] SPD, "Maltego," 9.
[93] Ibid., 6.
[94] Ibid., 6 and 14.
[95] Ibid., 6.
[96] Ibid.
[97] Ibid.

f. **Lack of Clarity on Data Retention Policies.** The SIR states that data that is not relevant to an investigation is not retained and that "pertinent" data is exported to a spreadsheet or diagram and then handled per department policy.[98] However, it does not make clear how and when the originally collected, pertinent data is deleted from Maltego, leaving open the possibility that such data is retained indefinitely.

g. **Lack of Clarity Around Relationship with Paterva.** The SIR states that SPD searches are stored by the vendor, as SPD is unable to stand up their own server using the free version of the software.[99] These searches contain sensitive information that indicates the contents and direction of a criminal investigation and are being exposed to a private third-party. Additionally, the SIR states that Maltego is not "used to process or collect internal data,"[100] but elsewhere says that private information gathered via search warrant can be input into Maltego.[101] The SIR does not describe measures to keep that private data secure nor outlines Paterva's or Maltego Technolgies's internal data security measures. The SIR also does not describe a contract between SPD and Paterva or Maltego Technologies for the use of the free Maltego software.

h. **Potential for Improper Use Without Auditing/Logging.** The free version of Maltego's software seems to include no auditing or logging capabilities.[102] Lack of auditing or logging increases the probability that the software will be misused. Given the software's potential for invasive surveillance and monitoring that could intrude upon protected speech, more careful monitoring is essential. Notably, upgrading to the paid version of the software would not resolve the problem and would likely exacerbate the overall civil liberties concerns posed by the software; the paid version includes additional privacy risks given the far wider breadth of data available.

III. *Outstanding Questions that Must be Addressed in the Final SIR*

- When can Maltego be used for non-cyber investigations?
- Once an investigation is opened, are there any internal guidelines restricting what public data or whose public data may be collected and analyzed using Maltego?
- Which specific data sources does SPD analyze using Maltego? Are there any limits on the kinds of data that can be assessed?
- Are Maltego outputs ever used for any predictive or "defensive" policing?
- Are errors in the data Maltego pulls systematically tracked? Are there any safeguards against errors or processes for analyzing the data?
- How often has Maltego been used, and is there any data suggestive of its efficacy in resolving cybersecurity crimes?

[98] Ibid., 9.
[99] Ibid, 10.
[100] Ibid., 9.
[101] Ibid., 6.
[102] Ibid., 11.

- After data is exported, how and when is pertinent data deleted from within Maltego?
- Does SPD have any kind of written agreement or contract with Paterva/Maltego Technologies for the use of the free Maltego software? If so, what are the provisions?
- Does SPD enter private information collected via search warrant into Maltego? If so, what data security protocols are in place to protect that private information?
- Does Paterva/Maltego Technologies have access to and store data that is requested and collected by SPD, beyond requests/searches made?
- What are the vendor's policies for data security, how is data stored, and who owns the data collected and analyses generated?

IV. *Recommendations for Regulation*

Pending answers to the to the questions above, we can make only preliminary recommendations for regulation of Maltego. SPD should adopt clearer and enforceable policies that include, at a minimum, the following:

- Guidelines as to when Maltego may be used, such as a regulation that permits its use only for cybercrime investigations.
- Limits on who associated with an investigation may have their data collected using Maltego, such as a regulation requiring reasonable suspicion that an individual committed a crime before their public data can be amassed and assessed.
- Limits on the kinds of public data that may be assessed using Maltego, such as a prohibition on dragnet social media analysis.
- A regulation that prevents internal SPD data from being inputted into Maltego.
- A prohibition on use of Maltego for predictive policing.
- An analysis of the impacts of any Maltego outputs.
- A process to analyze the accuracy of data and analyses generated by Maltego.
- The deletion of originally collected, pertinent data from within Maltego after it is exported.
- A clear agreement with the vendor for the use of the free Maltego software that prohibits the vendor from storing or accessing SPD data.
- The creation of additional security measures to prevent improper access of Maltego by unauthorized officers, given the lack of auditing and logging capabilities.

Sincerely,

Jennifer Lee
Technology and Liberty Project Manager

Farris Peale
Policy and Advocacy Group Intern

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

June 8, 2021

Re: Surveillance Ordinance Group 4a Request for Clarification from CTAB Privacy & Cybersecurity

The Community Technology Advisory Board (CTAB) Privacy & Cybersecurity Committee appreciates the opportunity to provide comment on the Group 4a Surveillance Impact Reports (SIRs). Volunteers from this committee have reviewed the Surveillance Impact Reports for the Group 4a technologies as a group. Our comment with requests for clarification is attached.

Our expectations for the onboarding of new technologies and the use of current technologies extend those as communicated in our 12 March 2019 memo to the Seattle City Council regarding Group 2 technologies with additions:

- Implicit bias has a material and potentially destructive impact on individuals and communities. It is important to keep in mind the ways in which bias can be streamlined and exacerbated through the use of technology.
- Interdepartmental sharing of privacy best practices: When we share what we've learned with each other, the overall health of the privacy ecosystem goes up.
- Regular external security audits: Coordinated by ITD (Seattle IT), routine third-party security audits are invaluable for both hosted-service vendors and on-premises systems.
- Mergers and acquisitions: These large, sometimes billion-dollar ownership changes introduce uncertainty. Any time a vendor, especially one with a hosted service, changes ownership, a thorough review of any privacy policy or contractual changes should be reviewed.
- Remaining a Welcoming City: As part of the Welcoming Cities Resolution, no department should comply with a request for information from Immigration and Customs Enforcement (ICE) without a criminal warrant. In addition, the privacy of all citizens should be protected equally and without consideration of their immigration status.

Sincerely,

CTAB Privacy and Cybersecurity subcommittee members

Nicole Espy, Committee co-chair
Camille Malonzo, Committee co-chair
Eryk Waligora, Committee volunteer

Community Technology Advisory Board

Femi Adebayo, CTAB Member
Nicole Espy, CTAB Member
Dr. Tyrone Grandison, CTAB Member
David Kirichenko, CTAB Member
John Krull, CTAB Member
Brandon Lindsey, CTAB Member
Lassana Magassa, CTAB Member
Camille Malonzo, CTAB Vice-Chair
René Peters, CTAB Chair
Leah Shin, CTAB Member

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

Callyo (Police)

1. Data from this application is stored on Amazon Web Services[1]. Will any SPD generated date be stored by Callyo or AWS?
2. Do other Callyo users or Callyo engineers have access to data generated by SPD?
3. How is data generated by SDP protected from Callyo or AWS?
4. Callyo was recently acquired by Motorola Systems in August 2020. Are there any changes to the terms of use as a result of the acquisition? If any data is collected by the technology provider, has its use / handling changed since acquisition?
5. Callyo is an Amazon Web Services (AWS) partner, which is a cloud services provider. Will any future usage of AWS via Callyo or any changes as a result of the acquisition by Motorol be reviewed by City Council prior to onboarding?
6. The SIR states that "Callyo is utilized in two different ways by units within SPD: Technical and Electronic Support Unit (TESU) and the High Risk Victims Unit (HRVU). The High Risk Victims Unit uses Callyo to mask phone numbers but does not utilize the recording features of Callyo" and goes on to describe the use of the technology by TESU officers/detectives. What is the data that HRVU keep about the call, if any, and for how long? Is that metadata used for any other purposes? Is that shared with any other department either internal to SPD or externally?
7. The SIR states "TESU maintains logs of requests (including copies of request forms and warrants) and extractions that are available for audit. SPD's Audit, Policy and Research Section (APRS) can conduct an audit of any system at any time. The Office of Inspector General and the federal monitor can also access all data and audit for compliance at any time." How often do these audits occur?
8. Recordings are retained for a maximum of a year ("Per the Washington Secretary of State's Law Enforcement Records Retention Schedule, investigational conversation recordings are retained "for 1 year after transcribed verbatim and verified OR until disposition of pertinent case file, whichever is sooner, then Destroy" (LE06-01-04 Rev. 1). TESU maintains a log of requests (including copies of warrants), extractions, and deployments that are available to any auditor, including the Officer of Inspector General and federal monitor."). What is the retention schedule for logs on calls?

[1]https://aws.amazon.com/blogs/publicsector/harnessing-the-power-of-cloud-startups-deliver-innovative-services-to-public-safety-agencies-faster/

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

Audio Recording Systems (Police)

1. The SIR states that "All audio recording devices are managed and maintained by the Technical and Electronic Support Unit (TESU). When an Officer/Detective has obtained consent and/or a court order, having established probable cause, to utilize an audio recording device, s/he makes a verbal request to the TESU. TESU staff completes TESU's Request Form that requires a reason for the request, a case number associated with the investigation, and a copy of the consent form and/or court order. Each request is screened by the TESU Supervisor prior to deployment."
2. Is there are limit to the how long an officer/detective can use the device? What are the limits / safeguards in place for timely use? For example, is there ever a scenario where an Officer/Detective indefinitely records individuals in the scope of the court order and potentially other scenarios outside the scope of the warrant, but only the latter is ultimately transcribed for use as part of a criminal investigation. What safeguards are in place to ensure this does not happen?
3. The SIR states that "[a]udio recording devices capture sounds as they are happening in the moment. The devices do not check for accuracy, as they are simply capturing a live exchange of sounds. They are not interpreting or otherwise, analyzing any data they collect." What happens when the device records audio that is background / not part of a warrant to record but just happens to record other people? Is that data deleted? Is that transcribed?

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

I2 iBase (Police)

1. The SIR states "The most important unintended possible consequence related to the continued utilization of the iBase system is the possibility that erroneous links between individuals related to criminal investigations may be considered. However, because all analysis conducted in the RTCC is developed manually by analysts the risk is mitigated by the efficiencies provided by the use of the iBase system."
2. This is deeply concerning. The implicit bias in the network analysis done by analysts themselves can have negative impacts on individuals and communities when unchecked[2]. The SIR states that officers/detectives undergo security training and training on the use of the technology. Is there any training around implicit bias, especially with respect to network analysis?
3. The SIR states "i2 iBase is a relational database environment for searching through investigation data imported from RMS and CAD as well as manually imported information gathered by investigators during the course of a criminal investigation." Is the scope of any search query at all limited or does an Officer/Detective have access to all of the data in the SPD system regardless of scope? For example, if an Officer/Detective searches for a given name in the database will the search return all instances of an entity attached to a given name even if that would relate to different people of the same name, individuals who may not be involved in the specific criminal investigation for which the visualisation is being created?
4. The SIR states "[t]he software logs: user sign on/off, each time a user accesses any piece of data, and any data manually added by a user. These logs are periodically reviewed to ensure proper use of the software; they may also be reviewed at any time by the Seattle Intelligence Ordinance Auditor." Are any of these logs captured by the technology provider? What is the retention policy / other data handling procedures for this data?
5. Does data from Maltego (or other publicly available info) go into I2? Do analysts generate links between this external data with internal data?

[2] https://gspp.berkeley.edu/assets/uploads/research/pdf/SpencerCharbonneauGlaser.Compass.2016.pdf

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

Maltego (Police)

Governance

1. What does it mean that "Maltego is governed by SPD Policy"? What is this policy specifically?
2. What is the 'City of Seattle Intelligence Ordinance'? Is it this?: https://www.washingtonpost.com/archive/politics/1979/07/03/seattle-law-limits-police-in-intelligence-gathering/916c9159-31da-4a1f-ab55-9804ba5cfa19/
3. The governance structure also includes the 28 Code of Federal Regulations [CFR] Part 23 and Criminal Justice Information Services (CJIS) requirements, which are both very broad criminal justice/intelligence guidelines. Among other capabilities, Maltego is able to pull intelligence from the dark web in reconnaissance efforts. Is there any governance or training for ethical hacking?
4. The SIR states that "[a] paid version includes the ability to stand up an internal SPD server that would allow for logging, but that would involve significant costs to implement and maintain." The logging makes it easier for audits by the department and also the Office of Inspector General. Is this a requirement to ensure proper auditing? While access logs can be inspected on the workstations utilizes to use Maltego, these logs may not necessarily retain the search parameters and the actual use of the technology.

Use of the Technology

1. "Maltego…allows investigators to analyze connections between individuals related to criminal investigations." Is Maltego used only for "criminal investigations"? Maltego has many more capabilities beyond criminal investigations. This is not simply a tool used for or by law enforcement. Maltego can be used for all types of data collection, analysis, and tracking. Maltego's users vary. In fact, the company has a discounted program for academics and non-profits. However, this also means Maltego can be used by anyone, not just law enforcement, academics, and nonprofits, but by anyone attempting to collect and track key information on groups or individuals.
2. "The tool is used by law enforcement partners". Who are the "partners"? Is this service contracted out? If so, to whom? Are the "partners" from the public or private sector?
3. "Maltego is used infrequently to investigate cybercrime incidents." Why infrequently? What is the average frequency of use?
4. "This software simply visualizes data collected is from publicly available information on the internet." Data visualization is just one capability, but not its primary function. Software like Tableau is primarily used for importing and visualizing big data sets. Maltego is also heavily used to pull data from APIs, collate the data, and produce intelligence based on the collected and organized data. It also has capabilities, such as operating on the dark web.
5. "Data, when pertinent, is exported as a spreadsheet and/or visual diagram, at which point it is handled per department policy regarding digital evidence as part of a criminal investigation." How is this data considered evidence? Information that is not considered "evidence" could indicate that a certain person/entity is under criminal investigation; so how is that information protected?

City of Seattle

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

Protections

1. "SPD utilizes Maltego to investigate cybercrimes, primarily in determining the digital origin of attacks against cyber infrastructure." And "Maltego is restricted to use for the related security incident and/or pertinent criminal investigations and subject to Department Policy regarding ongoing criminal investigations."
2. "Primarily" in determining the digital origin of attacks? What else is it used for then?
3. "Restricted to use…" by whom or what policy specifically?
4. The use of this tool for the purposes of the SPD is difficult to justify. OSINT tools like Malego are used PRIMARILY for intelligence gathering in proactive defensive security, or as some even call it, "pre-crime". Intelligence is only useful before an attack, in order to help prevent it from occurring. But as this justification for use explains, the primary purpose of this tool will be used for investigations on crimes or incidents already committed.It is likely the SPD and all other PDs already have sophisticated tools designed specifically for this very purpose. Yes, Maltego can be used for all types of investigations, which can include criminal activities or even non-malicious vulnerability audits. But what is striking is that the primary function of this tool, as justified by SPD, will not be utilized. Main point: until there is clearer policy on the limitations of the SPD's use of Maltego, it will remain a powerful tool with multiple capabilities at the hands of law enforcement.
5. "Search warrant authorization is required, and would be obtained, to further any investigation into accessing private individual information." Maltego is only authorized for use with a warrant? This includes all cyber-crime and cyber attacks?
6. "Maltego is used by two trained TESU detectives within TESU, and by no other entity." "Users of Maltego undergo training on the use of the software, which includes privacy training." Law enforcement/criminal justice training is VERY different from intelligence analysis and/or data analysis training. What type of training and background do these detectives have? Is there any implicit bias training for the TESU officers/detectives who use the technology? (Stated policy on bias-based policy does not indicate specific training or mitigation of bias before it happens: 5.140 - Bias-Free Policing - Police Manual | seattle.gov)
7. "Data collected by Maltego is stored on an encrypted workstation within TESU." What type of encryption? This this stored on an on-premises server, hybrid, or cloud?

Use Case Example: "The City's network is attacked with ransomware"

1. The scenario described may not actually unfold as described. It is likely that upon a ransomware attack, the City would contract a cybersecurity consulting company it has a partnership with for incident response, which would include a team of highly trained engineers and security operation center (SOC) professionals to stop the attack and attempt to recover any lost or damaged data. It would also include attribution of the threat actor. How effective SPD's involvement would actually be in this case comparatively?