



# SEATTLE CITY COUNCIL

## Economic Development, Technology, and City Light Committee

### Agenda

Wednesday, April 27, 2022

9:30 AM

Remote Meeting. Call 253-215-8782; Meeting ID: 586 416 9164; or  
Seattle Channel online.

Sara Nelson, Chair  
Debora Juarez, Vice-Chair  
Lisa Herbold, Member  
Kshama Sawant, Member  
Dan Strauss, Member

Chair Info: 206-684-8809; [Sara.Nelson@seattle.gov](mailto:Sara.Nelson@seattle.gov)

[Watch Council Meetings Live](#) [View Past Council Meetings](#)

Council Chamber Listen Line: 206-684-8566

For accessibility information and for accommodation requests, please call  
206-684-8888 (TTY Relay 7-1-1), email [CouncilAgenda@Seattle.gov](mailto:CouncilAgenda@Seattle.gov), or visit  
<http://seattle.gov/cityclerk/accommodations>.



**SEATTLE CITY COUNCIL**  
**Economic Development, Technology, and City**  
**Light Committee**  
**Agenda**  
**April 27, 2022 - 9:30 AM**

**Meeting Location:**

Remote Meeting. Call 253-215-8782; Meeting ID: 586 416 9164; or Seattle Channel online.

**Committee Website:**

<https://www.seattle.gov/council/committees/economic-development-technology-and-city-light>

---

This meeting also constitutes a meeting of the City Council, provided that the meeting shall be conducted as a committee meeting under the Council Rules and Procedures, and Council action shall be limited to committee business.

*Pursuant to Washington State Governor's Proclamation No. 20-28.15 and Senate Concurrent Resolution 8402, this public meeting will be held remotely. Meeting participation is limited to access by the telephone number provided on the meeting agenda, and the meeting is accessible via telephone and Seattle Channel online.*

Register online to speak during the Public Comment period at the 9:30 a.m. Economic Development, Technology, and Seattle City Light Committee meeting at

<http://www.seattle.gov/council/committees/public-comment>.

Online registration to speak at the Economic Development, Technology, and Seattle City Light Committee meeting will begin two hours before the 9:30 a.m. meeting start time, and registration will end at the conclusion of the Public Comment period during the meeting. Speakers must be registered in order to be recognized by the Chair.

Submit written comments to Councilmember Sara Nelson at [Sara.Nelson@seattle.gov](mailto:Sara.Nelson@seattle.gov)

Sign-up to provide Public Comment at the meeting at

<http://www.seattle.gov/council/committees/public-comment>

Watch live streaming video of the meeting at

<http://www.seattle.gov/council/watch-council-live>

Listen to the meeting by calling the Council Chamber Listen Line at 253-215-8782 Meeting ID: 586 416 9164

One Tap Mobile No. US: +12532158782,,5864169164#

*Please Note: Times listed are estimated*

**A. Call To Order**

**B. Approval of the Agenda**

**C. Public Comment**

**D. Items of Business**

1. [CB 120307](#) **AN ORDINANCE relating to surveillance technology implementation; authorizing approval of uses and accepting the 2021 surveillance impact report and 2021 executive overview for the Seattle Police Department's use of Audio Recording Systems.**

Attachments: [Att 1 - 2021 SIR Audio Recording Systems](#)  
[Att 2 - 2021 SIR Audio Recording Systems Executive Overview](#)

Supporting Documents: [Summary and Fiscal Note](#)  
[Department Presentation - Group 4a SIRs](#)  
[Central Staff Presentation \(4/27/22\)](#)  
[Central Staff Memo \(4/27/22\)](#)  
[Background: Surveillance Impact Report Process and Related Legislation](#)

**Briefing & Discussion** (20 minutes)

**Presenters:** Jim Loter, Interim Director and Sarah Carrier, Seattle IT; James Britt, Brian Maxey, and Rebecca Boatright, Seattle Police Department (SPD); Lise Kaye, Council Central Staff

2. [CB 120308](#) **AN ORDINANCE** relating to surveillance technology implementation; authorizing approval of uses and accepting the 2021 surveillance impact report and 2021 executive overview for the Seattle Police Department's use of Maltego.

Attachments: [Att 1 - 2021 SIR Maltego](#)  
[Att 2 - 2021 SIR Maltego Executive Overview](#)

Supporting Documents: [Summary and Fiscal Note](#)  
[Central Staff Memo \(4/27/22\)](#)  
[Background: Surveillance Impact Report Process and Related Legislation](#)

**Briefing & Discussion** (20 minutes)

**Presenters:** Jim Loter, Interim Director and Sarah Carrier, Seattle IT; James Britt, Brian Maxey, and Rebecca Boatright, SPD; Lise Kaye, Council Central Staff

3. [CB 120309](#) **AN ORDINANCE** relating to surveillance technology implementation; authorizing approval of uses and accepting the 2021 surveillance impact report and 2021 executive overview for the Seattle Police Department's use of IBM i2 iBase.

Attachments: [Att 1 - 2021 Surveillance Impact Report: Link Analysis Software - IBM i2 iBase](#)  
[Att 2 - 2021 Surveillance Impact Report Executive Overview: IBM i2 iBase](#)

Supporting Documents:

[Summary and Fiscal Note](#)  
[Central Staff Memo \(4/27/22\)](#)  
[Background: Surveillance Impact Report Process and Related Legislation](#)

**Briefing & Discussion** (20 minutes)

**Presenters:** Jim Loter, Interim Director and Sarah Carrier, Seattle IT; James Britt, Brian Maxey, and Rebecca Boatright, SPD; Lise Kaye, Council Central Staff

## E. Adjournment



Legislation Text

---

**File #:** CB 120307, **Version:** 1

---

**CITY OF SEATTLE**

**ORDINANCE \_\_\_\_\_**

**COUNCIL BILL \_\_\_\_\_**

AN ORDINANCE relating to surveillance technology implementation; authorizing approval of uses and accepting the 2021 surveillance impact report and 2021 executive overview for the Seattle Police Department's use of Audio Recording Systems.

WHEREAS, Section 14.18.020 of the Seattle Municipal Code (SMC), enacted by Ordinance 125376 and last amended by Ordinance 125679, requires City Council approval of a surveillance impact report (SIR) related to uses of surveillance technology, with existing/retroactive technology to be placed on a Master Technology List; and

WHEREAS, SMC 14.18.020 applies to the Audio Recording Systems in use by the Seattle Police Department (SPD); and

WHEREAS, SPD conducted policy rule review and community review as part of the development of the SIR; and

WHEREAS, SMC 14.18.080, enacted by Ordinance 125679, also requires review of the SIR by the Community Surveillance Working Group, composed of relevant stakeholders, and a statement from the Chief Technology Officer in response to the Working Group's recommendations; and

WHEREAS, development of the SIR and review by the Working Group have been completed; NOW,

THEREFORE,

**BE IT ORDAINED BY THE CITY OF SEATTLE AS FOLLOWS:**

Section 1. Pursuant to Ordinances 125376 and 125679, the City Council approves use of the Seattle Police Department's Audio Recording Systems. The City Council accepts the December 17, 2021, Surveillance

Impact Report (SIR) for this technology, attached to this ordinance as Attachment 1, and the Executive Overview for the same technology, attached to this ordinance as Attachment 2.

Section 2. This ordinance shall take effect and be in force 30 days after its approval by the Mayor, but if not approved and returned by the Mayor within ten days after presentation, it shall take effect as provided by Seattle Municipal Code Section 1.04.020.

Passed by the City Council the \_\_\_\_\_ day of \_\_\_\_\_, 2022, and signed by me in open session in authentication of its passage this \_\_\_\_\_ day of \_\_\_\_\_, 2022.

\_\_\_\_\_  
President \_\_\_\_\_ of the City Council

Approved / returned unsigned / vetoed this \_\_\_\_\_ day of \_\_\_\_\_, 2022.

\_\_\_\_\_  
Bruce A. Harrell, Mayor

Filed by me this \_\_\_\_\_ day of \_\_\_\_\_, 2022.

\_\_\_\_\_  
Monica Martinez Simmons, City Clerk

(Seal)

Attachments:

Attachment 1 - 2021 Surveillance Impact Report: Audio Recording Systems (“Wires”)

Attachment 2 - 2021 Surveillance Impact Report Executive Overview: Audio Recording Systems (“Wires”)

**2021 Surveillance Impact Report**

# **Audio Recording Systems (“Wires”)**

**Seattle Police Department**



<b>Surveillance Impact Report (“SIR”) overview .....</b>	<b>3</b>
<b>Privacy Impact Assessment .....</b>	<b>4</b>
<b>Financial Information.....</b>	<b>16</b>
<b>Expertise and References.....</b>	<b>17</b>
<b>Racial Equity Toolkit (“RET”) and engagement for public comment worksheet .</b>	<b>19</b>
<b>Privacy and Civil Liberties Assessment .....</b>	<b>32</b>
<b>CTO Response .....</b>	<b>37</b>
<b>Appendix A: Glossary .....</b>	<b>45</b>
<b>Appendix B: Meeting Notice(s) .....</b>	<b>47</b>
<b>Appendix C: All Comments Received from Members of the Public.....</b>	<b>50</b>
<b>Appendix D: Letters from Organizations or Commissions.....</b>	<b>56</b>

## 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”.

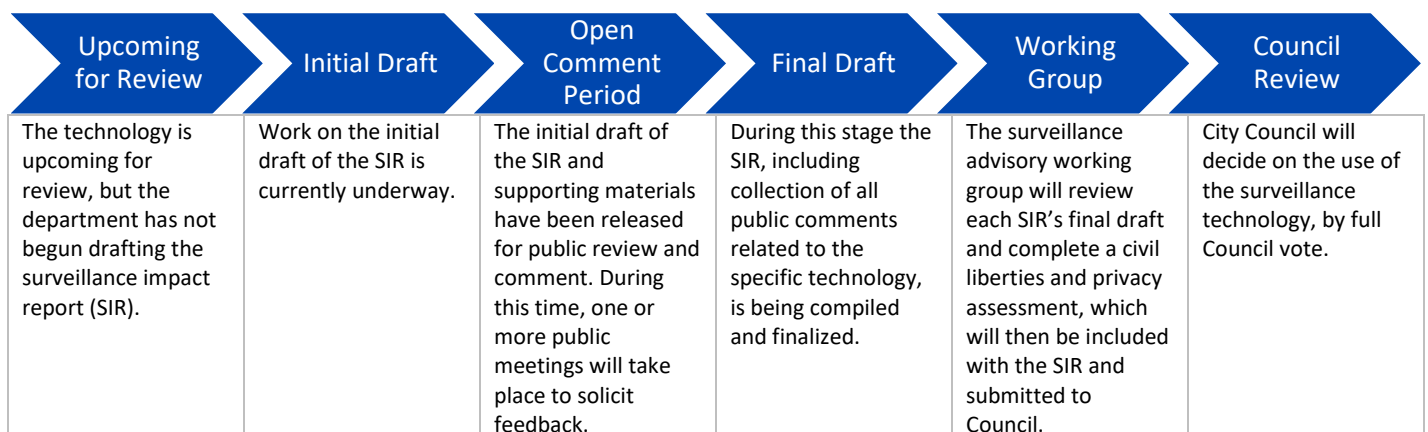
### How this Document is Completed

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.



# 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.

Seattle Police Department (SPD) utilizes audio recording systems in a handful of ways to obtain information during a criminal investigation. Pursuant to the Washington Privacy Act, [Chapt.9.73 RCW](#), these technologies are applied only after obtaining appropriate consent and/or legal search warrant authority. In such a circumstance, SPD employs audio recording devices on a person's body or situated and concealed in place within an environment to capture audio conversations between individuals, wherein at least one participant is unaware of the recording.

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

SPD's audio recording systems capture conversations of identifiable individuals, some of whom are unaware of the recording. Without appropriate safeguards, this raises significant privacy concerns. Recognizing these concerns, SPD only utilizes audio recording systems in a limited fashion with appropriate consent and/or court order.

## 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.

Audio recording systems allow SPD to pursue resolution of criminal investigations expeditiously by recording conversations of suspects, wherein an appropriate determination that sufficient probable cause exists has been made and a warrant has been issued. Per law, probable cause is required to obtain a search warrant. Without this technology, SPD would be unable to interrupt ongoing criminal activity and collect important evidence in some criminal investigations.

### 2.2 Provide any data or research demonstrating anticipated benefits.

The primary benefit of audio recording systems is in the gathering of evidence used in the resolution of criminal investigations. Audio recording technologies have been utilized by law enforcement in the United States since the 1920s. "The value of employing electronic surveillance in the investigation of some forms of serious crime, in particular organized crime, is unquestionable. It allows the gathering of information unattainable through other means."<sup>1</sup>

---

<sup>1</sup> [https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic\\_surveillance.pdf](https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf)

### **2.3 Describe the technology involved.**

Audio recording devices are typically known as “wires” and can be concealed on a person or hidden in or on objects within a particular environment. Audio recording devices must be turned on by an individual and they record only portions of a conversation that occur while the device is on. The recording is stored locally on the device and must be downloaded onto a storage device (i.e., thumb drive, external hard drive) before it can be accessed and transcribed.

These devices have the ability to capture audio, video, or both. The legal and investigatory circumstances under which video is captured are different than those under which audio is captured. Video recording systems are discussed in the SIR entitled “Camera 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. Audio recording systems contribute to crime reduction by assisting in collecting evidence related to serious and/or violent criminal activity as part of the investigation of criminal activity. These technologies are used only with proper consent and/or a warrant.

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

All audio recording systems utilized by SPD are managed and maintained with the Technical and Electronic Support Unit (TESU). TESU receives verbal requests for the deployment of this technology from SPD detectives investigating crimes and documents the equipment requested, the case number, and saves a copy of the consent form and/or court order authorizing the equipment’s use. TESU then deploys the equipment to the requesting Officer/Detective to engage within the scope of the consent form and/or court order.

When the requesting Officer/Detective has completed recording, TESU downloads the audio on a thumb drive or external hard drive, provides this copy to the Officer/Detective for inclusion in the investigation file, and then purges all data from the audio recording device. No data is retained on the device or within TESU.

If no data was collected by the device that assists in the pursuit of the criminal investigation or falls within the scope of the consent form and/or court order, the device is purged in its entirety and no data is provided to the Officer/Detective for the investigation file.

### 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.

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. TESU detectives then assign the audio recording device to the requesting Officer/Detective. Each deployment is logged, and all request forms (including consent form and/or court order) are maintained within TESU.

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

Audio recording devices are utilized only after legal standards of consent and/or court-issued warrant have been met, as required by the Washington Privacy Act, [Chapt. 9.73 RCW](#).

#### 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. Audio recording devices may only be issued/deployed by TESU detectives. All TESU staff that deploy audio recording devices have received vendor training in their use. Once 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. TESU staff then train requesting Officers/Detectives in their use when they deploy the equipment. The TESU Supervisor screens all deployments, and ensures that all staff receive adequate training, specific to the technologies.

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](#).

## 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.

Audio recording devices collect conversations and sounds of individuals related to a criminal investigation. The information is extracted onto a thumb drive from the device using locally stored computer application that resides on a computer in the TESU Unit. This application, accessible only to TESU staff, is used solely to extract audio data from a device and stores no data.

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

Deployment of audio recording devices is constrained to the conditions stipulated by consent and/or court order, which provides the legal authority and the scope of collection. All deployments of audio recording devices are documented by TESU and subject to audit by the Office of Inspector General and the federal monitor at any time.

As outlined in 2.5 above, if no data is collected by the device that assists in the pursuit of the criminal investigation or falls within the scope of the consent form and/or court order warrant (as determined by the judge), the device is purged in its entirety and no data is provided to the requesting Officer/Detective for the investigation file.

Data collected from audio recording devices is provided to the requesting Officer/Detective for the investigation and no data is retained by TESU.

### 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?

All of SPD's audio recording devices are managed and maintained by the Technical and Electronic Support Unit (TESU). Once 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.

TESU detectives then assign the audio recording device to the requesting Officer/Detective.

Each deployment is logged, and all request forms (including consent form and/or court order warrant) are maintained within TESU.

### 4.4 How often will the technology be in operation?

Consent and court ordered warrants determine the scope of each deployment. Audio recording devices are generally used to meet the needs of a criminal investigation, and the scope is specifically limited to the stipulations of consent and/or the court-ordered warrants providing authorization of use.

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

When audio recording devices are in use, they are installed temporarily within the scope of consent and/or warrant.

#### **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?**

When audio recording devices are being utilized, they are used in a covert capacity, which necessitates authorization via consent and/or court-ordered warrant. Audio recording devices are intended to be disguised and are, thus, not visible to the public. There are no visible markings indicating when it is in use. This means that there are no markings that identify department ownership. Each device has an assigned number, however, that can be used to audit the device's deployment and use.

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

Only authorized SPD users can access the audio recording devices or the data while it resides in the devices. Access to the systems/technology is limited to TESU personnel via password-protected login credentials.

Data removed from the system/technology and entered into investigative files is securely input 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.**

SPD's audio recording devices are not operated or used by other agencies.



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

On probable cause, the court can issue order authorizing interception, transmission, and recording of private communications or conversations when one party to the conversation or communication has consented. Detailed requirements spelled out in RCW 9.73.090(2), (4), and (5), and RCW 9.73.120, .130, and .140

Officers/Detectives must establish probable cause, as well as a showing of necessity, and obtain consent and/or court-ordered warrant to utilize audio recording devices. Once this has been obtained, they must complete TESU's Request Form that requires an acceptable reason for deployment, case number, and copy of consent form and/or warrant, which must then be approved by the TESU Supervisor, before an audio recording device is deployed.

After TESU has extracted data and provided it to the requesting Officer/Detective, the data is included in the investigation file and treated as evidence.

#### **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.)?**

Audio recording devices store audio data directly on the device. Access to the equipment and data stored on the device is accessible only to TESU staff. TESU staff extract the data, document the extraction, provide the data to the requesting Officer/Detective, and retain no copies of the data.

TESU maintains logs of requests (including copies of request forms and consent and/or warrants) and extractions that are available for audit. SPD's Audit, Policy and Research Section (APRS) can conduct an audit of the 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.

### **5.0 Data Storage, Retention and Deletion**

#### **5.1 How will data be securely stored?**

Until data is extracted from an audio recording device by TESU staff, the data is temporarily stored on the device. A TESU detective extracts the data onto a SPD disc and provides the disc to the requesting Officer/Detective for inclusion in the investigation file. The audio recording device is then purged and no data is retained by TESU.

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

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 consent forms and warrants), extractions, and deployments that are available to any auditor, including the Officer of Inspector General and federal monitor.

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

The scope of audio recording authorization is outlined in consent and court-ordered warrants. Any data that is collected outside the established scope is purged by the investigating detective.

All data collected within the scope of the appropriate authorization is provided to the requesting Officer/Detective and the device is purged. No data is retained by TESU.

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

All information 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?

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

SPD's Intelligence and Analysis Section reviews the audit logs and ensures compliance with all regulations and requirements.

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 audio recording devices. No person, outside of SPD, has direct access to audio recording devices or the data while it resides in the device.

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 with outside entities in connection with criminal prosecutions:

- Seattle City Attorney's Office
- King County Prosecuting Attorney's Office
- King County Department of Public Defense
- Private Defense Attorneys
- Seattle Municipal Court
- King County Superior Court
- Similar entities where prosecution is in Federal or other State jurisdictions

Data may be made available to requesters pursuant to the Washington Public Records Act, [Chapter 42.56 RCW](#) ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department ([RCW 10.97.030](#), [SPD Policy 12.050](#)). Individuals can access their own information by submitting a public disclosure request.

Per [SPD Policy 12.080](#), the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

Discrete pieces of data collected by audio recording devices 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 the devices.

## 6.2 Why is data sharing necessary?

Data sharing is necessary for SPD to fulfill its mission of contributing to crime reduction by assisting in collecting evidence related to serious and/or violent criminal activity as part of investigation, and to comply with legal requirements.

## 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](#), regulating criminal justice information systems. In addition, Washington State law enforcement agencies are subject to the provisions of [WAC 446-20-260 \(auditing and dissemination of criminal history record information systems\)](#), and [RCW Chapter 10.97 \(Washington State Criminal Records Privacy Act\)](#).

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](#).

Following Council approval of the SIR, SPD must seek Council approval for any material change to the purpose or manner in which the audio recording devices may be used.

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

Audio 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.

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

Individuals may request records pursuant to the PRA, and individuals have the right to inspect criminal history record information maintained by the department ([RCW 10.97.030](#), [SPD Policy 12.050](#)). Individuals can access their own information by submitting a public disclosure request.

## 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?

SPD's use of audio recording devices is governed at the state level by the [Washington Privacy Act](#). These devices are utilized only with consent and/or court-ordered warrant.

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

[SPD Policy 12.050](#) mandates that all employees, including TESU personnel, receive Security Awareness Training (Level 2), and all employees also receive City Privacy Training.

### 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 revolve around improper collection of sounds and conversations between members of the general public. As it relates to covert audio recording, SPD mitigates this risk by deploying them consistent to the stipulations outlined in the Washington Privacy Act, [Chapt. 9.73 RCW](#), and only by consent and/or with authorization of a court-ordered warrant.

[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 legal requirements and auditing processes (i.e., maintenance of all requests, copies of consent forms and warrants) that allow for any auditor, including the Office of Inspector General and the federal monitor, to inspect use and deployment of audio recording devices. The potential of privacy risk is mitigated by the requirement of consent and/or court ordered warrant before the technology is utilized.

## 8.0 Monitoring and Enforcement

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

TESU itself does not disclose information collected by audio recording devices. This information is provided to the requesting Officer/Detective to be included in the requisite investigation file. TESU then purges all data collected. TESU maintains a log of all requests, deployments, and access.

Per [SPD Policy 12.080](#), the Crime Records Unit is responsible to receive and record all requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

Any requests for public disclosure are logged by SPD's Public Disclosure Unit. Any action taken, and data released subsequently, is then tracked through the request log. Responses to Public Disclosure Requests, including responsive records provided to a requestor, are retained by SPD for two years after the request is completed.

### 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.

Requests to utilize audio recording devices, as well as logs of deployments, are kept within TESU and are subject to audit by the TESU Supervisor, Office of the Inspector General, and the federal monitor at any time.

Audit data is available to the public via Public Records Request.

## 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:

Initial acquisition costs are unavailable, as SPD has been using audio recording devices for decades.

#### 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
\$5000.00				SPD Budget

Notes:

Periodic equipment maintenance and end of life replacement

#### 1.3 Cost savings potential through use of the technology

Audio recording devices are used with consent and/or search warrant to resolve investigations. They provide invaluable evidence that could not be calculated in work hours.

#### 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
United Nations Office on Drugs and Crime	Karen Kramer, Senior Expert karen.kramer@unodc.org	Virtually all law enforcement agencies throughout the world rely on audio recording devices in the routine course of criminal investigations.

### 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
Current Practices in Electronic Surveillance	United Nations Office on Drugs and Crime	<a href="https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf">https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf</a>
Personal Electronics for Law Enforcement Solid State Recorders and Body Wires	Georgia Tech Research Institute	<a href="https://www.ncjrs.gov/pdffiles1/nij/grants/210488.pdf">https://www.ncjrs.gov/pdffiles1/nij/grants/210488.pdf</a>

# 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 personally identifiable information (PII) gathered during criminal investigations could be used to identify individuals who are associates of criminal suspects, such as their name, home address or contact information. Victims of criminal activity may also be identified during incident responses, whose identities should be protected in accordance with RCW 42.56.240 and RCW 70.02. SPD mitigates these risks by retaining as evidence only recordings within the framework established by the consent document and/or warrant obtained for each use of the technology.

**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 the risks for racial or ethnicity-based bias in the use of these audio recording systems, these devices are utilized only with consent and/or court-ordered warrant, having established probable cause.

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

all Seattle neighborhoods

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

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

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

### **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?**

Audio recording systems are used exclusively during the investigation of crimes and only with consent and/or court-ordered warrant, having established probable cause. There is no distinction in the levels of service SPD provides to the various and diverse neighborhoods, communities, or individuals within the city.

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

### **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.”<sup>1</sup> 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 obtained by the audio recording systems 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 / have you taken to ensure these consequences do not occur.**

The most important unintended possible consequence related to the continued utilization of the audio recording systems is the possibility that the civil rights of individuals may be compromised by unlawful surveillance. SPD mitigates this risk by requiring consent and/or a court-ordered warrant, having established probable cause, prior to the utilization of these technologies.

## 2.0 Public Outreach

### 2.1 Scheduled public meeting(s).

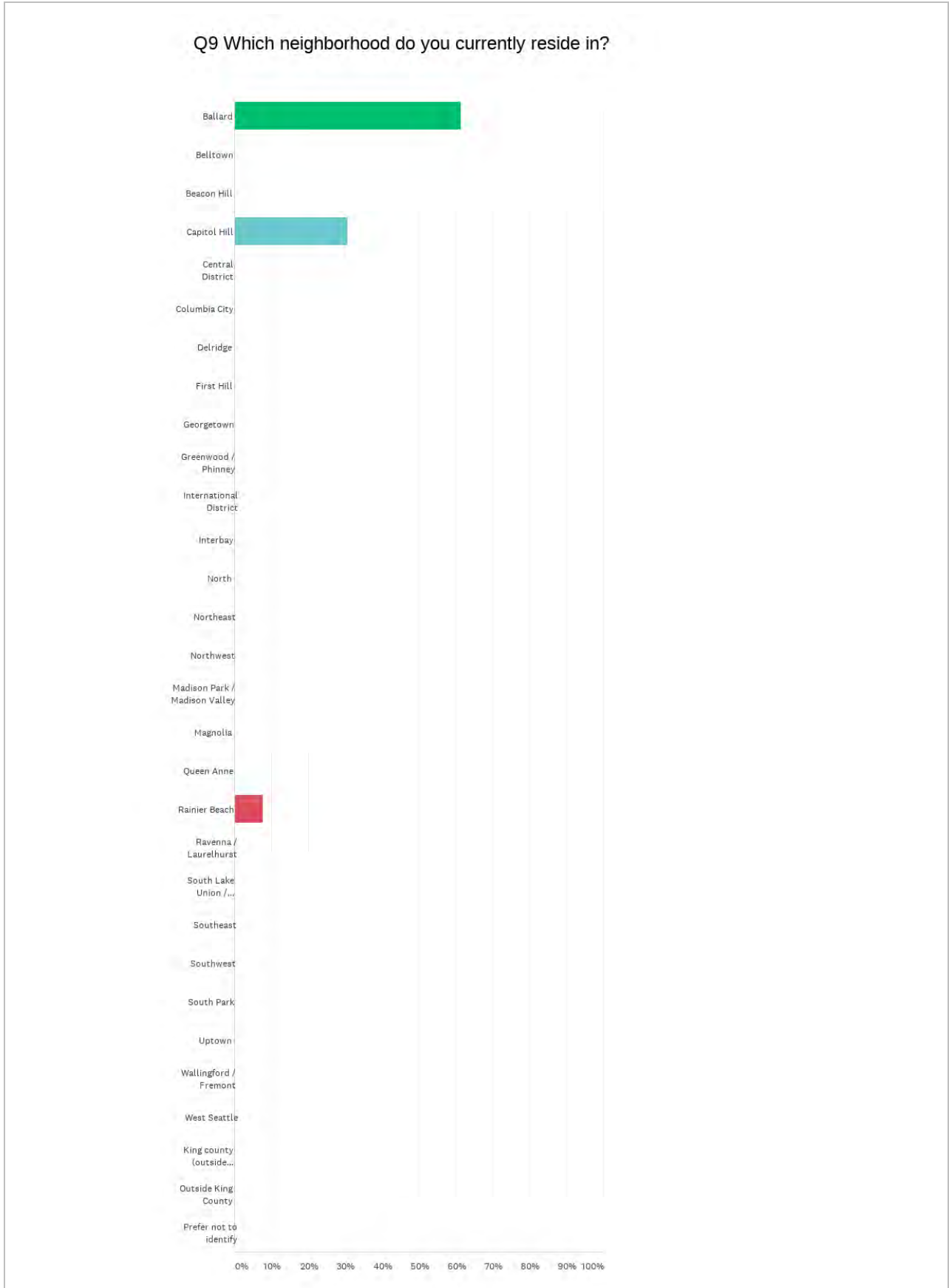
<b>Location</b>	Virtual Event
<b>Time</b>	Thursday, June 10 <sup>th</sup> , 12 PM

<b>Location</b>	Virtual Event
<b>Time</b>	Tuesday, June 29 <sup>th</sup> , 3 PM

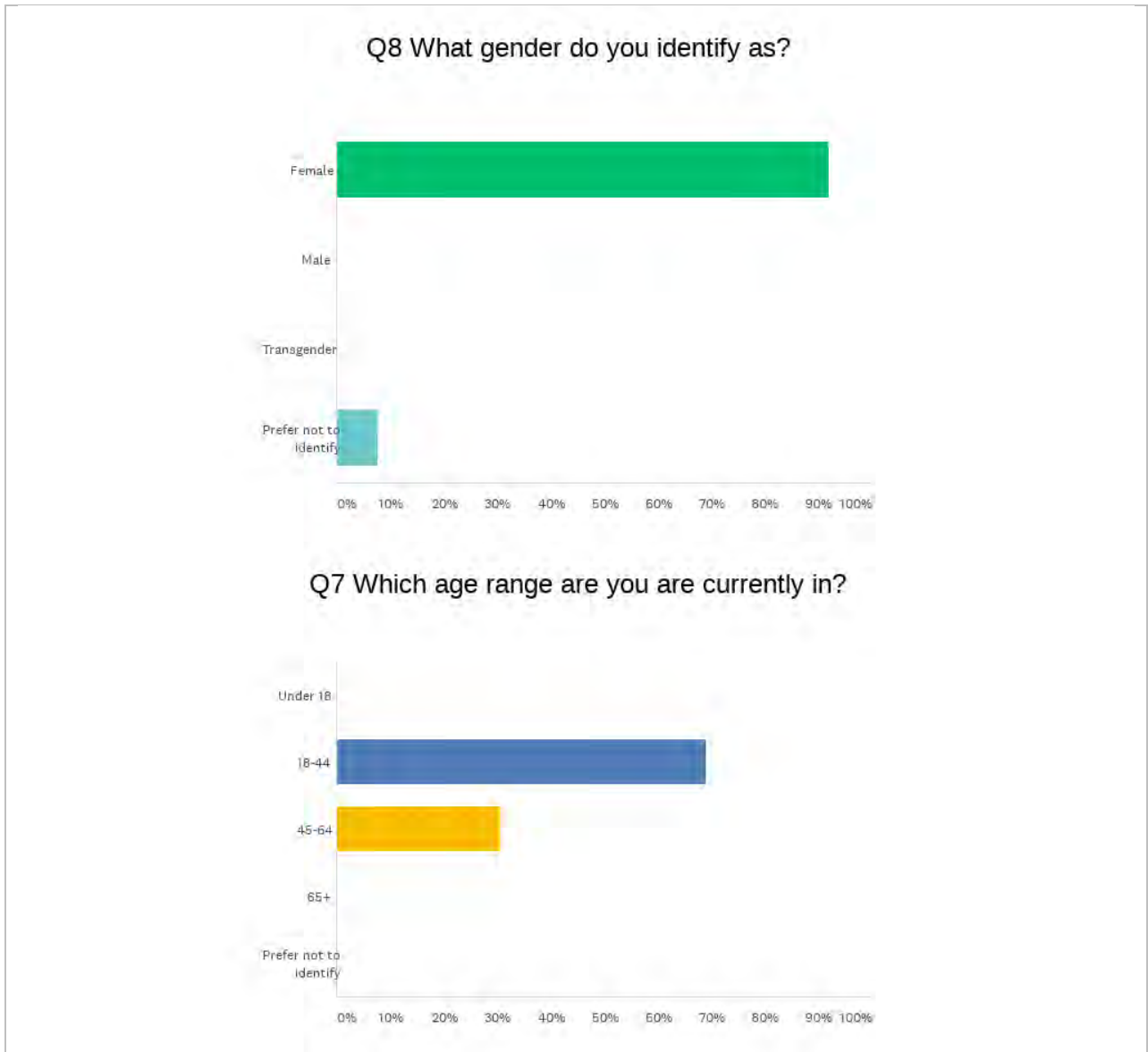
### **3.0 Public Comment Analysis**

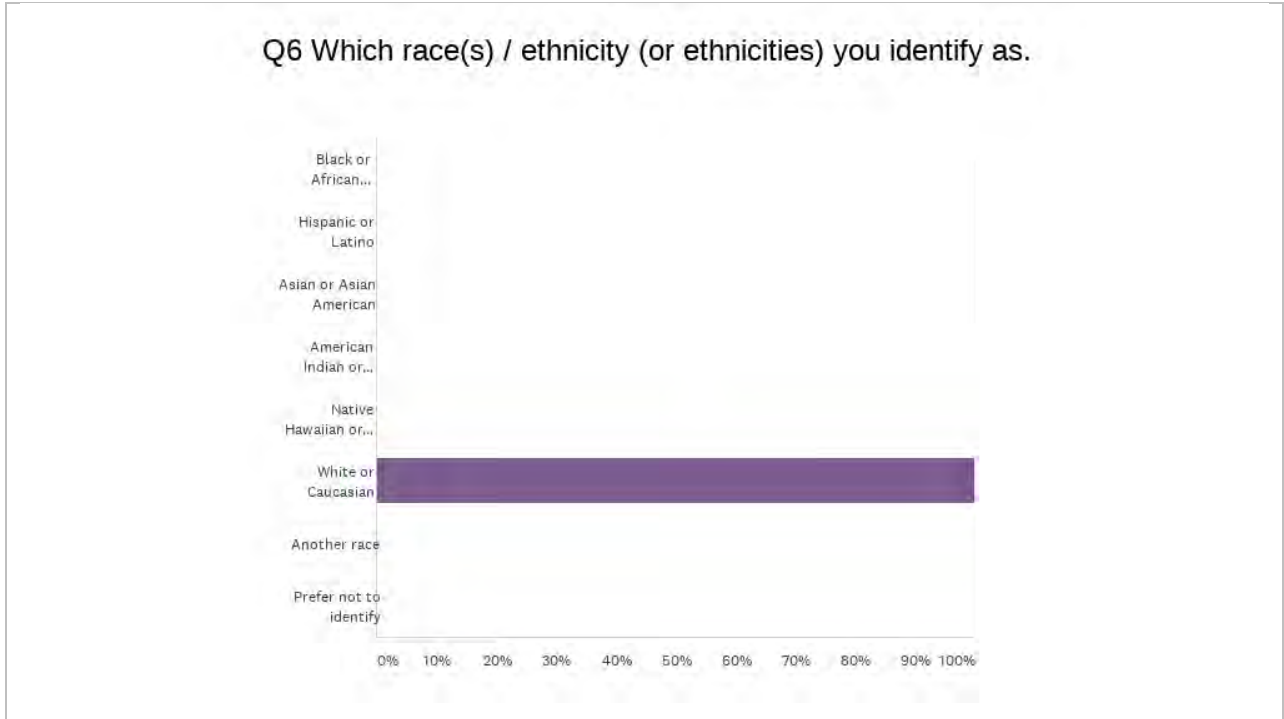
This section will be completed after the public comment period has been completed. Please note due to the volume of comments, analysis represents a summarization of all comments received. Technology specific comments will be included in Appendix C.

#### **3.1 Summary of Response Volume**









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

Q2 What concerns, if any, do you have about the use of this technology?

response question survey withholding information public comment open questions  
RMS Mark43 opposed informed public comment Missing information due  
hinder ability informed SPD using thus greatly hinder TESU public answered thus  
incorporates numerous questions public regarding answers questions numerous since  
dodged providing answers per year use Additionally SPD dodged  
many incidents per engagement meetings Additionally SPD specified many  
4a public engagement clarity regarding magnitude public Group 4a  
data retention period allocated questions public incident types SPD  
little time allocated CAD etc incident audio recordings defining limiting CAD  
Lack transparency Thus concerns include use Maltego concerns will Thus whether  
questions list concerns via answers open questions etc worst missing answers  
used privacy-wise assume worst **Callyo apps**  
approach security privacy-wise  
**audio recording devices** Since safest approach  
**data** survey Since safest **SPD** safest approach security **iBase**  
security privacy-wise assume **Maltego** assume worst missing  
**Lack clarity regarding** missing answers open  
**use Callyo apps** open questions list access list concerns will installed  
will Thus concerns apps policy defining limiting Maltego SIR limiting CAD etc  
regarding whether etc incident types use iBase types SPD may  
time allocated questions SPD RMS Mark43 questions public Group  
regarding magnitude use Group 4a public specified many incidents  
public engagement meetings incidents per year meetings Additionally SPD  
Surveillance always concern SPD dodged providing Security  
providing answers questions record questions numerous questions audio  
questions public answered deployment answered thus greatly write access  
greatly hinder ability One safely assume ability informed public SPD withholding information  
public comment open recording devices use SPD use Maltego question survey Since

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

Q3 What value, if any, do you see in the use of this technology?

Remains seen value **None**

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

Q4 What do you want City leadership to consider about the use of this technology?

past history prior Callyo apps Require City leadership past stop funding tool tool Given City security requiring SPD recommend City leadership etc Require SPD problems fixed SPD may used fixed systemic problems version criminal system fixed considerations depend SPD support pipelines criminal TBD valid considerations community needs support update Callyo SIR tools money community per year use surveil residents SPD many incidents per use Maltego SPD disclose many record specific incident types audio recording devices Policy state specific report recent audit questions Require SPD provide date report Require SPD answer SPD publicly provide changes made Require Require SPD Policy changes superficial changes access limited cosmetic changes Require SPD update will pursue limited SPD answer public right instead will

**Require SPD disclose** suspect fundamentally right

**use** surveillance technologies suspect **data**

prior surveillance technologies **iBase** technologies suspect fundamentally

**Maltego** fundamentally right instead

**answer public questions** instead will pursue **Callyo apps** pursue limited cosmetic devices cosmetic changes superficial Require SPD publicly superficial changes made publicly provide date made Require SPD date report recent public questions Require recent audit SPD SPD Policy state systems state specific incident Ban Improve security requiring SPD surveil residents disclose many incidents need tools money incidents per year money community needs SPD update Callyo needs support pipelines apps Require SPD pipelines criminal system valid considerations depend system fixed systemic depend SPD answering systemic problems fixed audited tools recommend City audio recordings City leadership stop etc Improve security Given City leadership leadership stop funding leadership past history funding tool Given history prior surveillance

### 3.5 General Surveillance Comments

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

Q5 Do you have any other comments or questions?

legal representative someone conducted audit report always disclosed legal  
answered policy defining SPD RMS Roughly iBase SIR 6.1 Mark43 instead SPD  
IBM s Security SPD use Maltego SPD licenses IBM SIR updated include  
accurately mapped person questions public answered  
individual voice accurately Callyo apps SPD  
recording specific individual many incidents per  
ensure voice recording SPD s brother girlfriend mother  
year SPD use concealed audio recording  
Roughly many incidents voice recognition identification  
types SPD may SPD use voice  
defining incident types someone facing charges  
audio recording devices  
representative someone facing iBase SPD s investigation  
policy defining incident use voice recognition  
incident types SPD recognition identification technology  
SPD may use younger brother girlfriend per year SPD  
SPD ensure voice used voice recording specific Will SIR updated  
specific individual voice incidents per year voice accurately mapped  
Many questions public SPD using information community version Maltego  
licenses IBM s also use Maltego s Security i2 RMS Mark43 instead  
public answered policy officer manually add Maltego Transform Hub  
RMS Roughly many audit report found disclosed legal representative

## 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 Audio Recording Systems

### 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 Audio Recording Systems 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 Audio Recording Systems.

Our assessment of Audio Recording Systems as used by Seattle Police Department (SPD) focuses on five major issues:

1. It is unclear what specific devices are used by SPD, as the SIR does not specify the manufacturer or function of devices used and it is unclear how devices are used and where they may be used.
2. It is unclear what specific data extraction software is used by SPD to extract audio data from devices.
3. It is unclear what consent procedures exist to ensure that SPD is only capturing and retaining audio that falls within the terms of an individual's consent.
4. There are inadequate policies regarding data collection, sharing, retention, deletion, storage, and protection.
5. There are inadequate policies for the issuance of recording devices and processing of recordings that limit the role of the investigating officer and ensure oversight.

### Recommendations

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

1. The purpose and allowable uses of Audio Recording Systems must be narrowly and clearly defined, and any SPD use of Audio Recording Systems must be limited to that specific purpose and those allowable uses. There must be a requirement for SPD to state for which specific incident types Audio Recording Systems may be used.
2. There must be a requirement for SPD to publicly disclose the names of the manufacturers, vendors, model names, and model numbers of the Audio Recording Systems in use.
3. There must be a requirement for SPD to make clear the warrant and/or consent procedures authorizing the use of a recording device.



4. There must be 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 that makes clear who is responsible for deleting improperly collected data, ensuring regular oversight of deletion, and providing clarity as to what data must be deleted when no warrant is used.
5. There must be clear procedures for securely sharing data with third parties, including a policy that ensures the erasure of shared data.
6. There must be a requirement for SPD to disclose how they ensure authenticity of recordings and individuals in audio recordings.
7. There must be a requirement for SPD to disclose for how many incidents per year they use Audio Recording Systems.
8. There must be a requirement for an independent audit of SPD’s audio recording devices and that audit must be made publicly available.
9. There must be a prohibition on use of biometric technology on or with audio recordings.

## Key Concerns

1. **It is unclear how audio recording 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.” 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’ flaws.
2. **There is lack of clarity around warrant and consent procedures.** The SIR indicates that either a warrant or consent may authorize use of a recording device. However, neither the SIR nor the June 10<sup>th</sup> or July 20<sup>th</sup> 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.
3. **There are inadequate 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.

4. **It is unclear what devices are used.** The SIR does not specify the manufacturer or function of devices used. 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.
5. **It is unclear what specific data extraction software is used.** 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.” 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.
6. **There are inconsistencies in deletion policies.** The SIR states that the TESU officer is responsible for purging improperly collected data, but also that the investigating officer is responsible for the purge. 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 4<sup>th</sup> amendment rights and Washington consent laws.
7. **There are security risks associated with third party data sharing.** The SIR describes third-party data sharing only vaguely. It does not describe the sharing process, or 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.
8. **There are inconsistencies in the 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 places states that the investigating officer completes the audio device request form but elsewhere states that TESU does so. 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.

## Outstanding Questions

- What is the manufacturer 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?

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.

## CTO Response

# MEMO

**To:** Seattle City Council  
**From:** Jim Loter, Interim Chief Technology Officer  
**Subject:** CTO Response to the Surveillance Working Group Audio Recording Systems 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 Audio Recording Systems.

### 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

The Seattle Police Department (SPD) utilizes audio recording systems in a handful of ways to obtain information during a criminal investigation. Pursuant to the Washington Privacy Act ([Chapt.9.73 RCW](#)) these technologies are applied only after obtaining appropriate consent and/or legal search warrant authority. In such a circumstance, SPD employs audio recording devices on a person’s body or situated and concealed in place within an environment to capture audio conversations between individuals, wherein at least one participant is unaware of the recording.

## **Working Group Concerns**

In their review, the Working Group has raised concerns about these devices being used in a privacy impacting way, including data collection, sharing, retention, deletion, storage, and protection.

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: Audio Recording Systems

**Concern: It is unclear what devices are used.**

CTO Assessment: The policies in place in the SIR and SPD manual operate regardless of the manufacturer or model of the devices. The conditions under which the devices are used are clearly outlined in the SIR and are further regulated by RCW 9.73.

SIR Response:

Section 2.3

“Audio recording devices are typically known as “wires” and can be concealed on a person or hidden in or on objects within a particular environment. Audio recording devices must be turned on by an individual and they record only portions of a conversation that occur while the device is on. The recording is stored locally on the device and must be downloaded onto a storage device (i.e., thumb drive, external hard drive) before it can be accessed and transcribed.”

**Concern: It is unclear what specific data extraction software is used.**

CTO Assessment: The policies in place in the SIR and SPD manual govern the use of data collected by audio recording devices and the circumstances under which they will be used, including in prosecutions. The conditions under which the devices are used are clearly outlined in the SIR and are further regulated by RCW 9.73. Once the audio has been collected, it is included in investigation files and treated as evidence subject to further guidelines.

**Concern: There is lack of clarity around warrant and consent procedures.**

CTO Assessment: These technologies are used surreptitiously and without consent. These technologies are operated under the authorization of a warrant from a court. Warrant and consent procedures are governed by state and federal law.

SIR Response:

Section 4.9

“On probable cause, the court can issue order authorizing interception, transmission, and recording of private communications or conversations when one party to the conversation or communication has consented. Detailed requirements spelled out in RCW 9.73.090(2), (4), and (5), and RCW 9.73.120, .130, and .140

Officers/Detectives must establish probable cause, as well as a showing of necessity, and obtain consent and/or court-ordered warrant to utilize audio recording devices. Once this has been obtained, they must complete TESU’s Request Form that requires an acceptable reason for deployment, case number, and copy of consent form and/or warrant, which must then be approved by the TESU Supervisor, before an audio recording device is deployed.

After TESU has extracted data and provided it to the requesting Officer/Detective, the data is included in the investigation file and treated as evidence.”

**Concern: Inadequate Policies on Data Collection, Sharing, Retention, Deletion, Storage, and Protection**

CTO Assessment: The SIR contains discrete sections relating to each of the concerns in addition to additional policies governing the use in the SPD manual and state law (RCW 9.73). As the data collected from these systems are primarily intended in use for criminal prosecution, there are other superseding policies and procedures that must be followed (circumstances around sharing or retention for example).

SIR Response:

## Section 4.2

"Deployment of audio recording devices is constrained to the conditions stipulated by consent and/or court order, which provides the legal authority and the scope of collection. All deployments of audio recording devices are documented by TESU and subject to audit by the Office of Inspector General and the federal monitor at any time.

As outlined in 2.5 above, if no data is collected by the device that assists in the pursuit of the criminal investigation or falls within the scope of the consent form and/or court order warrant (as determined by the judge), the device is purged in its entirety and no data is provided to the requesting Officer/Detective for the investigation file.

Data collected from audio recording devices is provided to the requesting Officer/Detective for the investigation and no data is retained by TESU."

## Section 4.7

"Only authorized SPD users can access the audio recording devices or the data while it resides in the devices. Access to the systems/technology is limited to TESU personnel via password-protected login credentials.

Data removed from the system/technology and entered into investigative files is securely input 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."

## Section 5.1

"Until data is extracted from an audio recording device by TESU staff, the data is temporarily stored on the device. A TESU detective extracts the data onto a SPD disc and provides the disc to the requesting Officer/Detective for inclusion in the investigation file. The audio recording device is then purged and no data is retained by TESU."



## Section 5.2

"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 consent forms and warrants), extractions, and deployments that are available to any auditor, including the Officer of Inspector General and federal monitor."

## Section 5.3

"The scope of audio recording authorization is outlined in consent and court-ordered warrants. Any data that is collected outside the established scope is purged by the investigating detective.

All data collected within the scope of the appropriate authorization is provided to the requesting Officer/Detective and the device is purged. No data is retained by TESU.

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

All information 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."

## Section 6.1

"SPD has no data sharing partners for audio recording devices. No person, outside of SPD, has direct access to audio recording devices or the data while it resides in the device.

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 with outside entities in connection with criminal prosecutions:

- Seattle City Attorney's Office
- King County Prosecuting Attorney's Office
- King County Department of Public Defense
- Private Defense Attorneys
- Seattle Municipal Court
- King County Superior Court
- Similar entities where prosecution is in Federal or other State jurisdictions

Data may be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

Discrete pieces of data collected by audio recording devices 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 the devices."

**Concern: Inadequate Policies relating to issuance of recording devices and processing of recordings**

CTO Assessment: The SIR outlines the conditions under which recording devices are used in investigations in addition to the standards that are required by a legal entity to authorize the use of audio recording devices. Data obtained from these devices are processed in accordance with SPD's evidence handling policies as well as state and federal law.

SIR Response:  
Section 3.1

“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.

TESU detectives then assign the audio recording device to the requesting Officer/Detective.

Each deployment is logged, and all request forms (including consent form and/or court order) are maintained within TESU.”

### Section 3.2

“Audio recording devices are utilized only after legal standards of consent and/or court-issued warrant have been met, as required by the Washington Privacy Act, Chapt. 9.73 RCW.”

## 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

Share

Share

Print

PDF

Embed

Search

Board

[<< Previous](#)

[Next >>](#)



## **Appendix C: All Comments Received from Members of the Public**

**ID:** 12841234860

**Submitted Through:** Online Comment

**Date:** 7/23/2021 3:58:44 PM

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

SPD: Audio Recording Devices

**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 Audio Recording Devices 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 SPD policy defining or limiting the (CAD/etc) incident types for which SPD may use Audio Recording Devices. (2) The potential use of voice recognition/identification technology on the audio recordings. (3) SPD is withholding information from the public about the names of the manufacturers/vendors and model names/numbers of the audio recording devices used by SPD. There are many audio recording devices on the market, each with different feature sets. SPD has not been transparent about the technology they use. One point of the Seattle Surveillance Ordinance (SMC 14.18) was to bring the surveillance technologies to light so that they could have a robust public assessment. This is not possible when SPD is choosing to keep the audio recording devices they use secret. This should not be permissible. SPD must disclose the audio recording devices they use. (4) Lack of clarity regarding the magnitude of the use of audio recording devices by SPD. SPD has not specified how many incidents per year they use audio recording devices for. (5) No safeguards in place to prevent or quickly remedy the retention of audio recordings (snippets or entirety) that contain non-targeted individual(s). Privacy is not maintained/ensured for individuals not in scope for the warrant (i.e. younger brother, girlfriend, mother, strangers, etc). Nothing ensures that data collected accidentally on innocent individuals is deleted in a timely manner. (6) SPD intentionally obscuring the circumstances under which they deploy the audio recording devices. The audio recording devices SIR mentions deploying the devices within the scope of the consent form and/or court order. However, an audio recording collected via a concealed audio device will ever be used with consent. The intended use requires the target to be unaware and therefore unconsenting. Therefore, it seems SPD referring to consent being given is incorrect and intentionally obscures the true circumstances under which these devices are used. (7) No SPD Policy that addresses both reducing the inadvertent capture and the post-capture deletion of audio of individuals not targeted in an investigation. (8) Possible issues with authenticity and authentication of target individuals in audio recordings. Specifically, it is unclear how SPD accurately maps a voice in a recording to a certain person. (9) No audit (by OIG/APRS/etc) of SPD's audio recording devices. If such an audit has been performed, then SPD has not disclosed the report to the public. (10) No audit (by OIG/APRS/etc) of the TESU. If such an audit has been performed, then SPD has not disclosed the report to the public.

**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?**

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 funding 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 audio recording devices may be used. (3) Ban the use of voice recognition/identification technology on audio recordings. (4) Require SPD to update the SIR to include the names of the manufacturers/vendors and model names/numbers of the audio recording devices used by SPD. Don't allow secret technologies. (5) Require SPD to disclose how many incidents per year they use audio recording devices for. (6) Ban SPD from retaining audio recordings of individuals who are not suspects nor found guilty of a crime (i.e. a suspect's younger brother, girlfriend, mother, neighbor, or a stranger like a shopkeeper, etc). (7) Require SPD to update the audio recording devices SIR to either remove or clarify if/how any of these devices would be used with consent (as opposed to only court approval). (8) Require SPD Policy be created to address both reducing the inadvertent capture and the post-capture deletion of audio of individuals not targeted in an investigation. (9) Require SPD to disclose how they ensure authenticity of recordings and authentication of target individuals in the audio recordings. Specifically, it is unclear how SPD accurately maps a voice in a recording to a certain person (and that the recording is not forged/fraudulent). (10) Require SPD to publicly provide the date and report from the most recent audit of SPD's use of audio recording devices. (11) Require SPD to publicly provide the date and report from the most recent audit of the SPD TESU.

### **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 these audio recording devices? (2) Does SPD use any voice recognition/identification technology on the audio recordings? (3) What are the names of the manufacturers/vendors and model names/numbers of the audio recording devices used by SPD? (4) Roughly how many incidents/investigations per year does SPD use these concealed audio recording devices for? (5) What happens to portions of the audio recordings that contain non-targeted individual(s)? How is the privacy maintained for individuals not in scope for the warrant (i.e. younger brother, girlfriend, mother, strangers, etc)? (6) The audio recording devices SIR mentions deploying the devices within the scope of the consent form and/or court order. Could you please describe an example when a concealed audio recording device will be used with consent? Wouldn't all use require the target(s) to be unaware and therefore unconsenting? (7) In regards to the audio recording devices, is there any SPD policy that addresses both reducing the inadvertent capture and the post-capture deletion of audio of individuals not targeted in an investigation? (8) How does SPD ensure that the voice in a recording is that of a specific individual? How is the voice accurately mapped to a person? (9) When was the last audit of the TESU conducted? Where is that audit report located?



**ID:** 12746763622

**Submitted Through:** Online Comment

**Date:** 6/15/2021 7:00:21 PM

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

SPD: Audio Recording Devices

**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 these audio recording devices? 2) Does SPD use any voice recognition/identification technology on the audio recordings? 3) What are the names of the manufacturers/vendors and model names/numbers of the audio recording devices used by SPD? 4) Roughly how many incidents/investigations per year does SPD use these concealed audio recording devices for? 5) What happens to portions of the audio recordings that contain non-targeted individual(s)? How is the privacy maintained for individuals not in scope for the warrant (i.e. younger brother, girlfriend, mother, strangers, etc)? 6) The audio recording devices SIR mentions deploying the devices within the scope of the consent form and/or court order. Could you please describe an example when a concealed audio recording device will be used with consent? Wouldn't all use require the target(s) to be unaware and therefore unconsenting? 7) In regards to the audio recording devices, is there any SPD policy that addresses both reducing the inadvertent capture and the post-capture deletion of audio of individuals not targeted in an investigation? 8) How does SPD ensure that the voice in a recording is that of a specific individual? How is the voice accurately mapped to a person? 9) When was the last audit of the TESU conducted? Where is that audit report located?

---

**ID:** 12698219042

**Submitted Through:** Online Comment

**Date:** 5/28/2021 2:21:42 PM

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

SPD: Audio Recording Devices

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

Privacy

**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?**

We don't need more surveillance

**Do you have any other comments or questions?**

We need to reduce police capabilities, not spy on our citizens.

---

## **Appendix D: Letters from Organizations or Commissions**

July 23, 2021

Seattle Information Technology  
700 5<sup>th</sup> 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.

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 contain inaccuracies and built-in race and gender biases.<sup>1</sup> Such audio could be later input into a voice recognition or biometrics database, which may further enable both corporate and government surveillance.<sup>2</sup>

<sup>1</sup> 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>.

<sup>2</sup> 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/interpol-s-new-automated-platform-will-recognize-criminals-by-their-voice>.



P.O. Box 2728  
Seattle, WA 98111-2728  
(206) 624-2184  
[aclu-wa.org](http://aclu-wa.org)

Michele Storms  
*Executive Director*



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,<sup>3</sup> the Surveillance Impact Report (SIR) states that Callyo is used to GPS locate individuals.<sup>4</sup> 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.<sup>5</sup> 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.<sup>6</sup> Elsewhere, the SIR states that Callyo's call recording functions may only be used with a search warrant.<sup>7</sup> However, the city's webpage states, "Callyo may be used with consent or search warrant."<sup>8</sup> Comments at the June 10<sup>th</sup> and July 20<sup>th</sup> 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

<sup>3</sup> "Speaker Identification" *GoVivian.com*, Accessed June 10, 2021, <https://www.govivian.com/products/speaker-identification/>; "Voice Authentication," *Aware Biometrics*, Accessed June 10, 2021, <https://www.noware.com/voice-authentication/>; "Forensic Voice Analysis," *Sestek.com*, Accessed June 10, 2021, <https://www.sestek.com/forensic-voice-analysis/>; "Voice Inspector for Forensic Experts," *Phonecta.com*, Accessed June 10, 2021, <https://www.phonecta.com/en/use-case/au-fic-forensics-software/>.

<sup>4</sup> 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=10FVHt2cyv8>.

<sup>5</sup> Seattle Police Department, "2021 Surveillance Impact Report: Callyo," Accessed June 7, 2021, <https://www.seattle.gov/Documents/Departments/Tech/Privacy/Public%20Engagement%20SIR%200-2%20Callyo.pdf>, 5-7.

<sup>6</sup> "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/>.

<sup>7</sup> SPD, "Callyo," 5.

<sup>8</sup> *Ibid.*, 7, 10, and 11.

<sup>9</sup> "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.<sup>9</sup> 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,<sup>10</sup> despite HRVU's larger share of the annual Callyo budget.<sup>11</sup> 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,"<sup>12</sup> 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.<sup>13</sup> 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.<sup>14</sup> When asked about possible Motorola collection of Callyo data during the July 20<sup>th</sup> 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

<sup>9</sup> SPD, "Callyo," 10, 11, 13, and 17.

<sup>10</sup> *Ibid.*, 7-11.

<sup>11</sup> *Ibid.*, 18.

<sup>12</sup> *Ibid.*, 14.

<sup>13</sup> "Investigative Solutions," *Callyo.com*, Accessed June 16, 2021,

<https://callyo.com/investigations/investigative-solutions>.

<sup>14</sup> "Callyo," *Amazon Web Services*,

<https://partners.amazonaws.com/partners/0010L0000pRHaCQA3W/Callyo>; "10-21 Video,"

*Callyo.com*, Accessed June 7, 2021, <https://callyo.com/public-safety/10-21-video>.

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.<sup>15</sup> 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.<sup>16</sup> 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.<sup>17</sup> 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.<sup>18</sup> 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 its surveillance capabilities more forceful.<sup>19</sup> Callyo also includes numerous additional surveillance features, such as video recording and live streaming<sup>20</sup> and “10-

<sup>15</sup> SPD, “Callyo,” 14-16.

<sup>16</sup> *Ibid.*, 7 and 10.

<sup>17</sup> See “Supervisors and commanding officers are responsible for ensuring compliance with policies,” at SPD, “Callyo,” 9.

<sup>18</sup> “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-1c5ERKAL5Mm9y271/>.

<sup>19</sup> 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/>.

<sup>20</sup> “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.<sup>21</sup> 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.<sup>22</sup> Flight-based video tools can be and have been<sup>23</sup> 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:

<sup>21</sup> "10-21 Flight," *Callyo.com*, Accessed June 7, 2021, <https://callyo.com/public-safety/10-21-flight>.

<sup>22</sup> Kade Crookford, "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/>.

<sup>23</sup> "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.<sup>24</sup> SPD uses i2 iBase in partnership with a second IBM application, i2 Analyst's Notebook,<sup>25</sup> 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."<sup>26</sup> 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.<sup>27</sup>

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

<sup>24</sup> "IBM Security i2 iBase: FAQs," *IBM.com*, Accessed June 10, 2021, <https://www.ibm.com/products/i2-ibase>.

<sup>25</sup> 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.

<sup>26</sup> "IBM Security i2 Analyst's Notebook," *IBM.com*, Accessed June 10, 2021, <https://www.ibm.com/products/i2-analysts-notebook>.

<sup>27</sup> "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.<sup>28</sup>

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.<sup>29</sup> The RTCC is a “centralized data and logistics hubs” that allows analysts to provide data to officers on the street.<sup>30</sup> Second, investigating officers use iBase to collect and organize timeline and relationship data for cases in progress.<sup>31</sup>

Although SPD describes using iBase only to assess RMS and CAD data, iBase can process larger data pools and operate as a data magnet. For instance, the Durham, NC Police Department has considered importing city utility data, recreational park logs, and daily jail visitor lists into iBase.<sup>32</sup> 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.”<sup>33</sup> 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.<sup>34</sup> The SIR does not describe any SPD policy that would prevent additional data from being added to iBase. During the July 20<sup>th</sup> 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.<sup>35</sup> 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

<sup>28</sup> “IBM Security i2 Analyst’s Notebook: Feature Spotlights,” IBM.com, Accessed June 10, 2021, <https://www.ibm.com/products/i2-analysts-notebook/details>.

<sup>29</sup> SPD, “IBM i2 iBase,” 5.

<sup>30</sup> 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/>.

<sup>31</sup> SPD, “i2 iBase,” 5-6.

<sup>32</sup> “Digital Dragnet: How Data Became a Cop’s Best Weapon,” *GCN*, November 29, 2011, <https://gcn.com/Articles/2011/12/05/Predictive-policing-tech-features.aspx?Page=2>.

<sup>33</sup> “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/>.

<sup>34</sup> “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/>.

<sup>35</sup> Timothy Crocker, “The Power of Social Network Analysis,” *Police Chief Magazine*, Accessed June 11, 2021, <https://www.policemagazine.com/power-social-network-analysis/>.

Indigenous<sup>36</sup> – 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).<sup>37</sup> SNA is a problematic mode of analysis, in part because it is often used for predictive policing via “heat-mapping.” iBase advertises such features.<sup>38</sup> 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.<sup>39</sup>

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<sup>40</sup> – 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

<sup>36</sup> 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://lps.cip.gov/content/guid/pdf/csp15.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/>;

<sup>37</sup> SPD “IBM i2 iBase,” 6.

<sup>38</sup> “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>.

<sup>39</sup> 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>.

<sup>40</sup> Andrew Papachristos and Michael Sierra-Arevalo, “Policing the Connected World,” *Department of Justice Community Oriented Policing Services*, 2018, <https://www.hsdj.org/?view&id=814315>; Reichart, et al. “Focused Deterrence: A Policing Strategy to Combat Gun Violence,” *ICJLA Research Hub*, Accessed July 23, 2021, <https://icja.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."<sup>41</sup> However, that claim conflicts with assertions that iBase's automated processing will "create[e] relevant intelligence from large amounts of data,"<sup>42</sup> and will create new "efficiencies" by avoiding manual data management.<sup>43</sup> 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"<sup>44</sup> 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.

---

<sup>41</sup> SPD, "IBM i2 iBase," 27.

<sup>42</sup> *Ibid.*, 7.

<sup>43</sup> *Ibid.*, 6, 21, and 27.

<sup>44</sup> *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.<sup>45</sup> 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<sup>46</sup> and suggests that officers would manually input only single “piece[s] of data.”<sup>47</sup> 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.

---

<sup>45</sup> Ibid., 7.

<sup>46</sup> Ibid.

<sup>47</sup> Ibid., 6.

- i. **Data Deletion.** The SIR states that manually entered data will be automatically deleted after five years.<sup>48</sup> 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."<sup>49</sup> 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"<sup>50</sup> 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?

---

<sup>48</sup> Ibid., 10.

<sup>49</sup> Ibid., 11.

<sup>50</sup> 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.<sup>51</sup> The SIR does not specify the particular audio recording technology

---

<sup>51</sup> 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-%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.<sup>52</sup> Although the SIR is unclear about the type or model of devices used, at the July 20<sup>th</sup> 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.<sup>53</sup> 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.<sup>54</sup> 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.<sup>55</sup> 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.

<sup>52</sup> *Ibid.*, 6.

<sup>53</sup> 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-ops-allentown-city-hall-investigation-wiretaps-20180201-story.html>.

<sup>54</sup> 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/interpol-new-automated-platform-will-recognize-criminals-by-their-voices>; “Speaker Identification” *GoVoice.com*, Accessed June 10, 2021, <https://www.govoice.com/products/speaker-identification/>; “Voice Authentication,” *Awave Biometrics*, Accessed June 10, 2021, <https://www.awave.com/voice-authentication/>; “Forensic Voice Analysis,” *Sivtek.com*, Accessed June 10, 2021, <https://www.sivtek.com/forensic-voice-analysis/>; “Voice Inspector for Forensic Experts,” *Phonocia.com*, Accessed June 10, 2021, <https://www.phonocia.com/en/use-case/au@-forensics-software/>.

<sup>55</sup> SPD, “Audio Recording Systems (“Wires”),” 12.

## 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.”<sup>56</sup> 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.<sup>57</sup> However, neither the SIR nor the June 10<sup>th</sup> or July 20<sup>th</sup> 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.

---

<sup>56</sup> Ibid., 4.

<sup>57</sup> Ibid.

- d. **Lack of Clarity on Types of Devices Used.** The SIR does not specify the manufacturer or function of devices used.<sup>58</sup> 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."<sup>59</sup> 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,<sup>60</sup> but also that the investigating officer is responsible for the purge.<sup>61</sup> 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 4<sup>th</sup> amendment rights and Washington consent laws.
- g. **Security Risks Associated with Third Party Data Sharing.** The SIR describes third-party data sharing only vaguely.<sup>62</sup> 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<sup>63</sup> but elsewhere states that TESU does so.<sup>64</sup> 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.

---

<sup>58</sup> Ibid., 5 and 16.

<sup>59</sup> Ibid., 8.

<sup>60</sup> Ibid., 6.

<sup>61</sup> Ibid., 11.

<sup>62</sup> Ibid., 12.

<sup>63</sup> Ibid., 10.

<sup>64</sup> 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.

- 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."<sup>65</sup> There are multiple versions of Maltego that include different functions and data packages.<sup>66</sup> SPD states that they use the free, community version to assess information which is already publicly available online, primarily in the course of cybercrime investigations.<sup>67</sup>

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

<sup>65</sup> "Law Enforcement," *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/law-enforcement/>.

<sup>66</sup> "Pricing," *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/pricing-plans/>.

<sup>67</sup> "Products," *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/products/>.

<sup>68</sup> 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.

<sup>69</sup> "The Five Pillars of the Maltego Officer," *Maltego.com*, Accessed June 4, 2021, <https://www.maltego.com/blog/the-five-pillars-of-the-maltego-officer/>.

<sup>70</sup> "Transform Hub," *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/transform-hub/>.

<sup>71</sup> "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>.

<sup>72</sup> "Social Links CE," *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/transform-hub/social-links-ce/>.



pieces of data.<sup>72</sup> 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.<sup>73</sup> Although the SIR identifies some types of data that SPD does collect, such as web domain ownership information,<sup>74</sup> 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,<sup>75</sup> 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.<sup>76</sup> Notably, Maltego includes a free integration from “Have I Been Pwned,” which may be used to search for such “public” hacked data.<sup>77</sup> 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.<sup>78</sup> 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.<sup>79</sup> 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

<sup>72</sup> John Weber, “Social Links: The All-Round Tools for OSINT Intern Investigations – Part 2,” *Corima*, August 13, 2020, <https://corima.de/en/4-social-links-the-all-round-tool-for-osint-internet-investigations-part-2/>.

<sup>73</sup> “Wayback Machine,” *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/transform-hub/wayback-machine/>.

<sup>74</sup> SPD, “Maltego,” 6.

<sup>75</sup> *Ibid.*, 5.

<sup>76</sup> Joseph Cox, “Police are Buying Access to Hacked Website Data,” *Vice.com*, July 8, 2020, <https://www.vice.com/en/article/3azrvy/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-services-15-websites-offering>.

<sup>77</sup> “Have I Been Pwned,” *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/transform-hub/has-been-pwned/>.

<sup>78</sup> 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>.

<sup>79</sup> 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/88661/2016-law-enforcement-use-of-social-media-survey\\_5.pdf](https://www.urban.org/sites/default/files/publication/88661/2016-law-enforcement-use-of-social-media-survey_5.pdf).

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

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.<sup>85</sup> 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,<sup>86</sup> 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.<sup>87</sup> During the July 20<sup>th</sup> 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.”<sup>88</sup> 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

---

<sup>80</sup> 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\\_Howard\\_L\\_Article.pdf](https://www.brennancenter.org/sites/default/files/publications/images/RLW_Howard_L_Article.pdf), 529.

<sup>81</sup> “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>.

<sup>82</sup> 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.

<sup>83</sup> Lau, “Predictive Policing Explained,” Friend, “Seattle’s New Crime Analytics Program.”

<sup>84</sup> Levinson-Waldman, “Government Access,” 530.

<sup>85</sup> *Ibid.*, 523.

<sup>86</sup> SPD, “Maltego,” 5.

<sup>87</sup> *Ibid.*, 8 and 10.

<sup>88</sup> *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."<sup>89</sup> 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,"<sup>90</sup> 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."<sup>91</sup> The SIR indicates that SPD exports Maltego charts back into SPD's system<sup>92</sup> and suggests that data from Maltego might be used for "defensive" purposes.<sup>93</sup> 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."<sup>94</sup> 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,"<sup>95</sup> and thereby "help in identifying unknown relationship[s]."<sup>96</sup>

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.<sup>97</sup>

---

<sup>89</sup> Ibid., 6.  
<sup>90</sup> SPD, "Maltego," 20.  
<sup>91</sup> Law Enforcement, "Maltego.com."  
<sup>92</sup> SPD, "Maltego," 9.  
<sup>93</sup> Ibid., 6.  
<sup>94</sup> Ibid., 6 and 14.  
<sup>95</sup> Ibid., 6.  
<sup>96</sup> Ibid.  
<sup>97</sup> 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.<sup>98</sup> 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.<sup>99</sup> 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,”<sup>100</sup> but elsewhere says that private information gathered via search warrant can be input into Maltego.<sup>101</sup> The SIR does not describe measures to keep that private data secure nor outlines Paterva’s or Maltego Technologies’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.<sup>102</sup> 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?

---

<sup>98</sup> Ibid., 9.

<sup>99</sup> Ibid., 10.

<sup>100</sup> Ibid., 9.

<sup>101</sup> Ibid., 6.

<sup>102</sup> 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



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



### **Callyo (Police)**

1. Data from this application is stored on Amazon Web Services<sup>1</sup>. Will any SPD generated data 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 SPD 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 Motorola 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 Office of Inspector General and federal monitor."). What is the retention schedule for logs on calls?

---

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



### **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?





## 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<sup>2</sup>. 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?

---

<sup>2</sup> <https://gspp.berkeley.edu/assets/uploads/research/pdf/SpencerCharbonneauGlaser.Compass.2016.pdf>



## **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?



### *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?

**2021 Surveillance Impact Report Executive Overview**

# **Audio Recording Systems (“Wires”)**

**Seattle Police Department**

## Overview

**The Operational Policy statements in this document represent the only allowable uses of the equipment and data collected by this technology.**

This Executive Overview documents information about the collection, use, sharing, security and access controls for data that is gathered through SPD’s Audio Recording Systems. All information provided here is contained in the body of the full Surveillance Impact Review (SIR) document but is provided in a condensed format for easier access and consideration.

### 1.0 Technology Description

Audio recording devices are typically known as “wires” and can be concealed on a person or hidden in or on objects within a particular environment. Audio recording devices must be turned on by an individual and they record only portions of a conversation that occur while the device is on. The recording is stored locally on the device and must be downloaded onto a storage device (i.e., thumb drive, external hard drive) before it can be accessed and transcribed.

These devices have the ability to capture audio, video, or both. The legal and investigatory circumstances under which video is captured are different than those under which audio is captured. Video recording systems are discussed in the SIR entitled “Camera Systems”.

### 2.0 Purpose

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.

Audio recording systems contribute to crime reduction by assisting in collecting evidence related to serious and/or violent criminal activity as part of the investigation of criminal activity. These technologies are used only with proper consent and/or a warrant.

Audio recording systems allow SPD to pursue resolution of criminal investigations expeditiously by recording conversations of suspects, wherein an appropriate determination that sufficient probable cause exists has been made and a warrant has been issued. Per law, probable cause is required to obtain a search warrant. Without this technology, SPD would be unable to interrupt ongoing criminal activity and collect important evidence in some criminal investigations.

### 3.0 Data Collection and Use

**Operational Policy: Audio recording devices are utilized only after legal standards of consent and/or court-issued warrant have been met, as required by the Washington Privacy Act, [Chapt. 9.73 RCW](#).**

Audio recording devices collect conversations and sounds of individuals related to a criminal investigation. The information is extracted onto a thumb drive from the device using locally stored computer application that resides on a computer in the TESU Unit. This application, accessible only to TESU staff, is used solely to extract audio data from a device and stores no data.

All of SPD’s audio recording devices are managed and maintained by the Technical and Electronic Support Unit (TESU). Once 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.

TESU detectives then assign the audio recording device to the requesting Officer/Detective.

Each deployment is logged, and all request forms (including consent form and/or court order warrant) are maintained within TESU.

## 4.0 Data Minimization & Retention

**Operational Policy: Audio recording devices are utilized only after legal standards of consent and/or court-issued warrant have been met, as required by the Washington Privacy Act, [Chapt. 9.73 RCW](#).**

Deployment of audio recording devices is constrained to the conditions stipulated by consent and/or court order, which provides the legal authority and the scope of collection. All deployments of audio recording devices are documented by TESU and subject to audit by the Office of Inspector General and the federal monitor at any time.

As outlined in 2.5 above, if no data is collected by the device that assists in the pursuit of the criminal investigation or falls within the scope of the consent form and/or court order warrant (as determined by the judge), the device is purged in its entirety and no data is provided to the requesting Officer/Detective for the investigation file.

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).

## 5.0 Access & Security

**Operational Policy: Regarding probable cause, detailed requirements spelled out in [RCW 9.73.090\(2\)](#), (4), and (5), and [RCW 9.73.120](#), .130, and .140.**

**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.

## Access

Only authorized SPD users can access the audio recording devices or the data while it resides in the devices. Access to the systems/technology is limited to TESU personnel via password-protected login credentials.

Data removed from the system/technology and entered into investigative files is securely input and used on SPD’s password-protected network with access limited to authorized detectives and identified supervisory personnel.

## Security

Audio recording devices store audio data directly on the device. Access to the equipment and data stored on the device is accessible only to TESU staff. TESU staff extract the data, document the extraction, provide the data to the requesting Officer/Detective, and retain no copies of the data.

## 6.0 Data Sharing and Accuracy

**Operational Policy:** 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](#).

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 may request records pursuant to the PRA, and individuals have the right to inspect criminal history record information maintained by the department ([RCW 10.97.030](#), [SPD Policy 12.050](#)).

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 with outside entities in connection with criminal prosecutions:

- Seattle City Attorney’s Office
- King County Prosecuting Attorney’s Office
- King County Department of Public Defense
- Private Defense Attorneys
- Seattle Municipal Court
- King County Superior Court
- Similar entities where prosecution is in Federal or other State jurisdictions

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 audio recording devices 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.

## 7.0 Equity Concerns

**Operational Policy: All use of the audio recording systems must also comply with [SPD Policy 12.050](#) – Criminal Justice Information Systems and may only be used for legitimate criminal investigative purposes.**

Audio recording systems are used exclusively during the investigation of crimes and only with consent and/or court-ordered warrant, having established probable cause. There is no distinction in the levels of service SPD provides to the various and diverse neighborhoods, communities, or individuals within the city.



## SUMMARY and FISCAL NOTE\*

<b>Department:</b>	<b>Dept. Contact/Phone:</b>	<b>CBO Contact/Phone:</b>
SPD / ITD	Rebecca Boatwright Vinh Tang/206-684-7640	Neal Capapas/206-684-5292

*\* Note that the Summary and Fiscal Note describes the version of the bill or resolution as introduced; final legislation including amendments may not be fully described.*

### **1. BILL SUMMARY**

**Legislation Title:** AN ORDINANCE relating to surveillance technology implementation; authorizing approval of uses and accepting the 2021 surveillance impact report and 2021 executive overview for the Seattle Police Department’s use of Audio Recording Systems.

**Summary and background of the Legislation:** Per SMC Chapter 14.18 (also known as the Surveillance Ordinance), authorizing the approval of the surveillance impact reports for Seattle Police Department’s continued use of Audio Recording Systems.

### **2. CAPITAL IMPROVEMENT PROGRAM**

**Does this legislation create, fund, or amend a CIP Project?**      \_\_\_ Yes X No

### **3. SUMMARY OF FINANCIAL IMPLICATIONS**

**Does this legislation amend the Adopted Budget?**      \_\_\_ Yes X No

**Does the legislation have other financial impacts to The City of Seattle that are not reflected in the above, including direct or indirect, short-term or long-term costs?**

This technology is currently in use by the Seattle Police Department and no additional costs, either direct or indirect, will be incurred based on the continued use of the technology. However, should it be determined, that SPD should cease use of the technology, there would be costs associated with decommissioning the technologies. Additionally, there may be potential financial penalty related to breach of contract with the technology vendors.

**Is there financial cost or other impacts of *not* implementing the legislation?**

Per the Surveillance Ordinance, the City department may continue use of the technology until legislation is implemented. As such, there are no financial costs or other impacts that would result from not implementing the legislation.

### **4. OTHER IMPLICATIONS**

**a. Does this legislation affect any departments besides the originating department?**

This legislation does not affect other departments. The technology under review is used exclusively by the Seattle Police Department.

**b. Is a public hearing required for this legislation?**

A public hearing is not required for this legislation.

**c. Is publication of notice with The Daily Journal of Commerce and/or The Seattle Times required for this legislation?**

No publication of notice is required for this legislation.

**d. Does this legislation affect a piece of property?**

This legislation does not affect a piece of property.

**e. Please describe any perceived implication for the principles of the Race and Social Justice Initiative. Does this legislation impact vulnerable or historically disadvantaged communities? What is the Language Access plan for any communications to the public?**

The Surveillance Ordinance in general is designed to address civil liberties and disparate community impacts of surveillance technologies. Each Surveillance Impact Review included in the attachments, as required by the Surveillance Ordinance, include a Racial Equity Toolkit review adapted for this purpose.

**f. Climate Change Implications**

**1. Emissions: Is this legislation likely to increase or decrease carbon emissions in a material way?**

No.

**2. Resiliency: Will the action(s) proposed by this legislation increase or decrease Seattle's resiliency (or ability to adapt) to climate change in a material way? If so, explain. If it is likely to decrease resiliency in a material way, describe what will or could be done to mitigate the effects.**

No.

**g. If this legislation includes a new initiative or a major programmatic expansion: What are the specific long-term and measurable goal(s) of the program? How will this legislation help achieve the program's desired goal(s)?**

There is no new initiative or programmatic expansion associated with this legislation. It approves the continuation of use for the specific technologies under review.

**List attachments/exhibits below:**

# Group 4A Surveillance Impact Reports (SIRs):

SPD Audio Recording Systems (CB 120307)

SPD Maltego (CB 120308)

SPD IBM i2 iBase (CB 120309)

Economic Development, Technology & City Light Committee

April 27, 2022

# SIR Overview Process

Jim Loter, Interim Chief Technology Officer

Sarah Carrier, Privacy Program Manager

# Surveillance Criteria

Definition: *Technology whose primary purpose is to observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice. Identifiable individuals also include individuals whose identity can be revealed by license plate data when combined with any other record.*

## Exclusions

- Consents to provide the data
- Opt-out notice
- Body-worn cameras
- Police vehicle cameras
- Cameras installed pursuant to state law...or to record traffic violations
- Security cameras
- City infrastructure protection cameras
- Technology that monitors only City employees

## Inclusions

- Disparately impacts disadvantaged groups
- PII shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service
- Collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection
- Raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice

# Surveillance Impact Report (SIR) Process

- Submitted for all retroactive and newly proposed technologies that meet the definition and have no exclusion criteria
- Created by the Departments with project management from IT

1

Privacy Impact Assessment

2

Financial Information

3

Racial Equity Toolkit

4

Public Engagement Comments and Analysis

5

Privacy and Civil Liberties Impact Assessment

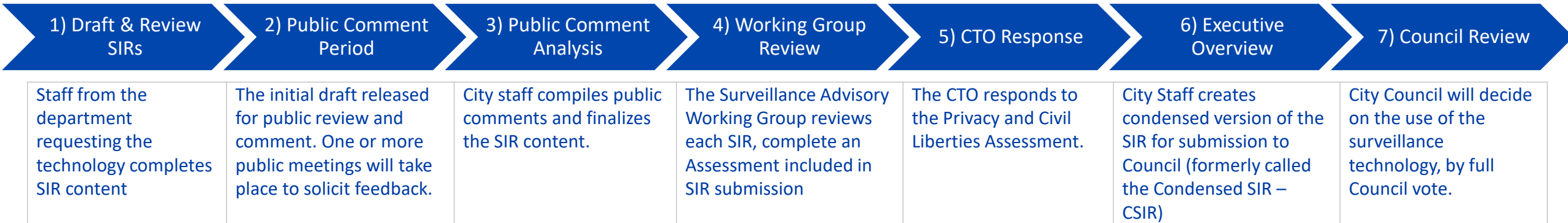
6




CTO Response

7

Appendices & Supporting Documentation

# General SIR Creation Timeline



Group	Depts.	28 Technologies (16 Completed)		Council Bill	Status
Group 1 (2)	SDOT	<ul style="list-style-type: none"> <li>License Plate Readers</li> <li>Closed Circuit Television Equipment "Traffic Cameras"</li> </ul>		CB 119519 CB 119519	Completed
Group 2 (9)	SCL  SFD SPD	<ul style="list-style-type: none"> <li>Binoculars/Spotting Scope</li> <li>Check Meter Device</li> <li>SensorLink Amp Fork</li> <li>Computer-Aided Dispatch</li> <li>911 Logging Recorder</li> <li>Automated License Plate Reader</li> <li>Parking Enforcement Systems including Automated License Plate Reader</li> <li>Computer-Aided Dispatch</li> <li>CopLogic</li> </ul>		CB 120002 CB 120002 CB 120002 CB 120003 CB 120024 CB 120025 CB 120026 CB 120027 CB 120028	Completed
Group 3 (3)	SPD	<ul style="list-style-type: none"> <li>Forward Looking Infrared Real-time video (FLIR)</li> <li>Situational Awareness Cameras Without Recording</li> <li>Video Recording Systems</li> </ul>		CB 120053 CB 120054 CB 120055	Completed
Group 4A (7)	SFD SDOT SPD	<ul style="list-style-type: none"> <li>Emergency Scene Cameras, Hazmat Camera</li> <li>*Acyclica</li> <li>Audio Recording Systems</li> <li>Maltego</li> <li>IBM i2 iBase</li> <li>*Callyo</li> </ul>		CB 120171 Memo CB 120307 CB 120308 CB 120309	Completed 9/15/21, 1/4/22 4/27 EDTCL 4/27 EDTCL 4/27 EDTCL
Group 4B (7)	SPD	<ul style="list-style-type: none"> <li>Camera systems; Tracking Devices; Remotely Operated Vehicles (ROVs); Hostage Negotiation Throw Phone; Crash Data Retrieval; GeoTime; Computer, cellphone and mobile device extraction tools</li> </ul>			Public Engagement Process



# Group 4A SIR Public Engagement

- Group 4a Surveillance Technologies Public Meetings on June 10th, 2021 & July 20th, 2021
- One Page Flyers
- Online Public Comment Meeting
  - Recorded and posted online

Engagement Method	(Approximate) Number of Individuals Participating	Number of Comments Received	Number of Questions Received
Public Meeting	13	-	8
Online Comments	13	13	-
Letters	2	2	-
<b>Total</b>	<b>28</b>	<b>15</b>	<b>8</b>

# Seattle Police Department Group 4A SIRs

SPD Audio Recording Systems

SPD Maltego

SPD IBM i2 iBase

Capt. James Britt, SPD

SEATTLE  
CITY HALL

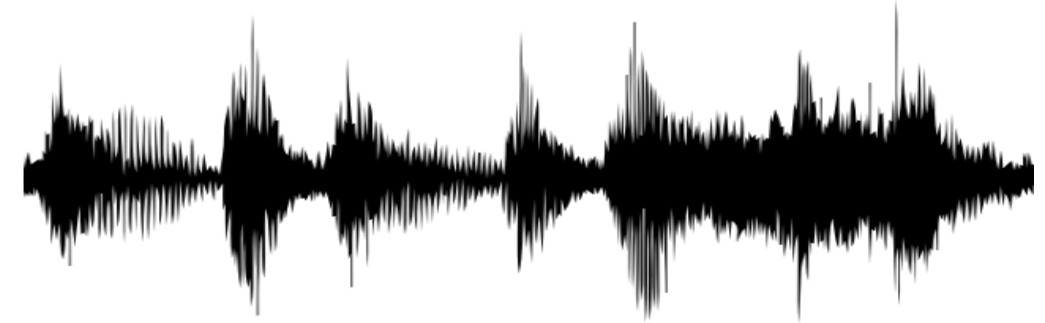
# Seattle Police Department Mission

- Prevent crime;
- Enforce the law; and
- Support quality public safety by delivering respectful, professional and dependable police services.

# Audio Recording Systems

## What is the technology?

- Audio recording devices are typically known as “wires” and can be concealed on a person or hidden in or on objects within a particular environment.
- Audio recording devices must be turned on by an individual and they record only portions of a conversation that occur while the device is on.



## Why do we use the technology?

- Audio recording systems contribute to crime reduction by assisting in collecting evidence related to serious and/or violent criminal activity as part of the investigation of criminal activity.
- Audio recording systems allow SPD to pursue resolution of criminal investigations expeditiously by recording conversations of suspects, once an appropriate determination that sufficient probable cause exists has been made and a warrant has been issued.

# Audio Recording Systems

## Data Collection

- All audio recording systems utilized by SPD are managed and maintained with the Technical and Electronic Support Unit (TESU).
- Data collected from audio recording devices is provided to the requesting Officer/Detective for inclusion in the investigation file and is stored following evidence guidelines.

## Protections

- Audio recording devices are utilized only after legal standards of consent and/or court-issued warrant have been met, as required by the Washington Privacy Act, Chapt. 9.73 RCW.
- Deployment of audio recording devices is constrained to the conditions stipulated by consent and/or court order, which provides the legal authority and the scope of collection.
- All deployments of audio recording devices are documented by TESU and subject to audit by the Office of Inspector General and the federal monitor at any time.

# Audio Recording Systems

## Related Policies

- Washington Privacy Act, Chapt.9.73 RCW
- SPD Policy 5.001 – Standards and Duties
- SPD Policy 5.002 – Responsibilities of Employees Concerning Alleged Policy Violations
- SPD Policy 5.140 – Bias-Free Policing
- SPD Policy 6.060 – Collection of Information for Law Enforcement Purposes
- SPD Policy 7.010 – Submitting Evidence
- 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
- SPD Policy 12.111 – Use of Cloud Storage Services

# Maltego

## What is the technology?

- 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 queries public data on the internet, such as domains, and displays it in a diagram showing links.



## Why do we use the technology?

- Maltego 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.
- A useful tool used in cyber-crime investigations, as these incidents often involve interactions between individuals, devices, and networks that are otherwise unknown.

# Maltego

## Data Collection

- Maltego queries publicly available data on the internet and collects information based on the parameters of the search request entered by a detective, much like Google returns results based on specific search terms.
- SPD utilizes Maltego to investigate cybercrimes, primarily in determining the digital origin of attacks against cyber infrastructure.

## Protections

- 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.
- Maltego is used by two trained TESU detectives within TESU, and by no other entity. Use of Maltego is governed by SPD Policy, the City of Seattle Intelligence Ordinance, 28 CFR Part 23, and CJIS requirements.



# Maltego

## Related Policies

- Washington Privacy Act, Chapt.9.73 RCW
- SPD Policy 5.001 – Standards and Duties
- SPD Policy 5.002 – Responsibilities of Employees Concerning Alleged Policy Violations
- SPD Policy 5.140 – Bias-Free Policing
- SPD Policy 6.060 – Collection of Information for Law Enforcement Purposes
- SPD Policy 7.010 – Submitting Evidence
- 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
- SPD Policy 12.111 – Use of Cloud Storage Services
- City of Seattle Intelligence Ordinance, 28 CFR Part 23

# IBM i2 iBase

## What is the technology?

- i2 iBase is a link analysis software used to combine data stored in SPD criminal information systems with information gathered during criminal investigations and display that information on a link chart.
- A virtual “pin board,” helping investigators to visualize the connections between known entities, vehicles, locations, etc. in the course of a criminal investigation.

## Why do we use the technology?

- IBM i2 iBase is used by analysts within the Real Time Crime Center (RTCC) to assist with criminal investigations and to provide actionable information to units in the field.
- Visualizing criminal information provides investigators a more thorough understanding of complicated criminal investigations.



# IBM i2 iBase

## Data Collection

- The iBase application imports specific data elements related to the investigation from SPD's Records Management System (RMS) and Computer Aided Dispatch (CAD) system.
- Users may also manually add additional information that they have collected during the course of a criminal investigation to assist in understanding complex investigations.

## Protections

- Only authorized users can access the system, technology, or the data. Access to the iBase system requires SPD personnel to log in with password-protected login credentials. All of these employees are ACCESS and Criminal Justice Information System (CJIS) certified.
- The I2 iBase system is CJIS compliant. The software also logs user sign on/off, each time a user accesses any piece of data, and any additions or changes a user makes.

# IBM i2 iBase

## Related Policies

- Washington Privacy Act, Chapt.9.73 RCW
- SPD Policy 5.001 – Standards and Duties
- SPD Policy 5.002 – Responsibilities of Employees Concerning Alleged Policy Violations
- SPD Policy 5.140 – Bias-Free Policing
- SPD Policy 6.060 – Collection of Information for Law Enforcement Purposes
- SPD Policy 7.010 – Submitting Evidence
- 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
- SPD Policy 12.111 – Use of Cloud Storage Services
- City of Seattle Intelligence Ordinance, 28 CFR Part 23

# Questions



SEATTLE CITY COUNCIL  
**CENTRAL STAFF**

# Group 4a Surveillance Impact Reports

---

LISE KAYE, COUNCIL CENTRAL STAFF

ECONOMIC DEVELOPMENT, TECHNOLOGY AND CITY LIGHT COMMITTEE | APRIL 27, 2022

# Proposed Council Bills

---

- CB 120307: Audio Recording Systems
- CB 120308: Maltego Link Analysis Software
- CB 120309: IBM i2 iBase Link Analysis Software

# Anticipated Process and Timeline

---

- April 19 – Introduction and Referral Calendar
- April 27 – First Committee Hearing
- May 11 – Second Committee Hearing/Possible Action



# Surveillance and Intelligence Ordinances

---

- **Surveillance Ordinances (2017 & 2018)**
  - Departments obtain advance Council approval of any new surveillance technology and request retroactive approval of existing surveillance technologies, consistent with an accepted Surveillance Impact Report
- **Intelligence Ordinances (1979 & 1982)**
  - Powers and functions of SPD's Criminal Information Section, including the collection, recording, retention and sharing of information

# Surveillance Impact Report Process

---



# CB 120307: Audio Recording Systems

---

- Used by SPD to covertly obtain information during a criminal investigation
- Devices not specifically identified in SIR due to safety concerns and to avoid risk of countermeasures
- Requires warrant and consent of person wearing the recorder

# Audio Recording Systems – Civil Liberties & Potential Disparate Impacts (per SIR)

- Risk of acquisition of private information about suspects and victims
- Data sharing, storage and retention could contribute to structural racism
- Mitigated through evidence procedures, anti-bias policies and warrant requirements

# Audio Recording Systems – Policy Considerations

---

1. Equity assessment metrics
2. Mitigation of civil liberties impacts
3. Authentication of recordings

# CB 120308: Maltego

---

- Used by SPD to investigate cybersecurity incidents and related criminal investigations
- Queries publicly available internet data and diagrams associations between individuals, devices and networks
- Operated by two authorized users in SPD's Technical and Electronic Support Unit

# Maltego – Civil Liberties & Potential Disparate Impacts (per SIR)

---

- Risk of erroneous links between individuals not related to criminal investigations
- Risk of acquisition of private data about individuals
- Potential algorithmic bias or ethnic bias
- Data sharing, storage and retention could contribute to structural racism
- Mitigated through limited number of detectives conducting analysis, cybercrime focus using publicly available information, anti-bias policies and warrant requirements

# Maltego – Policy Considerations

---

1. Equity assessment metrics
2. Response to public comments
3. Mitigation of civil liberties impacts
4. Contractual terms



# CB 120309: IBM's i2 iBase Link Analysis Software

---

- Visualization tool to identify relationships and reveal patterns in data related to ongoing investigations
- Combines data from SPD's Records Management and Computer Aided Dispatch systems, and information gathered during criminal investigations
- Also used to provide information to units in the field to increase officer safety, efficiency, and incident response

# i2 iBase – Civil Liberties & Potential Disparate Impacts (per SIR)

---

- Risk of erroneous links between individuals not related to criminal investigations
- Risk of acquisition of private data about individuals
- Potential algorithmic bias or ethnic bias
- Data sharing, storage and retention could contribute to structural racism
- Mitigated by the efficiencies provided by the system, evidence procedures, anti-bias policies and warrant requirements

## i2 iBase – Policy Considerations

---

1. Equity assessment metrics
2. Response to public comments
3. Mitigation of civil liberties impacts
4. Contractual terms
5. Retention schedule
6. Data sharing with Community Safety and Communications Center

# Questions?

---

April 19, 2022

## MEMORANDUM

**To:** Economic Development, Technology and City Light Committee  
**From:** Lise Kaye, Analyst  
**Subject:** Council Bill 120307 – Approves the use of and accepts the surveillance impact report for the Seattle Police Department’s use of Audio Recording Systems

---

On Wednesday, April 27, 2022, the Economic Development, Technology and City Light Committee will discuss [Council Bill 120307](#). This Council Bill would approve the Seattle Police Department’s (SPD’s) continued use of Audio Recording Systems and accept the Surveillance Impact Report (SIR) and an Executive Overview for this technology. The bill is intended to meet the requirements of [Seattle Municipal Code Chapter 14.18](#), Acquisition and Use of Surveillance Technologies, which requires City departments to obtain advance Council approval of the acquisition of surveillance technology and of a surveillance impact report (SIR).<sup>1</sup> Departments must also submit a SIR for surveillance technology in use when [Ordinance 125376](#) was adopted in 2017 (referred to in the ordinance as “retroactive technologies”), but failure to approve an ordinance for a retroactive technology does not require SPD to discontinue its use. Councilmembers may choose to amend the ordinance to request additional information or to request that SPD develop new and/or revised operational policies, which could restrict or modify the use of certain technologies.

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

### Audio Recording Systems

SPD uses Audio Recording Systems to covertly obtain information during a criminal investigation. SPD’s policies allow such use only after obtaining appropriate consent and/or legal search warrant authority, although SPD reports that they only use Audio Recording Systems with a search warrant. SPD conceals a device to capture conversations between individuals in which at least one participant is unaware of the recording. The SIR does not disclose the specific Audio Recording Systems used by SPD to avoid the risk of countermeasures and due to safety concerns for officers and cooperating witnesses. SPD reports that the department mitigates potential civil liberties risks and the risks of racial or ethnicity-based bias from the use of these systems and associated data sharing, storage and retention through its evidence procedures, anti-bias policies and warrant parameters. The Racial Equity Toolkit does not identify metrics to be used as part of the CTO’s required annual equity assessments.

---

<sup>1</sup> The Executive Overview summarizes SPD’s allowable uses of Audio Recording Systems. See also the [memo](#) summarizing process for developing a Surveillance Impact Report (SIR), consistent with [Ordinances 125376](#) and [125679](#) and [Ordinance 108333](#), Seattle’s “Intelligence Ordinance,” adopted in 1979 and amended in 1982 via adoption of [Ordinance 100572](#).

Surveillance Working Group Recommendations and CTO Response

The Community Surveillance Working Group’s Impact Assessment for SPD’s Audio Recording Systems makes nine recommendations to Council. The CTO’s response to the Impact Assessment finds that the “policy, training and technology limitations enacted by SPD provide adequate mitigation for the potential privacy and civil liberties concerns raised by the Working Group.” The CTO’s response does not specifically address the Working Group’s recommendations, but it identifies relevant citations from the SIR for each of the Working Group’s “key concerns.” **Table 1** describes whether the SIR as drafted and/or current law addresses the Working Group’s recommendations, as well as relevant responses from the CTO and/or SPD.

*Table 1. Working Group Recommendations*

<b>Working Group Recommendation</b>	<b>Whether/How Addressed by SIR, CTO or SPD and/or Current Law</b>
<p>1. The purpose and allowable uses of Audio Recording Systems must be narrowly and clearly defined, and any SPD use of Audio Recording Systems must be limited to that specific purpose and those allowable uses. There must be a requirement for SPD to state for which specific incident types of Audio Recording Systems may be used.</p>	<p><b>Executive Overview.</b> Operational Policies represent the only allowable uses of the equipment and data collected by this technology.</p> <p><i>SMC 14.12 (the “Intelligence Ordinance) governs the collection of data for a criminal investigation.</i></p>
<p>2. There must be a requirement for SPD to publicly disclose the names of the manufacturers, vendors, model names, and model numbers of the Audio Recording Systems in use.</p>	<p><i>SPD has requested not to publicly disclose this information to avoid the risk of countermeasures and due to safety concerns for officers and cooperating witnesses. OIG has confirmed that they can conduct their annual usage review without this information having been publicly disclosed.</i></p>
<p>3. There must be a requirement for SPD to make clear the warrant and/or consent procedures authorizing the use of a recording device</p>	<p><b>SIR §2.1</b> Audio recording systems allow SPD to pursue resolution of criminal investigations expeditiously by recording conversations of suspects, wherein an appropriate determination that sufficient probable cause exists has been made and a warrant has been issued.</p> <p><b>SIR §3.0</b> Once 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 [Technical and Electronic Support Unit]. 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.</p> <p><b>SIR §4.9</b> On probable cause, the court can issue order authorizing interception, transmission, and recording of private communications or conversations when one party to the conversation or communication has consented.</p>

Working Group Recommendation	Whether/How Addressed by SIR, CTO or SPD and/or Current Law
<p>4. There must be 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 that makes clear who is responsible for deleting improperly collected data, ensuring regular oversight of deletion, and providing clarity as to what data must be deleted when no warrant is used.</p>	<p><b>SIR §3.0</b> See description above re: issuance of recording devices.</p> <p><b>SIR §2.5</b> The Technical and Electronic Support Unit (TESU) downloads data related to the investigation or within the scope of the consent form and/or court order to a thumb drive or external hard drive and gives it to the Officer/Detective for inclusion in the investigation file and then purges all data from the recording device.</p> <p><i>According to SPD, case detectives are responsible for reviewing audio recordings as part of their investigation.</i></p>
<p>5. There must be clear procedures for securely sharing data with third parties, including a policy that ensures the erasure of shared data.</p>	<p><b>SIR §6.1</b> In addition to SPD Policies 12.050 and 12.110, SPD’s data sharing is governed by federal and state criminal justice policies and procedures including <a href="#">state records retention schedules</a>.<sup>2</sup></p>
<p>6. There must be a requirement for SPD to disclose how they ensure authenticity of recordings and individuals in audio recordings.</p>	<p>Not addressed in the SIR.</p> <p><i>Per SMC 14.12.290, SPD must confirm the degree of accuracy of information about incidents of unlawful activity “whenever possible.”</i></p> <p><i>According to SPD, case detectives are responsible for identifying individuals and reviewing any recordings obtained during investigations.</i></p>
<p>7. There must be a requirement for SPD to disclose for how many incidents per year they use Audio Recording Systems.</p>	<p>Not addressed in the SIR.</p> <p><i>According to SPD, TESU maintains request forms/log sheets, which are subject to audit by SPD and the Office of Inspector General for Public Safety (OIG).</i></p>
<p>8. There must be a requirement for an independent audit of SPD’s Audio Recording Systems and that audit must be made publicly available.</p>	<p><b>SIR § 4.2.</b> All deployment of these devices are [sic] documented by TESU and subject to audit by the OIG and federal monitor at any time.</p> <p><i>Per <a href="#">Ordinance 125376</a>, the OIG must conduct an annual review of all approved surveillance technologies.</i></p>
<p>9. There must be a prohibition on use of biometric technology<sup>3</sup> on or with audio recordings.</p>	<p>Not addressed in SIR.</p> <p><i>According to SPD, the department does not use biometric technology in conjunction with Audio Recording Systems.</i></p>

<sup>2</sup> LE06-01-04 Rev. 1

<sup>3</sup> Examples of biometrics include an individual’s DNA, fingerprints, eyeballs/irises/retinas, voiceprints, handprints, and facial geometry. Source: [American Bar Association Publication](#), Biometric Information – Permanent Personally Identifiable Information Risk, Alan S. Wernick, February 14, 2019.

## Policy Considerations

Central Staff has identified the following potential policy considerations. Requests for additional reports and/or policies may require additional resources, potentially via a supplemental budget appropriation.

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

### Options:

- A. Request a report on the proposed metrics by a date certain.
  - B. Take no action.
2. Mitigation of Civil Liberties Impacts. The SIR provides only a boilerplate reference to SPD's general anti-bias policing policies as providing mitigation against the risk of disproportionate surveillance and/or civil liberties impacts. In the absence of data tabulating the frequency of use of the Audio Recording Systems and the corresponding incident types, it is not possible to evaluate whether the Systems are being used inequitably.

### Options:

- A. Request that SPD report on deployment of Audio Recording Systems by incident type and location for the past three years and identify any disproportionate impacts.
  - B. Take no action.
3. Authentication of Recordings. The SIR does not address whether or how SPD ensures the authenticity of its audio recordings. Verification of authenticity would confirm that individuals have been accurately identified and that recordings haven't been accidentally or deliberately compromised.

### Options:

- A. Request that SPD develop policies and procedures for verifying the authenticity of its covert Audio Recordings.
  - B. Take no action.
- cc: Aly Pennucci, Deputy Director  
Brian Goodnight, Supervising Analyst



April 19, 2022

## MEMORANDUM

**To:** Economic Development, Technology and City Light Committee  
**From:** Lise Kaye, Analyst  
**Subject:** Surveillance Impact Report Process and Related Legislation

---

This memo describes legislative history of the City’s Intelligence and Surveillance Ordinances and the process by which the Executive produces a Surveillance Impact Report (SIR).

### **Powers and Functions of Seattle Police Department’s Criminal Information Section<sup>1</sup>**

The Seattle City Council (Council) adopted [Ordinance 108333](#), often referred to as Seattle’s “Intelligence Ordinance,” in 1979 and amended it in 1982 via adoption of [Ordinance 110572](#). Section 27 of Ordinance 108333 defines Seattle Police Department’s Criminal Intelligence powers and functions, including the following authority to:

- collect, evaluate, organize, and analyze data and specific investigative information about organized criminal activity (subsequently defined by Ordinance 100572 as “a continuing enterprise engaged in solely for the purpose of obtaining monetary gain... through racketeering, vice, narcotics, gambling, fencing, or similar criminal activity”);
- collect, evaluate, and classify information about incidents of unlawful activity, confirming the degree of accuracy of the information whenever possible;
- study, detect and explain any meaningful patterns of unlawful activities;
- furnish and exchange relevant criminal intelligence information with criminal justice agencies; and
- develop methods for evaluating the effectiveness of the Criminal Intelligence Section in accomplishing its law enforcement purposes and safeguarding the constitutional rights and privacy of all individuals.

Ordinance 110572 also established policies governing the collection, recording, retention and sharing of information by SPD personnel ([SMC 14.12.020](#)), including the following directives:

- All collected information shall reasonably appear relevant to the performance of an authorized police function;
- Only information deemed relevant to present and future law enforcement activities or required by law shall be retained;
- Authorized disclosure of information, including when needed by criminal justice functions, for scientific or law enforcement research under assurance of confidentiality, and when pertinent to agencies with regulatory responsibilities.

---

<sup>1</sup> [SMC 14.12.290](#)

## Acquisition and Use of Surveillance Technologies<sup>2</sup>

[Ordinance 125376](#), passed by Council on July 31, 2017, requires City of Seattle departments intending to acquire surveillance technology to obtain advance Council approval, by ordinance, of the acquisition and of a SIR.<sup>3</sup> Departments must also submit an SIR for surveillance technology in use when Ordinance 125376 was adopted (referred to in the ordinance as “retroactive technologies”), but failure to approve an ordinance for a retroactive technology does not require a department to discontinue its use. Councilmembers may choose to amend an ordinance to request additional information or to request that the Executive develop new and/or revised operational policies, which, if implemented, could restrict or modify the application of certain technologies. As of April 1, 2021, the Council has accepted SIRs for 16 of the 28 technologies on the current Master List and extended the initial March 3, 2020 deadline to complete the retroactive SIRs to September 1, 2022.<sup>4</sup>

Either the Chief Technology Officer or the Council may determine whether a specific technology is “surveillance technology” and thus subject to the requirements of SMC 14.18. Each SIR must describe protocols for a “use and data management policy” as follows:

- How and when the surveillance technology will be deployed or used and by whom.
- How surveillance data will be securely stored.
- How surveillance data will be retained and deleted.
- How surveillance data will be accessed.
- Whether a department intends to share access to the technology or data with any other entity.
- How the department will ensure that personnel who operate the technology and/or access its data can ensure compliance with the use and data management policy.
- Any community engagement events and plans.
- How the potential impact of the surveillance on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities have been taken into account, and a mitigation plan.
- The fiscal impact of the surveillance technology.

---

<sup>2</sup> [SMC 14.18](#)

<sup>3</sup> As codified in SMC 14.18.030, Ordinance 125376 identified a number of exemptions and exceptions to the required Council approval, including information voluntarily provided, body-worn cameras and cameras installed in or on a police vehicle, cameras that record traffic violations, security cameras and technology that monitors City employees at work.

<sup>4</sup> As provided for in [Ordinance 125679](#), Council has granted five six-month extension requests: first to accommodate extended deliberation of the first two SIRs; and then four more primarily due to COVID-related delays and/or to provide additional time for public engagement.

## Community Surveillance Working Group

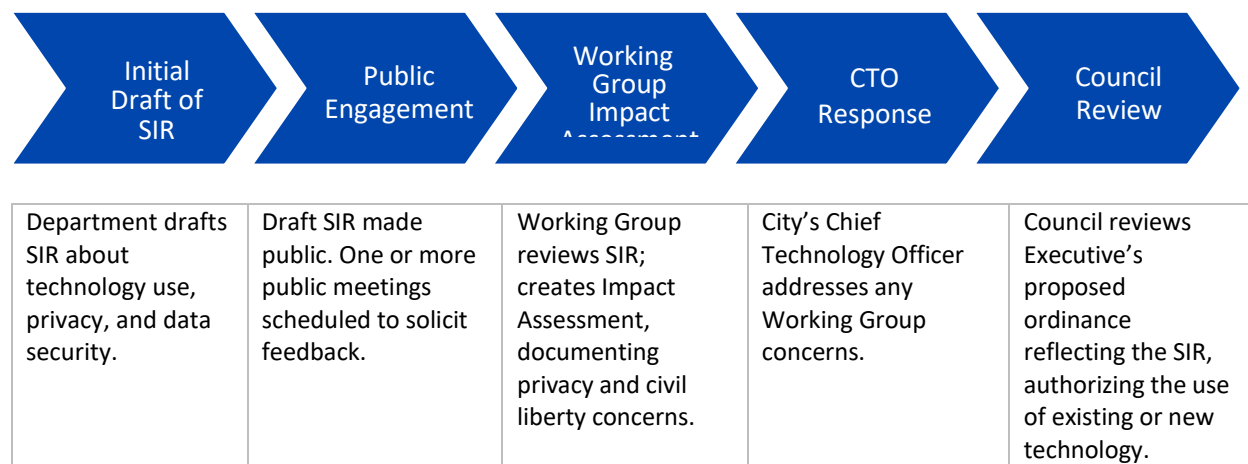
On October 5, 2018, Council passed [Ordinance 125679](#), amending SMC 14.18, creating a “community surveillance working group” charged with creating a Privacy and Civil Liberties Impact Assessment for each SIR. At least five of the seven members of the Working Group must represent groups that have historically been subject to disproportionate surveillance, including Seattle’s diverse communities of color, immigrant communities, religious minorities, and groups concerned with privacy and protest.<sup>5</sup> Each Privacy and Civil Liberties Impact Assessment must describe the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities and will be included in the SIR. Prior to submittal of a SIR to Council, the Chief Technology Officer may provide a written statement that addresses privacy rights, civil liberty or other concerns in the Working Group’s impact assessment.

## Executive Overviews

In May 2019, members of the Governance, Equity, and Technology Committee requested that the Seattle Information Technology Department staff prepare a summary section for each of the two lengthy SIR documents under review at that time. The Committee then accepted the resultant “Condensed Surveillance Impact Reports (CSIRs) together with the complete SIRs. The Executive has continued this practice with subsequent SIRs but has renamed the documents “Executive Overviews.” The Operational Policy Statements in the Executive Overview represent the only allowable uses of the subject technology.

## SIR Process

The following chart illustrates the SIR process from inception to Council Review:



cc: Aly Pennucci, Interim Director  
Brian Goodnight, Lead Analyst

<sup>5</sup> The Mayor appoints four members, and the Council appoints three members.



Legislation Text

---

**File #:** CB 120308, **Version:** 1

---

**CITY OF SEATTLE**

**ORDINANCE \_\_\_\_\_**

**COUNCIL BILL \_\_\_\_\_**

AN ORDINANCE relating to surveillance technology implementation; authorizing approval of uses and accepting the 2021 surveillance impact report and 2021 executive overview for the Seattle Police Department's use of Maltego.

WHEREAS, Section 14.18.020 of the Seattle Municipal Code (SMC), enacted by Ordinance 125376 and last amended by Ordinance 125679, requires City Council approval of a surveillance impact report (SIR) related to uses of surveillance technology, with existing/retroactive technology to be placed on a Master Technology List; and

WHEREAS, SMC 14.18.020 applies to the Maltego software in use by the Seattle Police Department (SPD); and

WHEREAS, SPD conducted policy rule review and community review as part of the development of the SIR; and

WHEREAS, SMC 14.18.080, enacted by Ordinance 125679, also requires review of the SIR by the Community Surveillance Working Group, composed of relevant stakeholders, and a statement from the Chief Technology Officer in response to the Working Group's recommendations; and

WHEREAS, development of the SIR and review by the Working Group have been completed; NOW,

THEREFORE,

**BE IT ORDAINED BY THE CITY OF SEATTLE AS FOLLOWS:**

Section 1. Pursuant to Ordinances 125376 and 125679, the City Council approves use of the Seattle Police Department's Maltego software. The City Council accepts the December 17, 2021, Surveillance Impact

Report (SIR) for this technology, attached to this ordinance as Attachment 1, and the Executive Overview for the same technology, attached to this ordinance as Attachment 2.

Section 2. This ordinance shall take effect and be in force 30 days after its approval by the Mayor, but if not approved and returned by the Mayor within ten days after presentation, it shall take effect as provided by Seattle Municipal Code Section 1.04.020.

Passed by the City Council the \_\_\_\_\_ day of \_\_\_\_\_, 2022, and signed by me in open session in authentication of its passage this \_\_\_\_\_ day of \_\_\_\_\_, 2022.

\_\_\_\_\_  
President \_\_\_\_\_ of the City Council

Approved / returned unsigned / vetoed this \_\_\_\_\_ day of \_\_\_\_\_, 2022.

\_\_\_\_\_  
Bruce A. Harrell, Mayor

Filed by me this \_\_\_\_\_ day of \_\_\_\_\_, 2022.

\_\_\_\_\_  
Monica Martinez Simmons, City Clerk

(Seal)

**Attachments:**

Attachment 1 - 2021 Surveillance Impact Report: Link Analysis Software - Maltego

Attachment 2 - 2021 Surveillance Impact Report Executive Overview: Maltego

**2021 Surveillance Impact Report**

# **Link Analysis Software - Maltego**

**Seattle Police Department**

<b>Surveillance Impact Report (“SIR”) overview .....</b>	<b>3</b>
<b>Privacy Impact Assessment .....</b>	<b>4</b>
<b>Financial Information.....</b>	<b>17</b>
<b>Expertise and References.....</b>	<b>18</b>
<b>Racial Equity Toolkit (“RET”) and engagement for public comment worksheet .</b>	<b>19</b>
<b>Privacy and Civil Liberties Assessment .....</b>	<b>32</b>
<b>CTO Response .....</b>	<b>37</b>
<b>Appendix A: Glossary .....</b>	<b>42</b>
<b>Appendix B: Meeting Notice(s) .....</b>	<b>44</b>
<b>Appendix C: All Comments Received from Members of the Public.....</b>	<b>47</b>
<b>Appendix D: Letters from Organizations or Commissions.....</b>	<b>56</b>

## 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”.

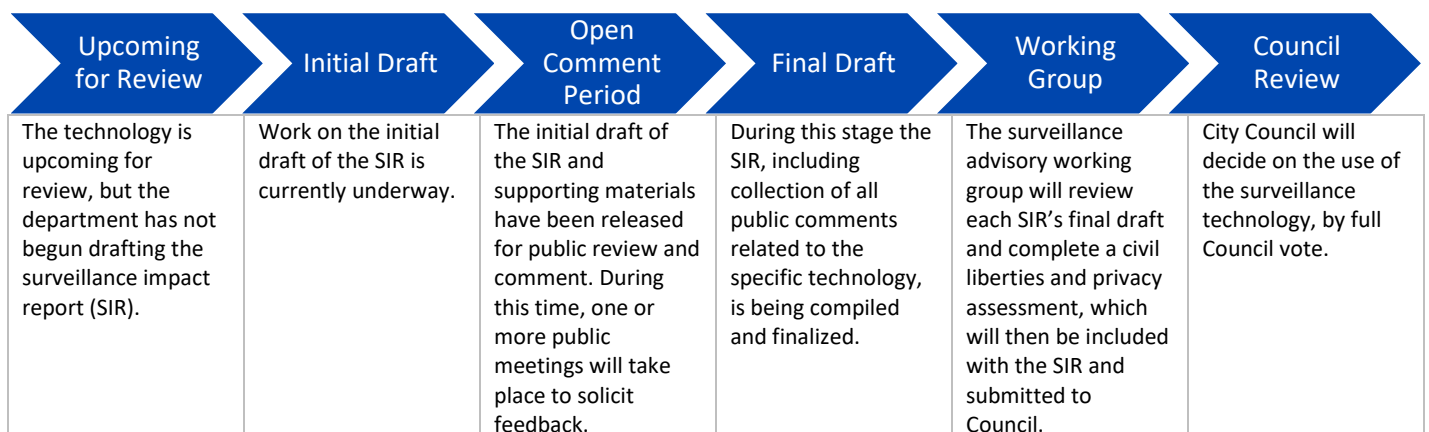
### How this Document is Completed

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.





# 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

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

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.”<sup>1</sup> 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).

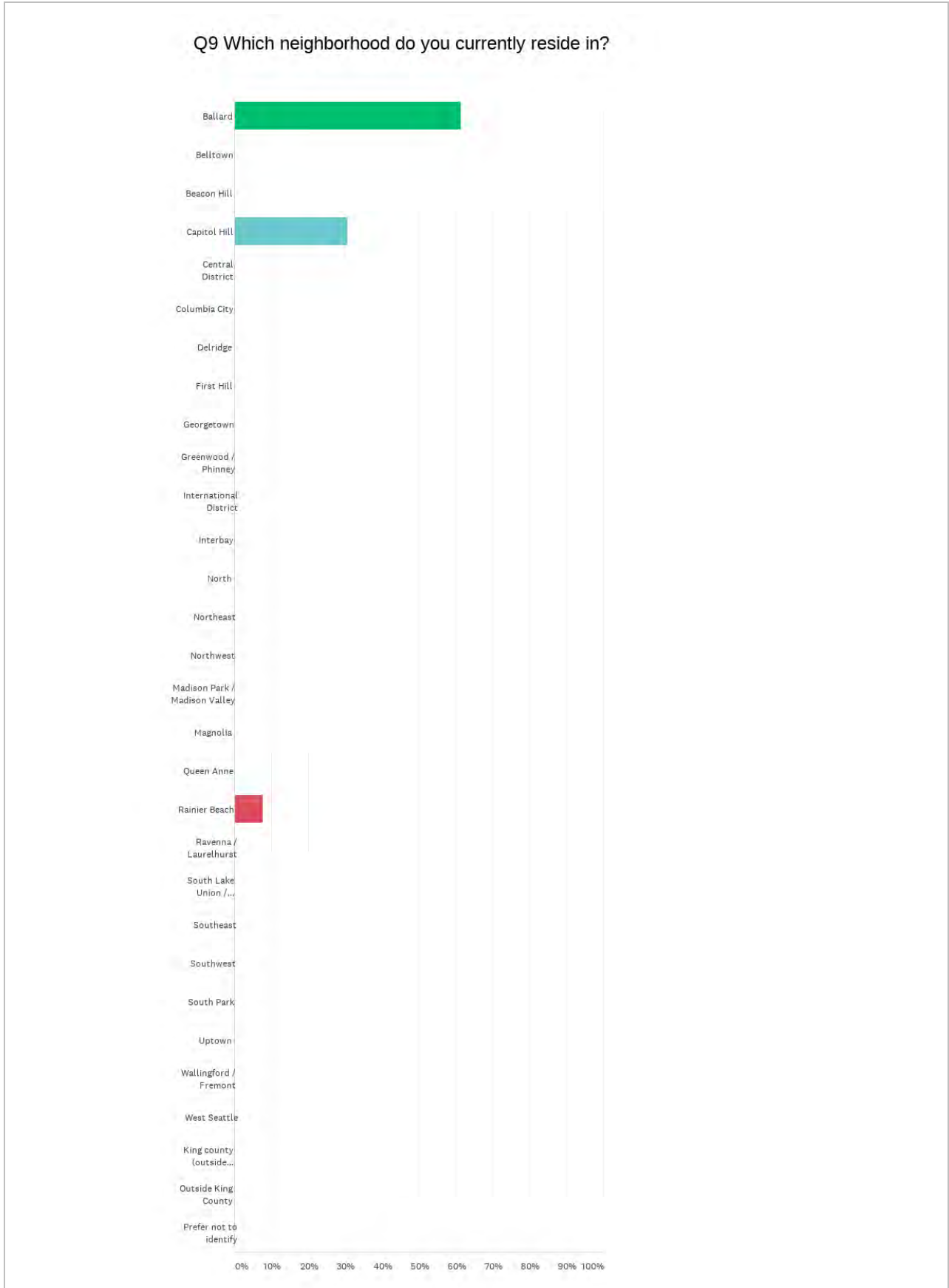
<b>Location</b>	Virtual Event
<b>Time</b>	Thursday, June 10 <sup>th</sup> , 12 PM

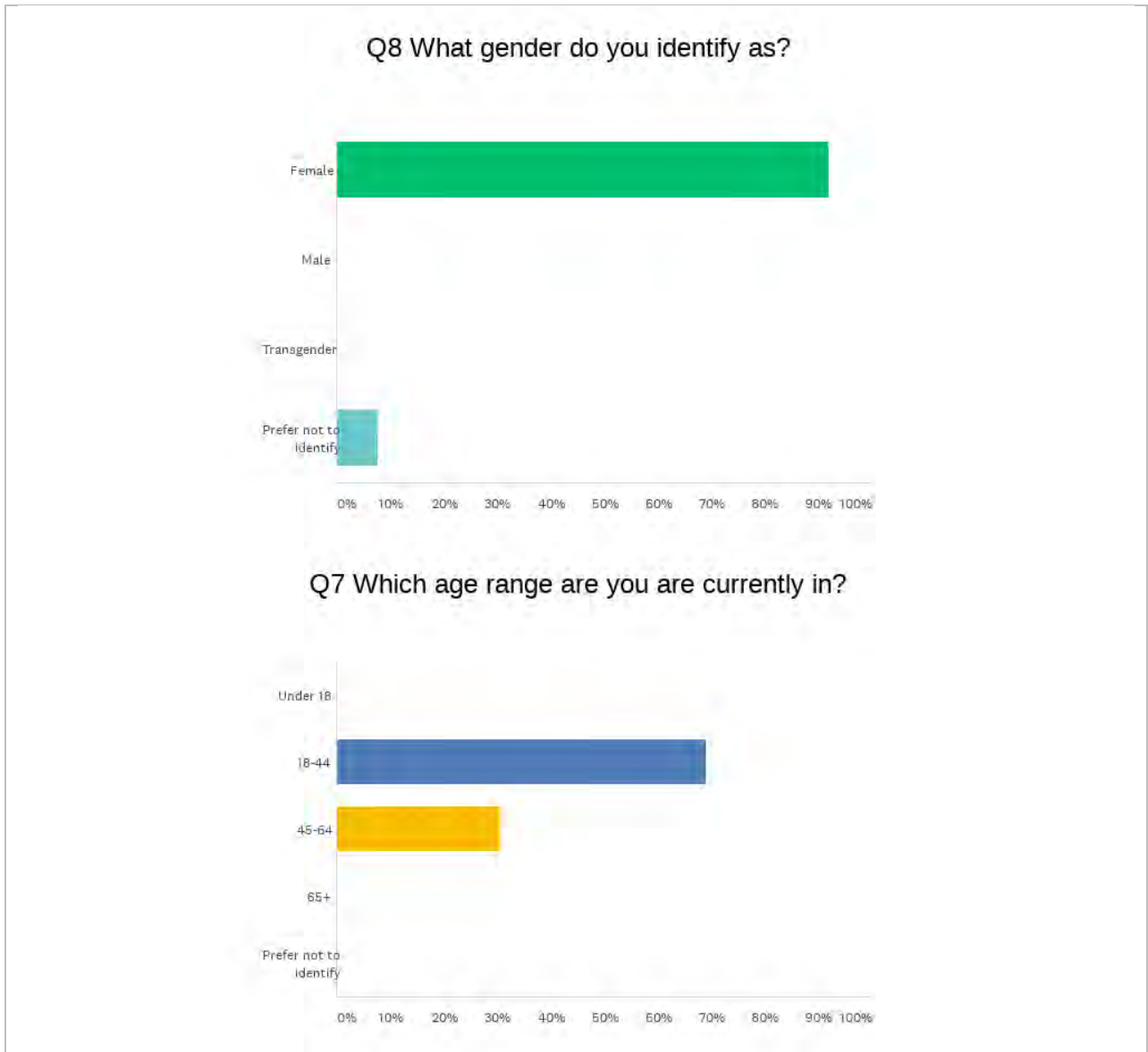
<b>Location</b>	Virtual Event
<b>Time</b>	Tuesday, June 29 <sup>th</sup> , 3 PM

### **3.0 Public Comment Analysis**

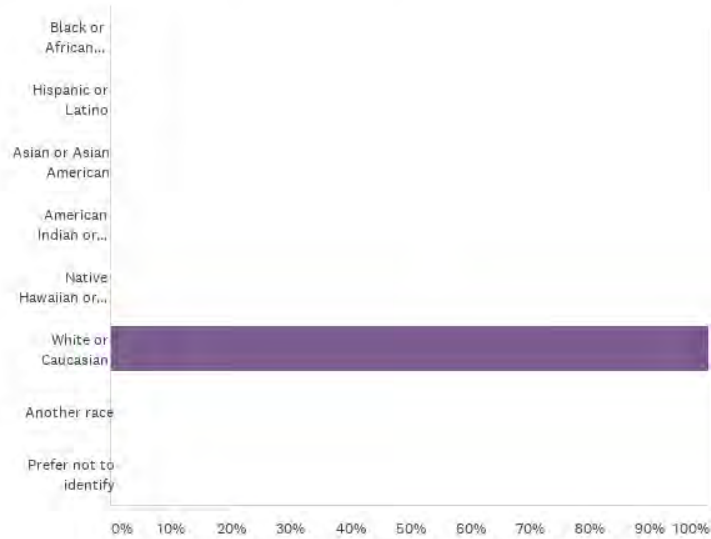
This section will be completed after the public comment period has been completed. Please note due to the volume of comments, analysis represents a summarization of all comments received. Technology specific comments will be included in Appendix C.

#### **3.1 Summary of Response Volume**





### Q6 Which race(s) / ethnicity (or ethnicities) you identify as.





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

Q2 What concerns, if any, do you have about the use of this technology?

response question survey withholding information public comment open questions  
 RMS Mark43 opposed informed public comment Missing information due  
 hinder ability informed SPD using thus greatly hinder TESU public answered thus  
 incorporates numerous questions public regarding answers questions numerous since  
 dodged providing answers per year use Additionally SPD dodged  
 many incidents per engagement meetings Additionally SPD specified many  
 4a public engagement clarity regarding magnitude public Group 4a  
 data retention period allocated questions public incident types SPD  
 little time allocated CAD etc incident audio recordings defining limiting CAD  
 Lack transparency Thus concerns include use Maltego concerns will Thus whether  
 questions list concerns via answers open questions etc worst missing answers  
 used privacy-wise assume worst **Callyo apps**  
 approach security privacy-wise  
**audio recording devices** Since safest approach  
**data** survey Since safest **SPD** safest approach security **iBase**  
 security privacy-wise assume **Maltego** assume worst missing  
**Lack clarity regarding** missing answers open  
**use Callyo apps** open questions list access list concerns will installed  
 will Thus concerns apps policy defining limiting Maltego SIR limiting CAD etc  
 regarding whether etc incident types use iBase types SPD may  
 time allocated questions SPD RMS Mark43 questions public Group  
 regarding magnitude use Group 4a public specified many incidents  
 public engagement meetings incidents per year meetings Additionally SPD  
 Surveillance always concern SPD dodged providing Security  
 providing answers questions record questions numerous questions audio  
 questions public answered deployment answered thus greatly write access  
 greatly hinder ability One safely assume ability informed public SPD withholding information  
 public comment open recording devices use SPD use Maltego question survey Since

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

Q3 What value, if any, do you see in the use of this technology?

Remains seen value **None**

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

Q4 What do you want City leadership to consider about the use of this technology?

past history prior Callyo apps Require City leadership past stop funding tool tool Given City security requiring SPD recommend City leadership etc Require SPD problems fixed SPD may used fixed systemic problems version criminal system fixed considerations depend SPD support pipelines criminal TBD valid considerations community needs support update Callyo SIR tools money community per year use surveil residents SPD many incidents per use Maltego SPD disclose many record specific incident types audio recording devices Policy state specific report recent audit questions Require SPD provide date report Require SPD answer SPD publicly provide changes made Require Require SPD Policy changes superficial changes access limited cosmetic changes Require SPD update will pursue limited SPD answer public right instead will

**Require SPD disclose** suspect fundamentally right

**use** surveillance technologies suspect **data**

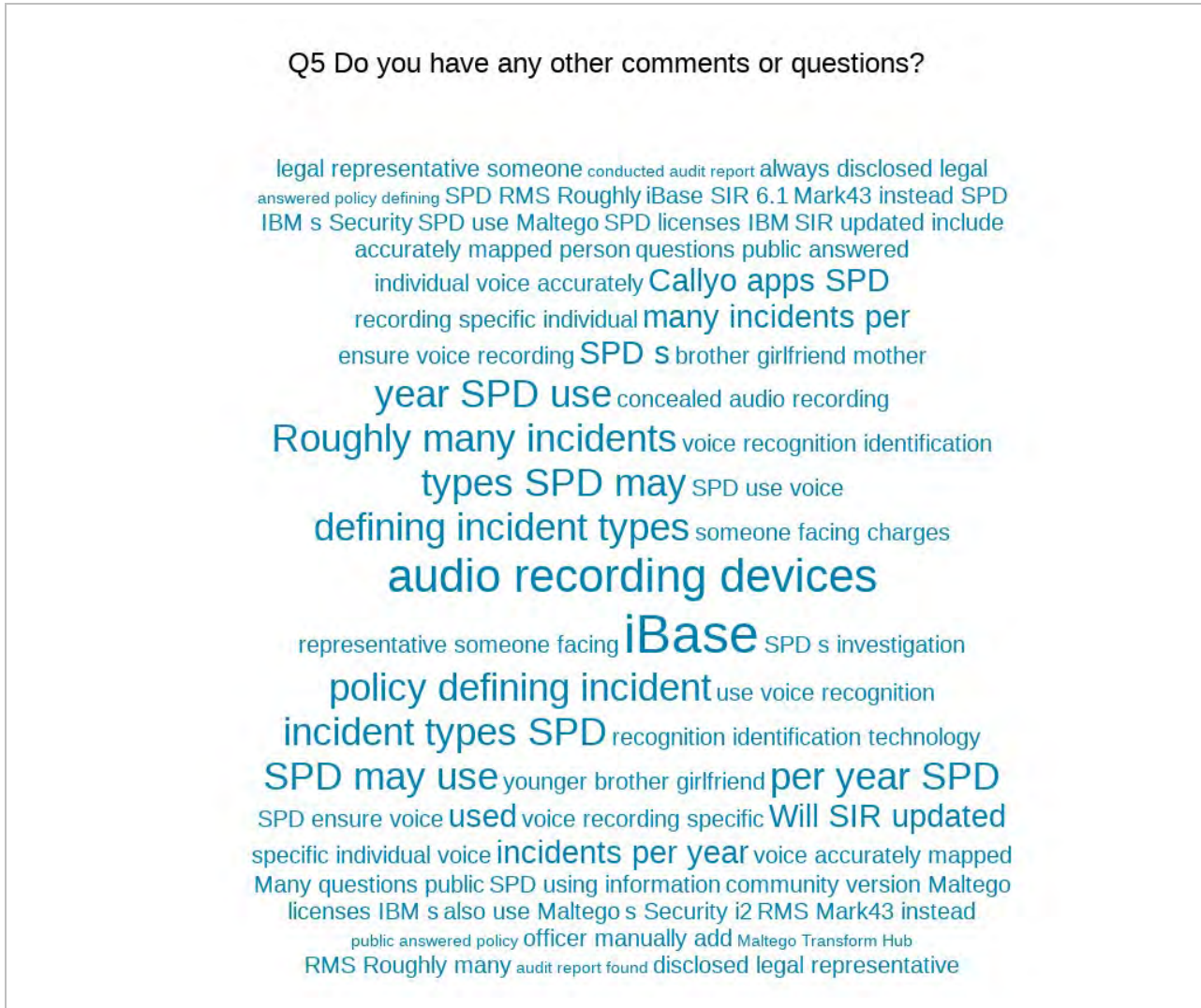
prior surveillance technologies **iBase** technologies suspect fundamentally

**Maltego** fundamentally right instead

**answer public questions** instead will pursue **Callyo apps** pursue limited cosmetic devices cosmetic changes superficial Require SPD publicly superficial changes made publicly provide date made Require SPD date report recent public questions Require recent audit SPD SPD Policy state systems state specific incident Ban Improve security requiring SPD surveil residents disclose many incidents need tools money incidents per year money community needs SPD update Callyo needs support pipelines apps Require SPD pipelines criminal system valid considerations depend system fixed systemic depend SPD answering systemic problems fixed audited tools recommend City audio recordings City leadership stop etc Improve security Given City leadership leadership stop funding leadership past history funding tool Given history prior surveillance

### 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 20<sup>th</sup> 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 Technologies’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.

## 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 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

Share

Share

Print

PDF

Embed

Search

Board

[<< 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.seattle.gov](http://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  $\geq 85$  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 Maltego 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.seattle.gov](http://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  $\geq 85$  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 Maltego 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 > 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 Maltego 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:** 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**

July 23, 2021

Seattle Information Technology  
700 5<sup>th</sup> 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.

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 contain inaccuracies and built-in race and gender biases.<sup>1</sup> Such audio could be later input into a voice recognition or biometrics database, which may further enable both corporate and government surveillance.<sup>2</sup>

<sup>1</sup> 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>.

<sup>2</sup> 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/interpol-s-new-automated-platform-will-recognize-criminals-by-their-voice>.



P.O. Box 2728  
Seattle, WA 98111-2728  
(206) 624-2184  
[aclu-wa.org](http://aclu-wa.org)

Michele Storms  
*Executive Director*

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,<sup>3</sup> the Surveillance Impact Report (SIR) states that Callyo is used to GPS locate individuals.<sup>4</sup> 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.<sup>5</sup> 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.<sup>6</sup> Elsewhere, the SIR states that Callyo's call recording functions may only be used with a search warrant.<sup>7</sup> However, the city's webpage states, "Callyo may be used with consent or search warrant."<sup>8</sup> Comments at the June 10<sup>th</sup> and July 20<sup>th</sup> 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

<sup>3</sup> "Speaker Identification" *GoVivian.com*, Accessed June 10, 2021, <https://www.govivian.com/products/speaker-identification/>; "Voice Authentication," *Aware Biometrics*, Accessed June 10, 2021, <https://www.noware.com/voice-authentication/>; "Forensic Voice Analysis," *Sestek.com*, Accessed June 10, 2021, <https://www.sestek.com/forensic-voice-analysis/>; "Voice Inspector for Forensic Experts," *Phonecta.com*, Accessed June 10, 2021, <https://www.phonecta.com/en/use-case/audio-forensics-software/>.

<sup>4</sup> 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=10FVHt2cyv8>.

<sup>5</sup> Seattle Police Department, "2021 Surveillance Impact Report: Callyo," Accessed June 7, 2021, <https://www.seattle.gov/Documents/Departments/Tech/Privacy/Public%20Engagement%20SIR%200-2%20Callyo.pdf>, 5-7.

<sup>6</sup> "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/>.

<sup>7</sup> SPD, "Callyo," 5.

<sup>8</sup> *Ibid.*, 7, 10, and 11.

<sup>9</sup> "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.<sup>9</sup> 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,<sup>10</sup> despite HRVU's larger share of the annual Callyo budget.<sup>11</sup> 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,"<sup>12</sup> 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.<sup>13</sup> 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.<sup>14</sup> When asked about possible Motorola collection of Callyo data during the July 20<sup>th</sup> 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

<sup>9</sup> SPD, "Callyo," 10, 11, 13, and 17.

<sup>10</sup> *Ibid.*, 7-11.

<sup>11</sup> *Ibid.*, 18.

<sup>12</sup> *Ibid.*, 14.

<sup>13</sup> "Investigative Solutions," *Callyo.com*, Accessed June 16, 2021,

<https://callyo.com/investigations/investigative-solutions>.

<sup>14</sup> "Callyo," *Amazon Web Services*,

<https://partners.amazonaws.com/partners/0010L00001pRHaCQA3W/Callyo>; "10-21 Video," *Callyo.com*, Accessed June 7, 2021, <https://callyo.com/public-safety/10-21-video>.



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.<sup>15</sup> 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.<sup>16</sup> 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.<sup>17</sup> 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.<sup>18</sup> 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 its surveillance capabilities more forceful.<sup>19</sup> Callyo also includes numerous additional surveillance features, such as video recording and live streaming<sup>20</sup> and “10-

<sup>15</sup> SPD, “Callyo,” 14-16.

<sup>16</sup> *Ibid.*, 7 and 10.

<sup>17</sup> See “Supervisors and commanding officers are responsible for ensuring compliance with policies,” at SPD, “Callyo,” 9.

<sup>18</sup> “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-1c5ERKAL5Mmn9y271/>.

<sup>19</sup> 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/>.

<sup>20</sup> “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.<sup>21</sup> 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.<sup>22</sup> Flight-based video tools can be and have been<sup>23</sup> 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:

<sup>21</sup> “10-21 Flight,” *Callyo.com*, Accessed June 7, 2021, <https://callyo.com/public-safety/10-21-flight>.  
<sup>22</sup> 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/>.  
<sup>23</sup> “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.<sup>24</sup> SPD uses i2 iBase in partnership with a second IBM application, i2 Analyst's Notebook,<sup>25</sup> 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."<sup>26</sup> 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.<sup>27</sup>

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

<sup>24</sup> "IBM Security i2 iBase: FAQs," *IBM.com*, Accessed June 10, 2021, <https://www.ibm.com/products/i2-ibase>.

<sup>25</sup> 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.

<sup>26</sup> "IBM Security i2 Analyst's Notebook," *IBM.com*, Accessed June 10, 2021, <https://www.ibm.com/products/i2-analysts-notebook>.

<sup>27</sup> "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.<sup>28</sup>

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.<sup>29</sup> The RTCC is a “centralized data and logistics hubs” that allows analysts to provide data to officers on the street.<sup>30</sup> Second, investigating officers use iBase to collect and organize timeline and relationship data for cases in progress.<sup>31</sup>

Although SPD describes using iBase only to assess RMS and CAD data, iBase can process larger data pools and operate as a data magnet. For instance, the Durham, NC Police Department has considered importing city utility data, recreational park logs, and daily jail visitor lists into iBase.<sup>32</sup> 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.”<sup>33</sup> 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.<sup>34</sup> The SIR does not describe any SPD policy that would prevent additional data from being added to iBase. During the July 20<sup>th</sup> 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.<sup>35</sup> 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

<sup>28</sup> “IBM Security i2 Analyst’s Notebook: Feature Spotlights,” IBM.com, Accessed June 10, 2021, <https://www.ibm.com/products/i2-analysts-notebook/details>.

<sup>29</sup> SPD, “IBM i2 iBase,” 5.

<sup>30</sup> 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/>.

<sup>31</sup> SPD, “i2 iBase,” 5-6.

<sup>32</sup> “Digital Dragnet: How Data Became a Cop’s Best Weapon,” *GCN*, November 29, 2011, <https://gcn.com/Articles/2011/12/05/Predictive-policing-tech-features.aspx?Page=2>.

<sup>33</sup> “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-to-social-links-brings-the-osint-solution-to-ibms-i2-analysts-notebook-platform/>.

<sup>34</sup> “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/>.

<sup>35</sup> Timothy Crocker, “The Power of Social Network Analysis,” *Police Chief Magazine*, Accessed June 11, 2021, <https://www.policemagazine.com/power-social-network-analysis/>.

Indigenous<sup>36</sup> – 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).<sup>37</sup> SNA is a problematic mode of analysis, in part because it is often used for predictive policing via “heat-mapping.” iBase advertises such features.<sup>38</sup> 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.<sup>39</sup>

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<sup>40</sup> – 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

<sup>36</sup> 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://hsa.tsp.gov/content/guid/pdf/csp15.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/>;

<sup>37</sup> SPD “IBM i2 iBase,” 6.

<sup>38</sup> “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>.

<sup>39</sup> 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>.

<sup>40</sup> 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,” *ICJLA Research Hub*, Accessed July 23, 2021, <https://icja.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."<sup>41</sup> However, that claim conflicts with assertions that iBase's automated processing will "create[e] relevant intelligence from large amounts of data,"<sup>42</sup> and will create new "efficiencies" by avoiding manual data management.<sup>43</sup> 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"<sup>44</sup> 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.

---

<sup>41</sup> SPD, "IBM i2 iBase," 27.

<sup>42</sup> *Ibid.*, 7.

<sup>43</sup> *Ibid.*, 6, 21, and 27.

<sup>44</sup> *Ibid.*, 10.

- c. Lack of Clarity 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.<sup>45</sup> 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<sup>46</sup> and suggests that officers would manually input only single “piece[s] of data.”<sup>47</sup> 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.

---

<sup>45</sup> Ibid., 7.

<sup>46</sup> Ibid.

<sup>47</sup> Ibid., 6.

- i. **Data Deletion.** The SIR states that manually entered data will be automatically deleted after five years.<sup>48</sup> 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.”<sup>49</sup> 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”<sup>50</sup> 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?

---

<sup>48</sup> Ibid., 10.

<sup>49</sup> Ibid., 11.

<sup>50</sup> 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.<sup>51</sup> The SIR does not specify the particular audio recording technology

---

<sup>51</sup> 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-%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.<sup>52</sup> Although the SIR is unclear about the type or model of devices used, at the July 20<sup>th</sup> 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.<sup>53</sup> 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.<sup>54</sup> 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.<sup>55</sup> 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.

<sup>52</sup> *Ibid.*, 6.

<sup>53</sup> 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-thinner.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-ops-allentown-city-hall-investigation-wiretaps-20180201-story.html>.

<sup>54</sup> Michael Dumiak, “Interpol’s New Software Will Recognize Criminals by Their Voices,” *Spectrum IEEE.org*, May 16, 2018, <https://spectrum.ieee.org/tech-talk/consensus/electronics/audiovideo/interpol-new-automated-platform-will-recognize-criminals-by-their-voices>; “Speaker Identification” *GoVoice.com*, Accessed June 10, 2021, <https://www.govoice.com/products/speaker-identification/>; “Voice Authentication,” *Awave Biometrics*, Accessed June 10, 2021, <https://www.awave.com/voice-authentication/>; “Forensic Voice Analysis,” *Sivtek.com*, Accessed June 10, 2021, <https://www.sivtek.com/forensic-voice-analysis/>; “Voice Inspector for Forensic Experts,” *Phonocia.com*, Accessed June 10, 2021, <https://www.phonocia.com/en/use-case/an-a-forensics-software/>.

<sup>55</sup> SPD, “Audio Recording Systems (“Wires”),” 12.

## 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.”<sup>56</sup> 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.<sup>57</sup> However, neither the SIR nor the June 10<sup>th</sup> or July 20<sup>th</sup> 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.

---

<sup>56</sup> Ibid., 4.

<sup>57</sup> Ibid.

- d. **Lack of Clarity on Types of Devices Used.** The SIR does not specify the manufacturer or function of devices used.<sup>58</sup> 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."<sup>59</sup> 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,<sup>60</sup> but also that the investigating officer is responsible for the purge.<sup>61</sup> 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 4<sup>th</sup> amendment rights and Washington consent laws.
- g. **Security Risks Associated with Third Party Data Sharing.** The SIR describes third-party data sharing only vaguely.<sup>62</sup> 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<sup>63</sup> but elsewhere states that TESU does so.<sup>64</sup> 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.

---

<sup>58</sup> Ibid., 5 and 16.

<sup>59</sup> Ibid., 8.

<sup>60</sup> Ibid., 6.

<sup>61</sup> Ibid., 11.

<sup>62</sup> Ibid., 12.

<sup>63</sup> Ibid., 10.

<sup>64</sup> 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.

- 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.”<sup>65</sup> There are multiple versions of Maltego that include different functions and data packages.<sup>66</sup> SPD states that they use the free, community version to assess information which is already publicly available online, primarily in the course of cybercrime investigations.<sup>67</sup>

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

<sup>65</sup> “Law Enforcement,” *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/law-enforcement/>.

<sup>66</sup> “Pricing,” *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/pricing-plans/>.

<sup>67</sup> “Products,” *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/products/>.

<sup>68</sup> 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.

<sup>69</sup> “The Five Pillars of the Maltego Officer,” *Maltego.com*, Accessed June 4, 2021,

<https://www.maltego.com/blog/the-five-pillars-of-the-maltego-officer/>.

<sup>70</sup> “Transform Hub,” *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/transformhub/>.

<sup>71</sup> “Social Links Pro,” *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/transformhub/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>.

<sup>72</sup> “Social Links CE,” *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/transformhub/social-links-ce/>.

pieces of data.<sup>72</sup> 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.<sup>73</sup> Although the SIR identifies some types of data that SPD does collect, such as web domain ownership information,<sup>74</sup> 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,<sup>75</sup> 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.<sup>76</sup> Notably, Maltego includes a free integration from “Have I Been Pwned,” which may be used to search for such “public” hacked data.<sup>77</sup> 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.<sup>78</sup> 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.<sup>79</sup> 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

<sup>72</sup> John Weber, “Social Links: The All-Round Tools for OSINT Intern Investigations – Part 2,” *Corima*, August 13, 2020, <https://corima.de/en/4-social-links-the-all-round-tool-for-osint-internet-investigations-part-2/>.

<sup>73</sup> “Wayback Machine,” *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/transform-hub/wayback-machine/>.

<sup>74</sup> SPD, “Maltego,” 6.

<sup>75</sup> *Ibid.*, 5.

<sup>76</sup> Joseph Cox, “Police are Buying Access to Hacked Website Data,” *Vice.com*, July 8, 2020, <https://www.vice.com/en/article/3azrvy/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-services-15-websites-offering>.

<sup>77</sup> “Have I Been Pwned,” *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/transform-hub/has-been-pwned/>.

<sup>78</sup> 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>.

<sup>79</sup> 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/88661/2016-law-enforcement-use-of-social-media-survey\\_5.pdf](https://www.urban.org/sites/default/files/publication/88661/2016-law-enforcement-use-of-social-media-survey_5.pdf).

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

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.<sup>85</sup> 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,<sup>86</sup> 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.<sup>87</sup> During the July 20<sup>th</sup> 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.”<sup>88</sup> 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

---

<sup>80</sup> 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\\_Howard\\_L\\_Article.pdf](https://www.brennancenter.org/sites/default/files/publications/images/RLW_Howard_L_Article.pdf), 529.

<sup>81</sup> “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>.

<sup>82</sup> 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.

<sup>83</sup> Lau, “Predictive Policing Explained,” Friend, “Seattle’s New Crime Analytics Program.”

<sup>84</sup> Levinson-Waldman, “Government Access,” 530.

<sup>85</sup> *Ibid.*, 523.

<sup>86</sup> SPD, “Maltego,” 5.

<sup>87</sup> *Ibid.*, 8 and 10.

<sup>88</sup> *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.”<sup>89</sup> 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,”<sup>90</sup> 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.”<sup>91</sup> The SIR indicates that SPD exports Maltego charts back into SPD’s system<sup>92</sup> and suggests that data from Maltego might be used for “defensive” purposes.<sup>93</sup> 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.”<sup>94</sup> 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,”<sup>95</sup> and thereby “help in identifying unknown relationship[s].”<sup>96</sup>

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.<sup>97</sup>

---

<sup>89</sup> Ibid., 6.  
<sup>90</sup> SPD, “Maltego,” 20.  
<sup>91</sup> Law Enforcement, “Maltego.com.”  
<sup>92</sup> SPD, “Maltego,” 9.  
<sup>93</sup> Ibid., 6.  
<sup>94</sup> Ibid., 6 and 14.  
<sup>95</sup> Ibid., 6.  
<sup>96</sup> Ibid.  
<sup>97</sup> 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.<sup>98</sup> 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.<sup>99</sup> 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,”<sup>100</sup> but elsewhere says that private information gathered via search warrant can be input into Maltego.<sup>101</sup> The SIR does not describe measures to keep that private data secure nor outlines Paterva’s or Maltego Technologies’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.<sup>102</sup> 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?

---

<sup>98</sup> Ibid., 9.

<sup>99</sup> Ibid., 10.

<sup>100</sup> Ibid., 9.

<sup>101</sup> Ibid., 6.

<sup>102</sup> 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



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



### **Callyo (Police)**

1. Data from this application is stored on Amazon Web Services<sup>1</sup>. Will any SPD generated data 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 Motorola 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?

---

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



### **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?



## 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<sup>2</sup>. 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?

---

<sup>2</sup> <https://gspp.berkeley.edu/assets/uploads/research/pdf/SpencerCharbonneauGlaser.Compass.2016.pdf>



## 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?





### *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 Maltego 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?

## 2021 Surveillance Impact Report Executive Overview

# Maltego

## Seattle Police Department

## Overview

**The Operational Policy statements in this document represent the only allowable uses of the equipment and data collected by this technology.**

This Executive Overview documents information about the collection, use, sharing, security and access controls for data that is gathered through SPD's Maltego. All information provided here is contained in the body of the full Surveillance Impact Review (SIR) document but is provided in a condensed format for easier access and consideration.

### 1.0 Technology Description

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.

### 2.0 Purpose

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.

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.

### 3.0 Data Collection and Use

**Operational Policy: 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.**

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.

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. 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.

## 4.0 Data Minimization & Retention

**Operational Policy: The software automatically alerts users of data that must be deleted under legal deletion requirements such as 28 CFR Part 23.**

**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.

## 5.0 Access & Security

**Operational Policy: 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.

### Access

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.

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.

### Security

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.

## 6.0 Data Sharing and Accuracy

**Operational Policy: 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.

## 7.0 Equity Concerns

**Operational Policy: 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 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.**

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.

## SUMMARY and FISCAL NOTE\*

<b>Department:</b>	<b>Dept. Contact/Phone:</b>	<b>CBO Contact/Phone:</b>
SPD / ITD	Rebecca Boatwright Vinh Tang/206-684-7640	Neal Capapas/206-684-5292

*\* Note that the Summary and Fiscal Note describes the version of the bill or resolution as introduced; final legislation including amendments may not be fully described.*

### **1. BILL SUMMARY**

**Legislation Title:** AN ORDINANCE relating to surveillance technology implementation; authorizing approval of uses and accepting the 2021 surveillance impact report and 2021 executive overview for the Seattle Police Department’s use of Maltego.

**Summary and background of the Legislation:** Per SMC Chapter 14.18 (also known as the Surveillance Ordinance), authorizing the approval of the surveillance impact reports for Seattle Police Department’s continued use of Maltego.

### **2. CAPITAL IMPROVEMENT PROGRAM**

**Does this legislation create, fund, or amend a CIP Project?**      \_\_\_ Yes X No

### **3. SUMMARY OF FINANCIAL IMPLICATIONS**

**Does this legislation amend the Adopted Budget?**      \_\_\_ Yes X No

**Does the legislation have other financial impacts to The City of Seattle that are not reflected in the above, including direct or indirect, short-term or long-term costs?**

This technology is currently in use by the Seattle Police Department and no additional costs, either direct or indirect, will be incurred based on the continued use of the technology. However, should it be determined, that SPD should cease use of the technology, there would be costs associated with decommissioning the technologies. Additionally, there may be potential financial penalty related to breach of contract with the technology vendors.

**Is there financial cost or other impacts of *not* implementing the legislation?**

Per the Surveillance Ordinance, the City department may continue use of the technology until legislation is implemented. As such, there are no financial costs or other impacts that would result from not implementing the legislation.

### **4. OTHER IMPLICATIONS**

**a. Does this legislation affect any departments besides the originating department?**

This legislation does not affect other departments. The technology under review is used exclusively by the Seattle Police Department.

**b. Is a public hearing required for this legislation?**

A public hearing is not required for this legislation.

**c. Is publication of notice with The Daily Journal of Commerce and/or The Seattle Times required for this legislation?**

No publication of notice is required for this legislation.

**d. Does this legislation affect a piece of property?**

This legislation does not affect a piece of property.

**e. Please describe any perceived implication for the principles of the Race and Social Justice Initiative. Does this legislation impact vulnerable or historically disadvantaged communities? What is the Language Access plan for any communications to the public?**

The Surveillance Ordinance in general is designed to address civil liberties and disparate community impacts of surveillance technologies. Each Surveillance Impact Review included in the attachments, as required by the Surveillance Ordinance, include a Racial Equity Toolkit review adapted for this purpose.

**f. Climate Change Implications**

**1. Emissions: Is this legislation likely to increase or decrease carbon emissions in a material way?**

No.

**2. Resiliency: Will the action(s) proposed by this legislation increase or decrease Seattle's resiliency (or ability to adapt) to climate change in a material way? If so, explain. If it is likely to decrease resiliency in a material way, describe what will or could be done to mitigate the effects.**

No.

**g. If this legislation includes a new initiative or a major programmatic expansion: What are the specific long-term and measurable goal(s) of the program? How will this legislation help achieve the program's desired goal(s)?**

There is no new initiative or programmatic expansion associated with this legislation. It approves the continuation of use for the specific technologies under review.

**List attachments/exhibits below:**



April 19, 2022

## MEMORANDUM

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

---

On Wednesday, April 27, 2022 the Economic Development, Technology and City Light Committee will discuss [Council Bill 120308](#). This Council Bill would approve the Seattle Police Department’s (SPD’s) continued use of Maltego’s Link Analysis Software and accept the Surveillance Impact Report (SIR) and an Executive Overview for this technology. The bill is intended to meet the requirements of [Seattle Municipal Code Chapter 14.18](#), Acquisition and Use of Surveillance Technologies, which requires City of Seattle departments intending to acquire surveillance technology to obtain advance Council approval of that acquisition and of a surveillance impact report (SIR).<sup>1</sup> Departments must also submit a SIR for surveillance technology in use when [Ordinance 125376](#) was adopted in 2017 (referred to in the ordinance as “retroactive technologies”), but failure to approve an ordinance for a retroactive technology does not require SPD to discontinue its use. Councilmembers may choose to amend the ordinance to request additional information or to request that SPD develop new and/or revised operational policies, which, if implemented, could restrict or modify the application of certain technologies.

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

### Maltego’s Link Analysis Software

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

---

<sup>1</sup> The Executive Overview summarizes SPD’s allowable uses of Maltego. See also the [memo](#) summarizing process for developing a Surveillance Impact Report (SIR), consistent with [Ordinances 125376](#) and [125679](#) and [Ordinance 108333](#), Seattle’s “Intelligence Ordinance,” adopted in 1979 and amended in 1982 via adoption of [Ordinance 100572](#).

## Surveillance Working Group Recommendations and CTO Response

The Community Surveillance Working Group’s Impact Assessment for Maltego’s Link Analysis Software makes 15 recommendations to Council. The CTO’s response finds that the “policy, training and technology limitations enacted by SPD provide adequate mitigation for the potential privacy and civil liberties concerns raised by the Working Group.” The CTO’s response does not specifically address the Working Group’s recommendations, but it identifies relevant citations from the SIR for each of the “key concerns” raised by the Working Group. **Table 1** describes whether the SIR as drafted or current law would address the Working Group’s recommendations, as well as relevant responses from the CTO and/or SPD.

*Table 1. Working Group Recommendations*

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

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

<sup>3</sup> According to SPD, Maltego is capable of performing “dark web” searches including forums, torrents, beacons, and other sources.

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

<sup>4</sup> RCW 10.97.080 – Inspection of information by subject-Challenges and corrections: All criminal justice agencies shall permit an individual who is, or who believes that he or she may be, the subject of a criminal record maintained by that agency, to appear in person during normal business hours of that criminal justice agency and request to see the criminal history record information held by that agency pertaining to the individual. *The individual's right to access and review of criminal history record information shall not extend to data contained in intelligence, investigative, or other related files, and shall not be construed to include any information other than that defined as criminal history record information by this chapter. (italics added)*

Working Group Recommendation	Whether/How Addressed by SIR, CTO or SPD
13. Execute agreement with Paterva that prevents them from storing or accessing SPD data	<p><b>SIR §4.7</b> ...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....</p> <p><i>According to SPD, Maltego owns the collected data; once SPD creates a copy of the data, it owns the copy of the data and any resultant analysis. Maltego does not have access to SPD's data or inputs. SPD uses the free, non-commercial use version of this technology and therefore does not have a signed agreement.</i></p>
14. Given lack of auditing and logging capabilities, create additional security measures to prevent improper use of Maltego by those with access	<p><b>SIR §2.4</b> Two users in SPD's Technical and Electronic Support Unit (TESU) are SPD's only trained and authorized users of Maltego.</p> <p><b>SIR §4.10</b> The free version of Maltego, which SPD uses, does not have any internal logging or auditing functions.</p> <p><b>SIR §4.10</b> ...the Unit Supervisor or any auditor may inspect and review the investigative workstation containing the software.</p>
15. SPD must disclose the number of incidents per year analyzed with Maltego	<p>Not addressed in the SIR.</p> <p><i>According to SPD, access to and use of Maltego is tracked at the login level, not at the case level. However, any information obtained from Maltego that is pertinent to a case would be added to SPD's Records Management System's case file.</i></p>

## Policy Considerations

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

1. Annual equity assessment metrics. SPD has not yet finalized metrics to be used in evaluating use of Maltego as part of the CTO's annual equity assessments. These assessments are intended to play a key role in determining whether the City's surveillance legislation is meeting the goals of the Race and Social Justice Initiative. In the absence of such metrics, it is unclear how SPD and/or the CTO could identify disproportionate impacts from the use of Maltego, such as the frequency of specific populations appearing on Maltego diagrams.

### Options:

- A. Request a report on the proposed metrics by a date certain.
  - B. Take no action.
2. Response to Public Comments. The SIR does not provide a response to question 4.1 "How will you address the concerns that have been identified by the public."

### Options:

- A. Request that SPD provide a written response to public comments associated with the SIR public engagement process by a date certain.
- B. Take no action.

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

Options:

- A. Obtain an independent evaluation of the civil liberties risks associated with the use of Maltego, which could include documentation of the types and number of incidents for which SPD has used the system, the databases used by SPD for these analyses, data input by SPD officers, data validation and accuracy of analyses, and demographic information about the individuals and groups associated with each analysis.
- B. Take no action.
4. Contractual Terms – Data and Security Protection. SPD reports that it uses the free version of Maltego and thus has no contractual relationship with its parent company, Paterva. The lack of a contract and/or reliance upon a vendor-provided licensing agreement may reduce the City's ability to restrict Paterva's access to sensitive and/or private information.<sup>5</sup>

Options:

- A. Request that SPD discontinue use of the free version of Maltego and acquire a version with contractual provisions for data and security protection. This may require additional resources, potentially through a supplemental budget action.<sup>6</sup>
- B. Take no action.
- cc: Aly Pennucci, Deputy Director  
Brian Goodnight, Supervising Analyst

---

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

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

April 19, 2022

## MEMORANDUM

**To:** Economic Development, Technology and City Light Committee  
**From:** Lise Kaye, Analyst  
**Subject:** Surveillance Impact Report Process and Related Legislation

---

This memo describes legislative history of the City’s Intelligence and Surveillance Ordinances and the process by which the Executive produces a Surveillance Impact Report (SIR).

### **Powers and Functions of Seattle Police Department’s Criminal Information Section<sup>1</sup>**

The Seattle City Council (Council) adopted [Ordinance 108333](#), often referred to as Seattle’s “Intelligence Ordinance,” in 1979 and amended it in 1982 via adoption of [Ordinance 110572](#). Section 27 of Ordinance 108333 defines Seattle Police Department’s Criminal Intelligence powers and functions, including the following authority to:

- collect, evaluate, organize, and analyze data and specific investigative information about organized criminal activity (subsequently defined by Ordinance 100572 as “a continuing enterprise engaged in solely for the purpose of obtaining monetary gain... through racketeering, vice, narcotics, gambling, fencing, or similar criminal activity”);
- collect, evaluate, and classify information about incidents of unlawful activity, confirming the degree of accuracy of the information whenever possible;
- study, detect and explain any meaningful patterns of unlawful activities;
- furnish and exchange relevant criminal intelligence information with criminal justice agencies; and
- develop methods for evaluating the effectiveness of the Criminal Intelligence Section in accomplishing its law enforcement purposes and safeguarding the constitutional rights and privacy of all individuals.

Ordinance 110572 also established policies governing the collection, recording, retention and sharing of information by SPD personnel ([SMC 14.12.020](#)), including the following directives:

- All collected information shall reasonably appear relevant to the performance of an authorized police function;
- Only information deemed relevant to present and future law enforcement activities or required by law shall be retained;
- Authorized disclosure of information, including when needed by criminal justice functions, for scientific or law enforcement research under assurance of confidentiality, and when pertinent to agencies with regulatory responsibilities.

---

<sup>1</sup> [SMC 14.12.290](#)

## Acquisition and Use of Surveillance Technologies<sup>2</sup>

[Ordinance 125376](#), passed by Council on July 31, 2017, requires City of Seattle departments intending to acquire surveillance technology to obtain advance Council approval, by ordinance, of the acquisition and of a SIR.<sup>3</sup> Departments must also submit an SIR for surveillance technology in use when Ordinance 125376 was adopted (referred to in the ordinance as “retroactive technologies”), but failure to approve an ordinance for a retroactive technology does not require a department to discontinue its use. Councilmembers may choose to amend an ordinance to request additional information or to request that the Executive develop new and/or revised operational policies, which, if implemented, could restrict or modify the application of certain technologies. As of April 1, 2021, the Council has accepted SIRs for 16 of the 28 technologies on the current Master List and extended the initial March 3, 2020 deadline to complete the retroactive SIRs to September 1, 2022.<sup>4</sup>

Either the Chief Technology Officer or the Council may determine whether a specific technology is “surveillance technology” and thus subject to the requirements of SMC 14.18. Each SIR must describe protocols for a “use and data management policy” as follows:

- How and when the surveillance technology will be deployed or used and by whom.
- How surveillance data will be securely stored.
- How surveillance data will be retained and deleted.
- How surveillance data will be accessed.
- Whether a department intends to share access to the technology or data with any other entity.
- How the department will ensure that personnel who operate the technology and/or access its data can ensure compliance with the use and data management policy.
- Any community engagement events and plans.
- How the potential impact of the surveillance on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities have been taken into account, and a mitigation plan.
- The fiscal impact of the surveillance technology.

---

<sup>2</sup> [SMC 14.18](#)

<sup>3</sup> As codified in SMC 14.18.030, Ordinance 125376 identified a number of exemptions and exceptions to the required Council approval, including information voluntarily provided, body-worn cameras and cameras installed in or on a police vehicle, cameras that record traffic violations, security cameras and technology that monitors City employees at work.

<sup>4</sup> As provided for in [Ordinance 125679](#), Council has granted five six-month extension requests: first to accommodate extended deliberation of the first two SIRs; and then four more primarily due to COVID-related delays and/or to provide additional time for public engagement.

## Community Surveillance Working Group

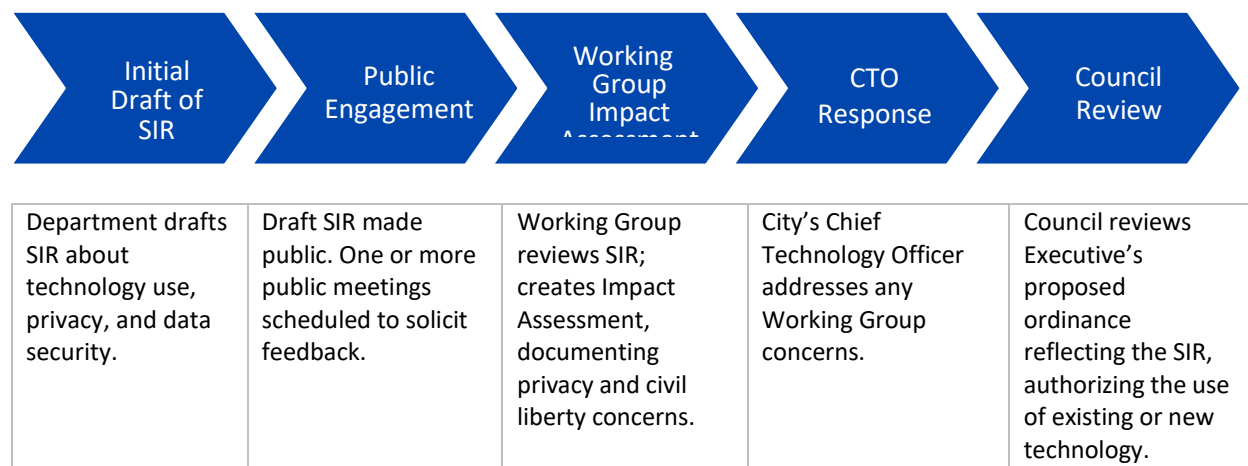
On October 5, 2018, Council passed [Ordinance 125679](#), amending SMC 14.18, creating a “community surveillance working group” charged with creating a Privacy and Civil Liberties Impact Assessment for each SIR. At least five of the seven members of the Working Group must represent groups that have historically been subject to disproportionate surveillance, including Seattle’s diverse communities of color, immigrant communities, religious minorities, and groups concerned with privacy and protest.<sup>5</sup> Each Privacy and Civil Liberties Impact Assessment must describe the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities and will be included in the SIR. Prior to submittal of a SIR to Council, the Chief Technology Officer may provide a written statement that addresses privacy rights, civil liberty or other concerns in the Working Group’s impact assessment.

## Executive Overviews

In May 2019, members of the Governance, Equity, and Technology Committee requested that the Seattle Information Technology Department staff prepare a summary section for each of the two lengthy SIR documents under review at that time. The Committee then accepted the resultant “Condensed Surveillance Impact Reports (CSIRs) together with the complete SIRs. The Executive has continued this practice with subsequent SIRs but has renamed the documents “Executive Overviews.” The Operational Policy Statements in the Executive Overview represent the only allowable uses of the subject technology.

## SIR Process

The following chart illustrates the SIR process from inception to Council Review:



cc: Aly Pennucci, Interim Director  
Brian Goodnight, Lead Analyst

<sup>5</sup> The Mayor appoints four members, and the Council appoints three members.





Legislation Text

---

**File #:** CB 120309, **Version:** 1

---

**CITY OF SEATTLE**

**ORDINANCE \_\_\_\_\_**

**COUNCIL BILL \_\_\_\_\_**

AN ORDINANCE relating to surveillance technology implementation; authorizing approval of uses and accepting the 2021 surveillance impact report and 2021 executive overview for the Seattle Police Department's use of IBM i2 iBase.

WHEREAS, Section 14.18.020 of the Seattle Municipal Code (SMC), enacted by Ordinance 125376 and last amended by Ordinance 125679, requires City Council approval of a surveillance impact report (SIR) related to uses of surveillance technology, with existing/retroactive technology to be placed on a Master Technology List; and

WHEREAS, SMC 14.18.020 applies to the IBM i2 iBase software in use by the Seattle Police Department (SPD); and

WHEREAS, SPD conducted policy rule review and community review as part of the development of the SIR; and

WHEREAS, SMC 14.18.080, enacted by Ordinance 125679, also requires review of the SIR by the Community Surveillance Working Group, composed of relevant stakeholders, and a statement from the Chief Technology Officer in response to the Working Group's recommendations; and

WHEREAS, development of the SIR and review by the Working Group have been completed; NOW,

THEREFORE,

**BE IT ORDAINED BY THE CITY OF SEATTLE AS FOLLOWS:**

Section 1. Pursuant to Ordinances 125376 and 125679, the City Council approves use of the Seattle Police Department's IBM i2 iBase software. The City Council accepts the December 17, 2021, Surveillance

Impact Report (SIR) for this technology, attached to this ordinance as Attachment 1, and the Executive Overview for the same technology, attached to this ordinance as Attachment 2.

Section 2. This ordinance shall take effect and be in force 30 days after its approval by the Mayor, but if not approved and returned by the Mayor within ten days after presentation, it shall take effect as provided by Seattle Municipal Code Section 1.04.020.

Passed by the City Council the \_\_\_\_\_ day of \_\_\_\_\_, 2022, and signed by me in open session in authentication of its passage this \_\_\_\_\_ day of \_\_\_\_\_, 2022.

\_\_\_\_\_  
President \_\_\_\_\_ of the City Council

Approved / returned unsigned / vetoed this \_\_\_\_\_ day of \_\_\_\_\_, 2022.

\_\_\_\_\_  
Bruce A. Harrell, Mayor

Filed by me this \_\_\_\_\_ day of \_\_\_\_\_, 2022.

\_\_\_\_\_  
Monica Martinez Simmons, City Clerk

(Seal)

**Attachments:**

Attachment 1 - 2021 Surveillance Impact Report: Link Analysis Software - IBM i2 iBase

Attachment 2 - 2021 Surveillance Impact Report Executive Overview: IBM i2 iBase

**2021 Surveillance Impact Report**

# **Link Analysis Software - IBM i2 iBase**

**Seattle Police Department**

<b>Surveillance Impact Report (“SIR”) overview .....</b>	<b>3</b>
<b>Privacy Impact Assessment .....</b>	<b>4</b>
<b>Financial Information.....</b>	<b>20</b>
<b>Expertise and References.....</b>	<b>22</b>
<b>Racial Equity Toolkit (“RET”) and engagement for public comment worksheet .</b>	<b>24</b>
<b>Privacy and Civil Liberties Assessment .....</b>	<b>37</b>
<b>CTO Response .....</b>	<b>43</b>
<b>Appendix A: Glossary .....</b>	<b>53</b>
<b>Appendix B: Meeting Notice(s) .....</b>	<b>55</b>
<b>Appendix C: All Comments Received from Members of the Public.....</b>	<b>58</b>
<b>Appendix D: Letters from Organizations or Commissions.....</b>	<b>66</b>

# 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”.

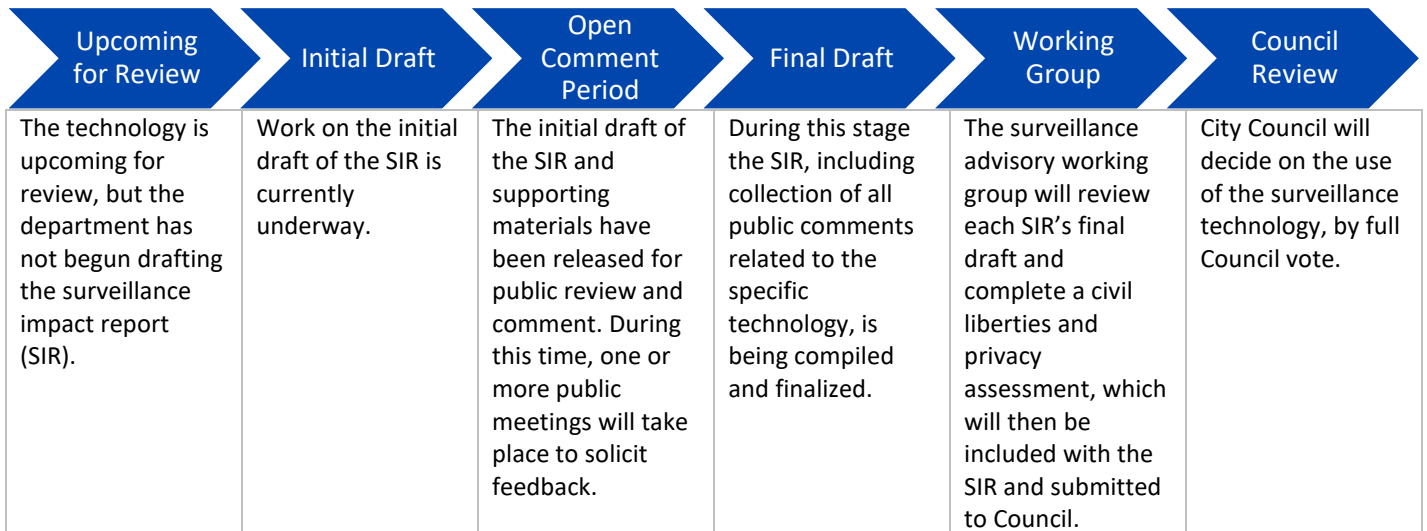
## How this Document is Completed

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.



# 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.

I2 iBase is the server backbone to the i2 Analysts Notebook application, a software system which organizes existing SPD data visually into more accessible information utilized by the SPD Real Time Crime Center (RTCC) employees. The purpose of the RTCC is to provide actionable information to units in the field to increase officer safety, efficiency, and response to incidents. It is also intended to be the information “hub” of the police department, utilizing its resources and collective knowledge to enhance the department's effectiveness at reducing crime and improving public safety. The iBase system combines data stored in SPD's Records Management System (RMS), the Community Safety and Communication Center's (CSCC) Computer Aided Dispatch (CAD) system, and information gathered during criminal investigations and displays information related to ongoing investigations. This type of link analysis software is similar to a virtual “link board” or “pin board”, helping investigators to visualize the connections between known entities, vehicles, locations, etc. in the course of a criminal investigation.

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

Prior to the implementation of the iBase software, investigators were required to re-type all criminal information from RMS onto visualization charts, which was a time-consuming and redundant process. Implementing iBase gave users direct access to that information without having to re-type it. This software is used exclusively for ongoing criminal investigations and therefore necessarily includes personal information about subjects of those investigations.

## 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.

This software prevents investigators from having to re-type RMS information onto a chart. Visualizing criminal information provides investigators a more thorough understanding of complicated criminal investigations.

### 2.2 Provide any data or research demonstrating anticipated benefits.

Professional police departments have been utilizing manual link analysis in the form of “link boards” or “pin boards” for decades, and “connecting the dots” is a hallmark of investigative practice. In the 1990s Malcom Sparrow first introduced the concept of social network analysis to law enforcement and criminal investigations. Link analysis, a component of social network analysis, is a tool used to identify relationships in data. Though simple link analysis with a limited number of points of data can be charted manually, as the number of pieces of data, or “observations” increases, the processing power of a computer helps the analyst provide a more thorough and complete analysis of the links between the available data. Beyond just demonstrating an association, link analysis frequently is employed in an effort to highlight the relative strength of relationships<sup>1</sup>. These types of analysis techniques in criminal intelligence are used to organize data and reveal patterns in the nature and extent of relationships between data points. They also provide effective visualizations of both qualitative and quantitative data which are valuable in presenting intelligence assessments<sup>2</sup>. An important component of link analysis software is the ability for investigators to identify the significance of new information as it is added<sup>3</sup>.

Prior to the implementation of the software, users had to re-type the information associated to a criminal investigation (e.g. Names, Dates of Birth, Criminal Histories) onto a chart if they wished to visualize the case. While no formal study was done of the time wasted on these tasks, adding a single person’s criminal history to a chart could take multiple days of work. With this software, a user can see a subject’s criminal history in minutes.

<sup>1</sup> McCue, Colleen. (2015). Data Mining and Predictive Analysis (Second Edition).

<sup>2</sup> Strang, Steven. (2014). Network Analysis in Criminal Intelligence.

<sup>3</sup> Burcher, Morgan, and Chad Whelan. (2018). “Social Network Analysis as a Tool for Criminal Intelligence: Understanding Its Potential from the Perspectives of Intelligence Analysts.” Trends in Organized Crime 21 (3): 278–94



### **2.3 Describe the technology involved.**

The iBase software is a SQL server that imports a portion of the data from SPD's RMS and CAD systems, allowing users to visualize the data in a link chart (rather than the standard textual display in RMS/CAD). The iBase server is an on-premise security encrypted server housed and managed by Seattle IT meeting CJIS approved requirements. The client i2 Analyst's Notebook software is locally installed on RTCC analysts' workstations. An automated electronic data transfer allows information located within SPD's RMS and CAD systems to be imported into the iBase system via a one-way transfer of data from the source systems to iBase. 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. IBM i2 Analyst's Notebook is the worldwide standard software solution for operational crime analysis and visualization, with the purpose of creating relevant intelligence from large amounts of data. Various types of structured data are compared and visualized through a variety of heatmaps, relationships, and diagrams.

### **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. The utilization of the IBM Security i2 iBase system increases efficiency of investigations, availability of data, awareness of situational information, and timeliness of actionable information to officers on the street.

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

Only trained, backgrounded, and CJIS certified employees of SPD's Real Time Crime Center and supporting Seattle IT employees have access to the i2 iBase system and i2 Analyst's Notebook software.

All authorized users of CAD 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.

IBM Security i2 iBase system is only used during the investigation of crimes by the SPD Real Time Crime Center. Access for personnel into the system is predicated on state and federal law governing access to Criminal Justice Information Services (CJIS). This includes pre-access background information, appropriate role-based permissions as governed by the [CJIS security Policy](#), and audit of access and transaction logs within the system. All users of i2 iBase must be CJIS certified and maintain Washington State ACCESS certification.

Each user must be directly granted an account (tied to their SPD network identity) in order to access the software. The 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.

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

IBM Security i2 iBase system is only used during the investigation of crimes by the SPD Real Time Crime Center and information collected and stored in the system is related to these criminal investigations.

All use of the i2 iBase system must also comply with [SPD Policy 12.050 – Criminal Justice Information Systems](#) and may only be used for legitimate criminal investigative purposes.

Use of the iBase system is governed by the [City of Seattle Intelligence Ordinance \(SMC 14.12\), 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 CAD must be CJIS certified and must maintain Washington State ACCESS certification, and trained directly in the use of the iBase software, in addition to all standard SPD training and Directives.

[SPD Policy 12.050](#) defines the proper use of criminal justice information systems.

Outside of SPD, Seattle Information Technology Department (ITD) client services interaction with SPD systems is governed according to the terms of the 2018 Management Control Agreement (MCA) between ITD and SPD, which states that:

“Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBI's Criminal Justice Information Services, (CJIS) Security Policy.”

## 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.

The only information pulled into iBase automatically comes from SPD's Records Management System (RMS) and CSCC's Computer Aided Dispatch (CAD) system. Users may manually add additional information that they have collected during the course of a criminal investigation,. All manually added information is deleted after five years, in accordance with 28 CFR Part 23. No data outside SPD's RMS/CAD (e.g. commercial data aggregators, publicly available data, or other city departments) is automatically collected.

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

All data entered into the iBase system is directly related to criminal investigations. Individual detectives and analysts may manually enter information not imported from the existing RMS and CAD data systems. Analysts use this software to build networks of individuals associated with criminal cases.

All data changes are logged in the software's audit log, which is reviewed periodically. In addition, when manually adding information, a user must provide the source description, source reliability, and content certainty; all manually added information is purged from the system after 5 years, in compliance with 28 CFR Part 23.

### 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?

IBM i2 iBase is currently in use by the RTCC to assist with criminal investigations and to provide actionable information to units in the field. SPD employees in the RTCC and Investigations Unit utilize the i2 Analyst's Notebook software and information stored in the i2 iBase system. It may also be used in compliance with the City of Seattle Intelligence Ordinance.

### 4.4 How often will the technology be in operation?

The software itself resides on a server that is operational 24/7. Users may access the data at any time, as part of criminal investigations.

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

The software is installed on a server and may be removed at any time. There is no physical installation aspect to this project.

**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?**

Data stored in the i2 iBase system is accessed by SPD employees assigned to the Real Time Crime Center and Investigations Unit. Access to the application requires SPD personnel to log in with password-protected login credentials which are granted to employees with business needs to access CAD. These employees are ACCESS and CJIS certified.

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

All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including:

- [SPD Policy 12.040](#) - Department-Owned Computers, Devices & Software,
- [SPD Policy 12.050](#) - Criminal Justice Information Systems,
- [SPD Policy 12.080](#) – Department Records Access, Inspection & Dissemination,
- [SPD Policy 12.110](#) – Use of Department E-mail & Internet Systems, and
- [SPD Policy 12.111](#) – Use of Cloud Storage Services.

Additionally, incidental data access may occur through delivery of technology client services. All ITD employees are required to comply with appropriate regulatory requirements regarding security and background review.

ITD client services interaction with SPD systems is governed according to the terms of the 2018 Management Control Agreement between ITD and SPD, which states that:

“Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBI’s Criminal Justice Information Services, (CJIS) Security Policy.”

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

No outside agency has direct access to the software.

I2 iBase is operated and used exclusively by SPD personnel. Seattle IT Department personnel have administrative access to the system for support services as outlined in 4.7. Use of the iBase system will be 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?**

I2 iBase is used by the RTCC to assist in ongoing criminal investigations and to provide actionable information to units in the field to increase officer safety, efficiency, and response to incidents. Data is only accessed as part of ongoing criminal investigations or under the City of Seattle Intelligence Ordinance.

#### **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.)?**

Only authorized SPD users can access the system, technology, or the data. Access to the application is limited to SPD personnel via password-protected login credentials. All user activity within the iBase system generates a log that is auditable.

Data is securely input and used on SPD's password-protected network with access limited to authorized users.

The entire system is located on the SPD network that is protect by industry standard firewalls. ITD performs routine monitoring of the SPD network.

The CAD system is CJIS compliant. More information on CJIS compliance may be found at the CJIS Security Policy website.

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.

SPD's Audit, Policy and Research Section (APRS) can conduct an audit of the 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.

ITD client services interaction with SPD systems is governed by the terms of the 2017 Management Control Agreement between ITD and SPD, which states that:

“Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBI's Criminal Justice Information Services, (CJIS) Security Policy.”

## 5.0 Data Storage, Retention and Deletion

### 5.1 How will data be securely stored?

All of the data in the iBase system are held in SPD/ITD servers, located on City premises on SPD networks. Access to these networks is as specified in 4.1. All data that goes to mobile clients are encrypted to FIP 140-2 standards and is therefore CJIS compliant.

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.

Network Diagrams - Network diagrams, i.e. topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the “big picture” – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest.”

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

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?

If improperly collected data is found during an audit log review (or through other means), it will be deleted from the server (includes a soft delete and purging of deleted records). The user responsible for the improper collection will be dealt with on a case-by-case basis, to include limiting their access to data or removal of their access to the system altogether.

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

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

All SPD employees must adhere to laws, City policy, and Department Policy ([SPD Policy 5.001](#)), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in [SPD Policy 5.002](#).

Per the CJIS Security Policy:

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

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

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

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



SPD's Intelligence and Analysis Section reviews the audit logs and ensures compliance with all regulations and requirements.

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?

No person, outside of SPD and Seattle IT, has direct access to the application or the data.

As Seattle IT supports the iBase system on behalf of SPD, a Management Control Agreement exists between SPD and Seattle IT. The agreement outlines the specifications for compliance, and enforcement related to supporting the iBase system through inter-departmental partnership. The MCA can be found in the appendices of this SIR.

Because all the data used in this project relates to criminal investigations, any information shared will follow standard policing practices and CJIS compliance.

### 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. For example, an investigator may send out a photo or description of a homicide suspect in order to find out if another LE agency knows their identity.

Products developed using this information may be shared with other law enforcement agencies. All products created with the information used in this project will be classified as Law Enforcement Sensitive. Any bulletins will be marked with the following restrictions: LAW ENFORCEMENT SENSITIVE — DO NOT LEAVE PRINTED COPIES UNATTENDED — DISPOSE OF IN SHREDDER ONLY — NOT FOR PUBLIC DISPLAY OR DISTRIBUTION — DO NOT FORWARD OR COPY.

### **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.**

All users with direct access to the data must have a Seattle Police Department network account. The software is not set up to allow any other agency to access the data.

### **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?**

No additional data sharing agreements have been established regarding the iBase system or the data it contains.

### **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 the data already available to investigators as part of their criminal investigations. The data collected in this database mirrors that in SPD's RMS/CAD, so no additional accuracy check is required for that data. All manually added information must include the source description, source reliability, and content certainty.

### **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?

IBM Security i2 iBase system is used during the investigation of crimes by the SPD Real Time Crime Center and information collected and stored in the system is related to these criminal investigations.

All use of the i2 iBase system must also comply with SPD Policy 12.050 – Criminal Justice Information Systems and may only be used for legitimate criminal investigative purposes.

Use of the iBase system 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 the iBase system and i2 Analyst's Notebook undergo training on the use of the software, which includes privacy training.

All authorized users of the iBase system 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.**

The nature of the Department’s mission will inevitably lead it to collect and maintain information many may believe to be private and potentially embarrassing. Minimizing privacy risks revolve around disclosure of personally identifiable information.

The primary privacy risk with this system pertains to Personally Identifiable Information (PII) being added on individuals not directly associated with criminal activity. To mitigate this risk, users only add PII on individuals associated with a criminal investigation and/or collected in accordance with the City of Seattle Intelligence Ordinance. In addition, SPD conducts regular reviews of audit logs to ensure proper use and retention of the data.

SMC 14.12 and SPD Policy 6.060 direct all SPD personnel that “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, officers must take care “when photographing demonstrations or other lawful political activities. If demonstrators are not acting unlawfully, police can’t photograph them.” iBase is not used to track demonstration participants and no demonstration-related images have been input into the iBase system.

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.

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 public may express concern over the consolidation of so much information about individuals, but all of the data that is included in the iBase system is already available to investigators in RMS/CAD and other legally accessible information repositories; this project simply works to make accessing and analyzing that information more efficient. Every individual in the database is related to a criminal investigation or part of an investigation under the City of Seattle Intelligence Ordinance. Under no circumstances will this project involve the collection of Personally Identifiable Information (PII) on people with no connection to criminal investigations or related to a Seattle Police response to an incident.

## 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 in iBase system 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 software's audit log tracks all log-ins/offers, data views, and data modifications. SPD periodically reviews these logs to ensure proper use of the software. In addition, the logs are available at any time for review by the Seattle Intelligence Ordinance Auditor.

SPD's Audit, Policy and Research Section is authorized to conduct audits of all investigative data collection software and systems. In addition, the Office of Inspector General and the federal monitor can conduct audits of the software, and its use, at any time. Audit data is available to the public via Public Records Request.

## 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
06/06/17	01/04/18	\$67,860	\$113,615	\$17,314	Federal Grant

Notes:

SPD has received a Department of Justice grant in order to build out the technology available to the RTCC.

#### 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
\$12,325	0	0	\$4,713.97	SPD Budget

Notes:

The primary ongoing cost of this project is the annual iBase licenses. Maintenance of the software and servers is handled by SPD and Seattle IT.

### **1.3 Cost savings potential through use of the technology**

Quantifying the cost savings through this technology is difficult as the primary purpose is to improve the department's effectiveness at reducing crime and improving public safety. While no formal study was done of the time previously wasted on manually re-entering information onto a chart, adding a single person's criminal history to a chart could take multiple days of work. With this software, a user can see a subject's criminal history in minutes. The man-hours saved on such tasks saves the department money, while also enhancing the department's overall understanding of crime within the City of Seattle.

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

Additional federal grants could be acquired to pay the continued licensing fees of the software.

## 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
Application of Link Analysis to Police Intelligence	<i>HUMAN FACTORS</i> Volume:17 Issue :2 Dated:(APRIL 1975) Pages:157-164	<a href="https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=45467">https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=45467</a>
Police Information Systems and Intelligence Systems	United Nations Office on Drugs and Crime	<a href="https://www.un.org/ruleoflaw/files/4_Police_Information_Intelligence_Systems.pdf">https://www.un.org/ruleoflaw/files/4_Police_Information_Intelligence_Systems.pdf</a>
Investigative Analysis in Law Enforcement	IBM Solution Brief	<a href="https://www.ibm.com/downloads/cas/OW3KJN1Y">https://www.ibm.com/downloads/cas/OW3KJN1Y</a>

# 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 personally identifiable information (PII) gathered during criminal investigations could be used to identify individuals who are associates of criminal suspects, such as their name, home address or contact information. Victims of criminal activity may also be identified during incident responses, whose identities should be protected in accordance with RCW 42.56.240 and RCW 70.02. SPD mitigates these risks by entering information into the iBase system only when it is related to the investigation of a crime and/or collected in accordance with the City of Seattle Intelligence Ordinance. In addition, SPD conducts regular reviews of audit logs to ensure proper use and retention of the data.

### 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 the iBase system, 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

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

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?**

IBM Security i2 iBase system is used during the investigation of crimes by the SPD Real Time Crime Center and information collected and stored in the system 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 the i2 iBase system must also comply with SPD Policy 12.050 – Criminal Justice Information Systems and may only be used for legitimate criminal investigative purposes.

Use of the iBase system 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.”<sup>1</sup> 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 stored within the iBase system 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 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.

## 2.0 Public Outreach

### 2.1 Scheduled public meeting(s).

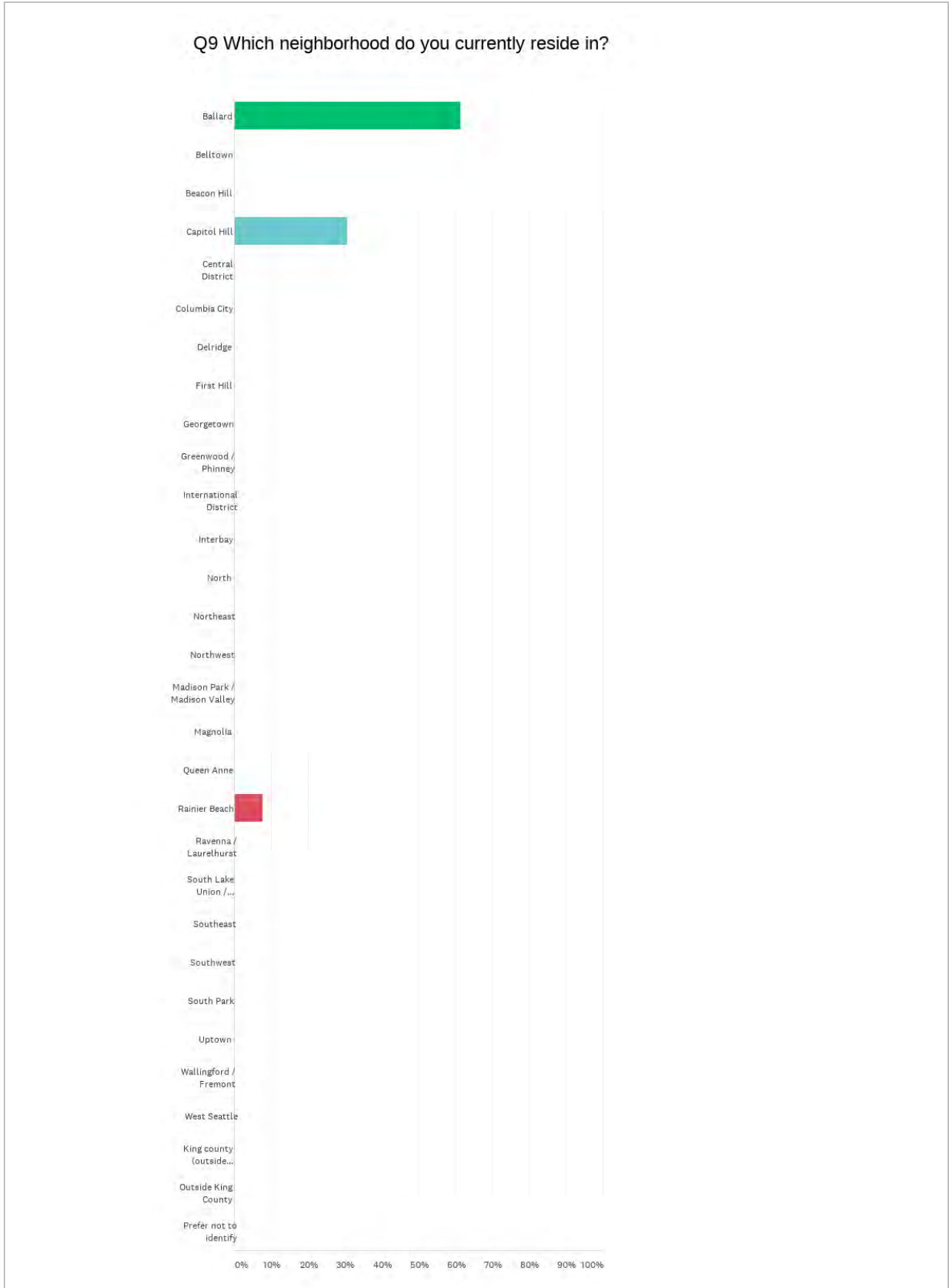
<b>Location</b>	Virtual Event
<b>Time</b>	Thursday, June 10 <sup>th</sup> , 12 PM

<b>Location</b>	Virtual Event
<b>Time</b>	Tuesday, June 29 <sup>th</sup> , 3 PM

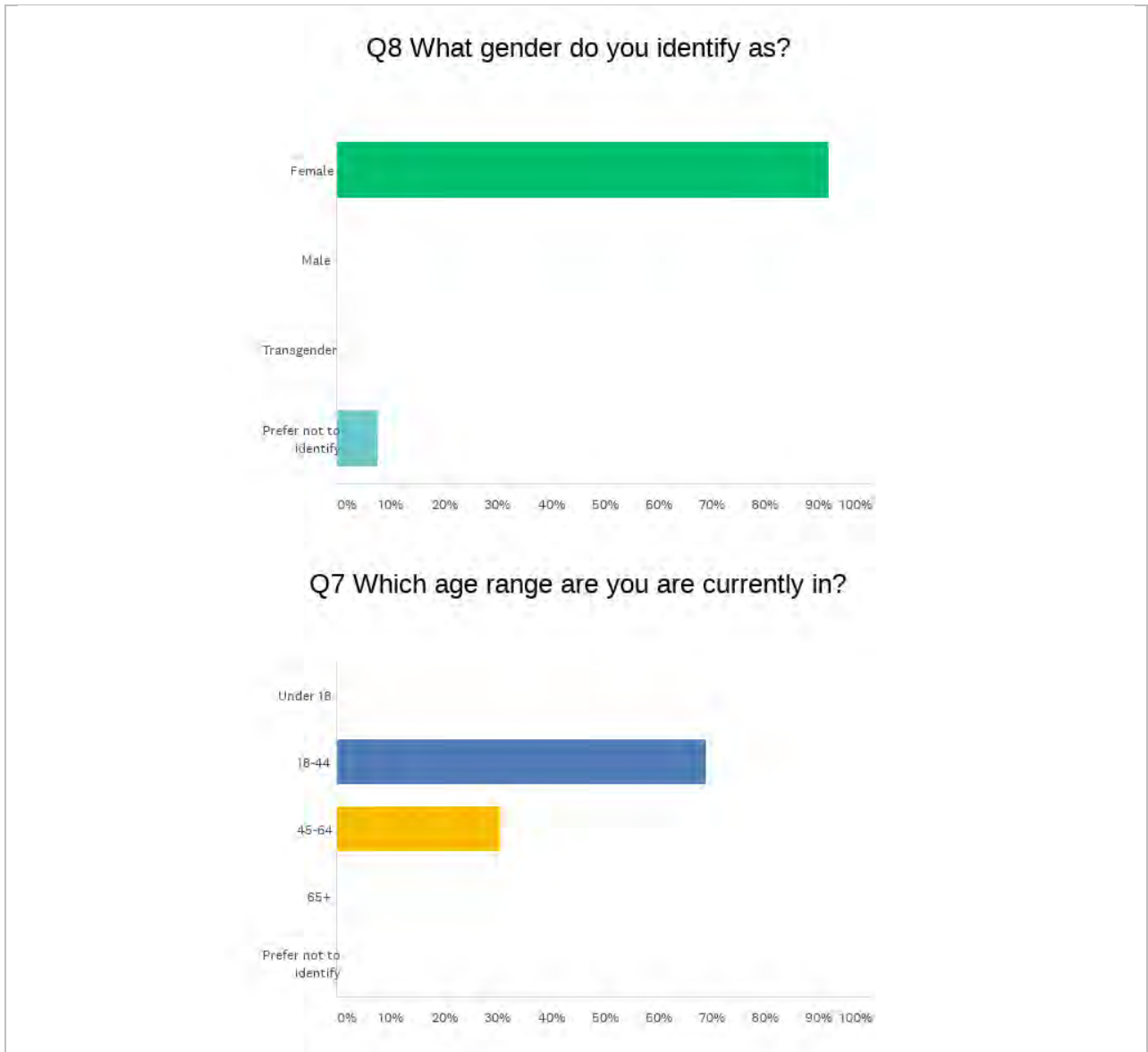
### **3.0 Public Comment Analysis**

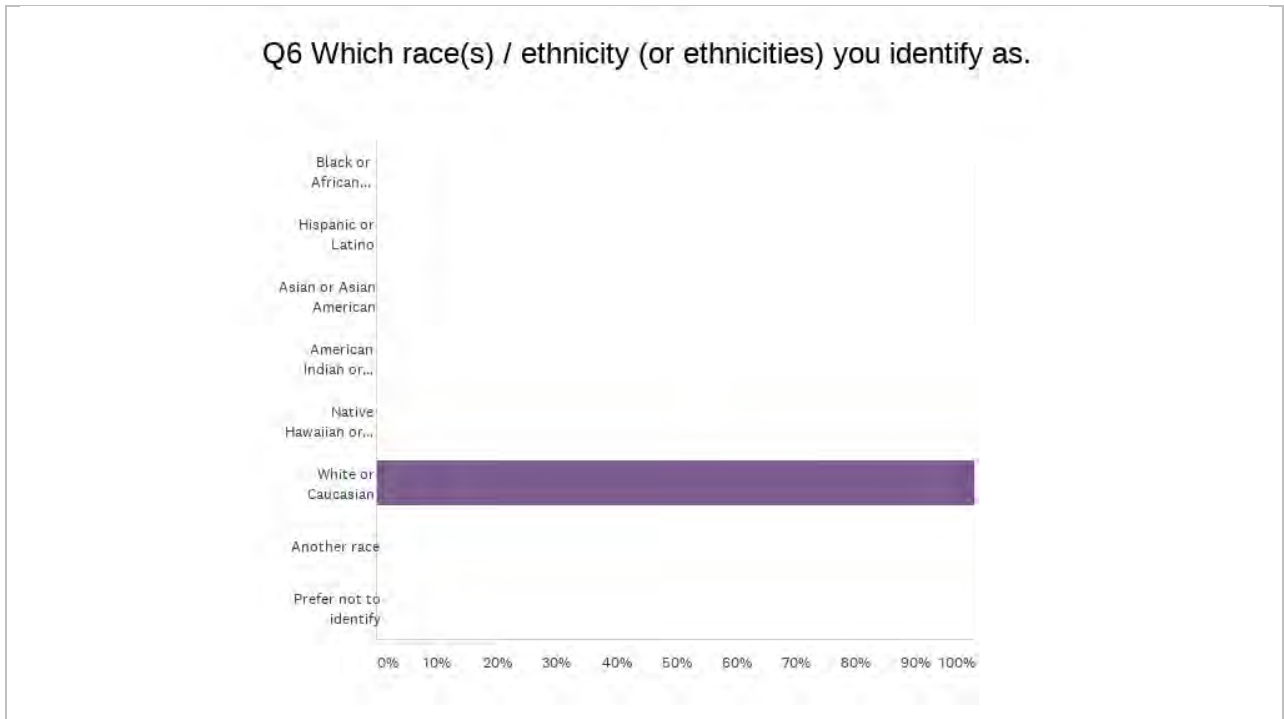
This section will be completed after the public comment period has been completed. Please note due to the volume of comments, analysis represents a summarization of all comments received. Technology specific comments will be included in Appendix C.

#### **3.1 Summary of Response Volume**









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

Q2 What concerns, if any, do you have about the use of this technology?

response question survey withholding information public comment open questions  
 RMS Mark43 opposed informed public comment Missing information due  
 hinder ability informed SPD using thus greatly hinder TESU public answered thus  
 incorporates numerous questions public regarding answers questions numerous since  
 dodged providing answers per year use Additionally SPD dodged  
 many incidents per engagement meetings Additionally SPD specified many  
 4a public engagement clarity regarding magnitude public Group 4a  
 data retention period allocated questions public incident types SPD  
 little time allocated CAD etc incident audio recordings defining limiting CAD  
 Lack transparency Thus concerns include use Maltego concerns will Thus whether  
 questions list concerns via answers open questions etc worst missing answers  
 used privacy-wise assume worst **Callyo apps**  
 approach security privacy-wise  
**audio recording devices** Since safest approach  
**data** survey Since safest **SPD** safest approach security **iBase**  
 security privacy-wise assume **Maltego** assume worst missing  
**Lack clarity regarding** missing answers open  
**use Callyo apps** open questions list access list concerns will installed  
 will Thus concerns apps policy defining limiting Maltego SIR limiting CAD etc  
 regarding whether etc incident types use iBase types SPD may  
 time allocated questions SPD RMS Mark43 questions public Group  
 regarding magnitude use Group 4a public specified many incidents  
 public engagement meetings incidents per year meetings Additionally SPD  
 Surveillance always concern SPD dodged providing Security  
 providing answers questions record questions numerous questions audio  
 questions public answered deployment answered thus greatly write access  
 greatly hinder ability One safely assume ability informed public SPD withholding information  
 public comment open recording devices use SPD use Maltego question survey Since

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

Q3 What value, if any, do you see in the use of this technology?

Remains seen value **None**

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

Q4 What do you want City leadership to consider about the use of this technology?

past history prior Callyo apps Require City leadership past stop funding tool tool Given City security requiring SPD recommend City leadership etc Require SPD problems fixed SPD may used fixed systemic problems version criminal system fixed considerations depend SPD support pipelines criminal TBD valid considerations community needs support update Callyo SIR tools money community per year use surveil residents SPD many incidents per use Maltego SPD disclose many record specific incident types audio recording devices Policy state specific report recent audit questions Require SPD provide date report Require SPD answer SPD publicly provide changes made Require Require SPD Policy changes superficial changes access limited cosmetic changes Require SPD update will pursue limited SPD answer public right instead will

**Require SPD disclose** suspect fundamentally right

**use** surveillance technologies suspect **data**

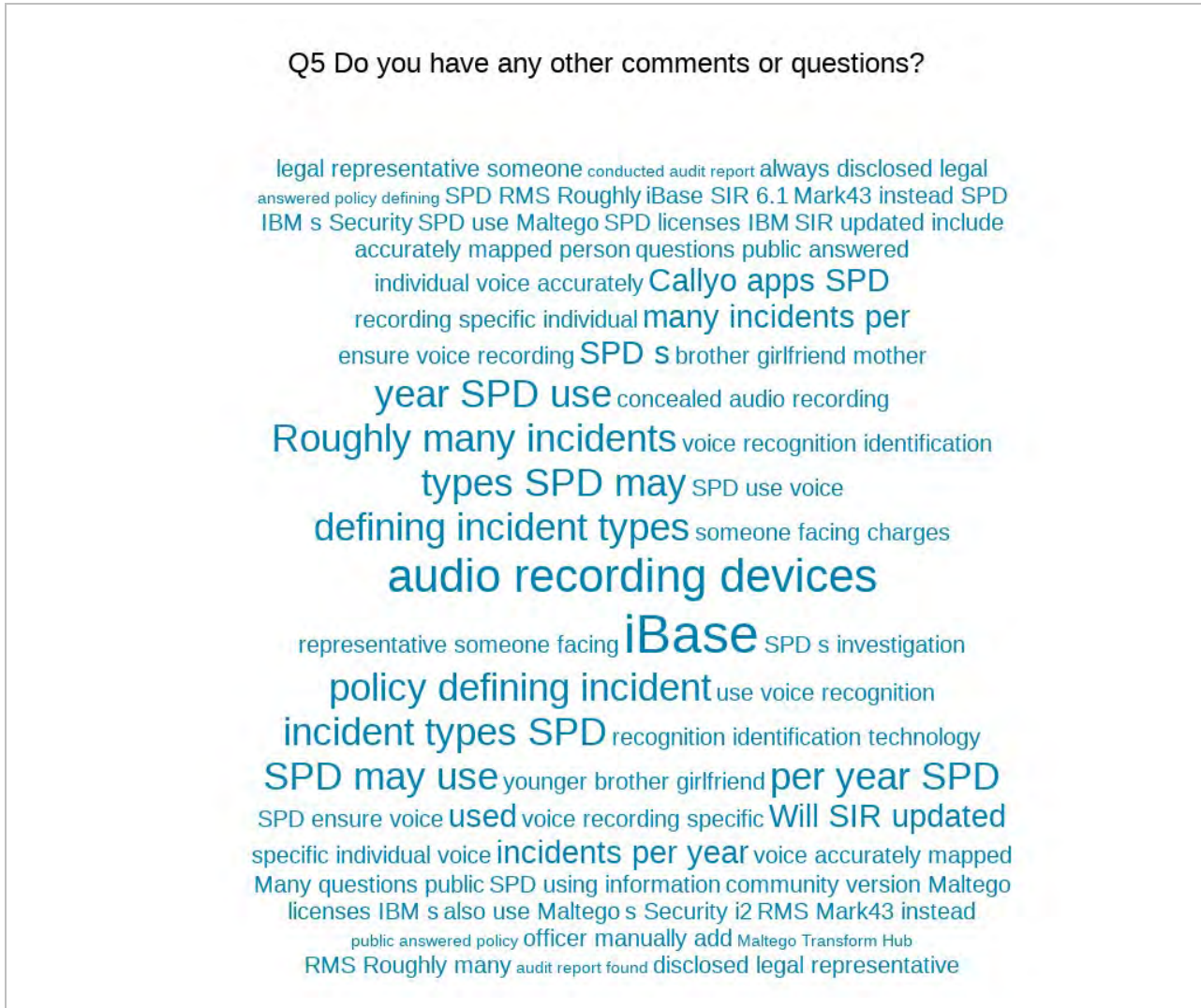
prior surveillance technologies **iBase** technologies suspect fundamentally

**Maltego** fundamentally right instead

**answer public questions** instead will pursue **Callyo apps** pursue limited cosmetic devices cosmetic changes superficial Require SPD publicly superficial changes made publicly provide date made Require SPD date report recent public questions Require recent audit SPD SPD Policy state systems state specific incident Ban Improve security requiring SPD surveil residents disclose many incidents need tools money incidents per year money community needs SPD update Callyo needs support pipelines apps Require SPD pipelines criminal system valid considerations depend system fixed systemic depend SPD answering systemic problems fixed audited tools recommend City audio recordings City leadership stop etc Improve security Given City leadership leadership stop funding leadership past history funding tool Given history prior surveillance

### 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 i2 iBase

### 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 i2 iBase 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 i2 iBase technology.

Our assessment of i2 iBase technology as used by Seattle Police Department (SPD) focuses on four major issues:

1. A regular audit is necessary to assess for biases, as i2 iBase's automated relationship analyses are likely to generate data errors that compound existing biases.
2. There must be a policy defining a specific and restricted purpose of use.
3. There must be clear and strong policies regarding data collection, retention, storage, and protection.
4. A prohibition on use of i2 iBase for predictive policing is necessary.

### Recommendations

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

1. The purpose and allowable uses of i2 iBase must be clearly defined, and any SPD use of i2 iBase must be limited to that specific purpose and those allowable uses. The specific incident types for which i2 iBase may be used must be clearly stated. The use limits must restrict when someone's relationship network may be assembled in i2 iBase, such as a requirement that a criminal investigation is opened before an analysis is begun, to prevent the widespread use of i2 iBase analysis on all individuals encountering the police.
2. There must be a requirement that SPD make publicly available the contract that governs SPD's use of i2 iBase if a contract or agreement exists.
3. SPD must publicly disclose all of its data sources, such as data brokers (e.g., LexisNexis, CoreLogic) and any use of non-public details from social media platforms (e.g., Facebook, Twitter).
4. SPD must not be permitted to share i2 iBase data with third parties.



5. There must be a regular audit to assess for biases in the data imported into i2 iBase and in the analyses generated by i2 iBase. There must be technical mechanisms in place to enable robust auditing to occur (e.g. detailed logs).
6. There must be limits on the kinds of data that may be inputted both manually and automatically into i2 iBase, ensuring that additional pools of public or private information are not added in the future.
7. There must be a shortened data retention period that does not exceed the time necessary to conduct a criminal investigation.
8. There must be a clear deletion oversight process to ensure that manually added data are deleted after the specified retention period.
9. There must be a requirement that limits employee access to i2 iBase records. For example, requiring that employee access is assigned per record in i2 iBase so that employees do not have access to records unrelated to a specific investigation to which they have been assigned.
10. There must be a manual relationships analysis process that includes clear checkpoints designed to ensure erroneous data and inaccurate linkages generated by i2 iBase are detected and corrected before they are actively investigated.
11. There must be limits on usage of potentially erroneous i2 iBase analyses and search data in rapid-response settings where manual analysis is not possible.
12. There must be a requirement for SPD to disclose for how many incidents per year they use i2 iBase.
13. There must be a requirement that the use of i2 iBase is always disclosed to the individual or the legal representative of an individual facing charges for which i2 iBase was used in an SPD investigation.
14. There must be a regulation prohibiting the use of i2 iBase for predictive policing.
15. There must be a contract with IBM that ensures IBM never possesses, uses, or accesses SPD data.

## Key Concerns

1. **i2 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." However, that claim conflicts with assertions that iBase's automated processing will "create[e] relevant intelligence from large amounts of data," and will create new "efficiencies" by avoiding manual data management. 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.

2. **There are inadequate policies defining purpose of use and use limitations.**
  - a. **Rapid Response Uses.** The SIR indicates that RTCC uses the social network analysis provided by i2 iBase to provide “actionable information” 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.
  - b. **Need for a Criminal Investigation.** The SIR does not specify at what point someone’s data is consolidated and viewed in i2 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 i2 iBase. Rather, anyone who is merely the subject of a 911 call might be analyzed using i2 iBase.
  - c. **Predictive Policing.** Without clearer usage limits, data compiled via i2 iBase might be used for predictive policing, which 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.
3. **It is unclear how data are stored and processed.** In the SIR, SPD does not specify what portion of existing data is automatically imported into i2 iBase, and what kinds of data have been manually inputted. The lack of information on data currently included or potentially included in i2 iBase raises numerous concerns.
  - a. **There are no limits on the types of data that may be imported.** The SIR indicates that additional data can be “manually imported” into the system and suggests that officers would manually input only single “piece[s] of data.” 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 i2 iBase’s potential to operate as a dragnet with a disparate surveillance impact.
  - b. **There is likely to be 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 i2 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 i2 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 i2 iBase generates, nor whether any policies exist which might mitigate this disparate impact.
4. **It is unclear whether SPD has a contract with IBM.** It is therefore difficult to assess what future uses of i2 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 i2 iBase via a one-way server transfer, the SIR does not describe enforceable provisions that could prevent future IBM use or review of data and analyses from i2 iBase.

**5. It is unclear what data security measures that would prevent third-party access to sensitive i2 iBase relationship analyses and searches.**

- a. **Data Deletion.** The SIR states that manually entered data will be automatically deleted after five years. 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.
- b. **Incidental Data Access.** The SIR specifies, “incidental data access may occur through delivery of technology client services.” 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 i2 iBase could be released to third-party entities.

### Outstanding Questions

- Which “portion” of SPD RMS and CAD data is automatically imported into i2 iBase? How often does the data use 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 i2 iBase in the future?
- How is manual relationship analysis performed using i2 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 i2 iBase or Analyst’s notebook, without verifying the accuracy of all the many data points involved?
- Is data compiled via i2 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 i2 iBase to provide “actionable information” 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 i2 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?
- What protections are in place to protect the privacy of individuals who are not part of an investigation but whose data may be captured?
- What are all of the i2 iBase suite products that SPD uses and does SPD use the premium version of any of those products?
- When was the last audit of i2 iBase?
- What specific security features of i2 iBase has SPD enabled or configured?
- How many or what percentage of SPD employees have access to i2 iBase?

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.

## CTO Response

# MEMO

**To:** Seattle City Council  
**From:** Jim Loter, Interim Chief Technology Officer  
**Subject:** CTO Response to the Surveillance Working Group i2 iBase 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 i2 iBase.

### 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

I2 iBase is the server backbone to the i2 Analysts Notebook application, a software system which organizes existing SPD data visually into more accessible information utilized by the SPD Real Time Crime Center (RTCC) employees. The purpose of the RTCC is to provide actionable information to units in the field to increase officer safety, efficiency, and response to incidents. It is also intended to be the information “hub” of the police department, utilizing its resources and collective knowledge to enhance the department's effectiveness at reducing crime and improving public safety. The iBase system combines data stored in SPD's Records Management System (RMS), CSCC's Computer Aided Dispatch (CAD) system, and information gathered during criminal investigations and displays information related to ongoing investigations. This type of link analysis software is similar to a virtual “link board” or “pin board”, helping investigators to visualize the connections between known entities, vehicles, locations, etc. in the course of a criminal investigation.

## 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 i2 iBase are addressed in the attached document.

## Response to Specific Concerns: i2 iBase

**Concern: i2 iBase’s automated relationship analyses are likely to generate data errors that compound existing biases**

SIR Response:

## Section 4.2

“All data entered into the iBase system is directly related to criminal investigations. Individual detectives and analysts may manually enter information not imported from the existing RMS and CAD data systems. Analysts use this software to build networks of individuals associated with criminal cases. All data changes are logged in the software’s audit log, which is reviewed periodically. In addition, when manually adding information, a user must provide the source description, source reliability, and content certainty; all manually added information is purged from the system after 5 years, in compliance with 28 CFR Part 23”

## Section 5.3

“If improperly collected data is found during an audit log review (or through other means), it will be deleted from the server (includes a soft delete and purging of deleted records). The user responsible for the improper collection will be dealt with on a case-by-case basis, to include limiting their access to data or removal of their access to the system altogether.

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

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

All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

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

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

**Concern: There are inadequate policies defining purpose of use and use limitations**



SIR Response:

### Section 3.1

“IBM Security i2 iBase system is only used during the investigation of crimes by the SPD Real Time Crime Center. Access for personnel into the system is predicated on state and federal law governing access to Criminal Justice Information Services (CJIS). This includes pre-access background information, appropriate role-based permissions as governed by the CJIS security policy, and audit of access and transaction logs within the system. All users of CAD must be CJIS certified and maintain Washington State ACCESS certification.

Each user must be directly granted an account (tied to their SPD network identity) in order to access the software. The 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.”

### Section 4.3

“IBM i2 iBase is currently in use by the RTCC to assist with criminal investigations and to provide actionable information to units in the field. SPD employees in the RTCC and Investigations Unit utilize the i2 Analyst’s Notebook software and information stored in the i2 iBase system. It may also be used in compliance with the City of Seattle Intelligence Ordinance”

**Concern: It is unclear how data are stored and processed.**

SIR Response:

### Section 4.1

“The only information pulled into iBase automatically comes from SPD’s Records Management System (RMS) and Computer Aided Dispatch (CAD) system. Users may manually add additional information that they have collected during the course of a criminal investigation. All manually added information is deleted after five years, in accordance with 28 CFR Part 23. No data outside SPD’s RMS/CAD (e.g. commercial data aggregators, publicly available data, or other city departments) is automatically collected.”

### Section 4.7

“Data stored in the i2 iBase system is accessed by SPD employees assigned to the Real Time Crime Center and Investigations Unit. Access to the application requires SPD personnel to log in with password-protected login credentials which are granted to employees with business needs to access CAD. These employees are ACCESS and CJIS certified.

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

All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including:

- SPD Policy 12.040 - Department-Owned Computers, Devices & Software,
- SPD Policy 12.050 - Criminal Justice Information Systems,
- SPD Policy 12.080 – Department Records Access, Inspection & Dissemination,
- SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and
- SPD Policy 12.111 – Use of Cloud Storage Services.

Additionally, incidental data access may occur through delivery of technology client services. All ITD employees are required to comply with appropriate regulatory requirements regarding security and background review.

ITD client services interaction with SPD systems is governed according to the terms of the 2018 Management Control Agreement between ITD and SPD, which states that: “Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBI’s Criminal Justice Information Services, (CJIS) Security Policy.””

#### Section 5.1

“All of the data in the iBase system are held in SPD/ITD servers, located on City premises on SPD networks. Access to these networks is as specified in 4.1. All data that goes to mobile clients are encrypted to FIP 140-2 standards and is therefore CJIS compliant.

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.

Network Diagrams - Network diagrams, i.e. topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the “big picture” – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest.”

#### **Concern: It is unclear whether SPD has a contract with IBM**

This concern is not addressed in the SIR.

#### **Concern: It is unclear what data security measures that would prevent third-party access to sensitive i2 iBase relationship analyses and searches.**

CTO Assessment: The information contained within the system are held to security best practices and are CJIS compliant.

SIR Response:  
Section 4.10

“Only authorized SPD users can access the system, technology, or the data. Access to the application is limited to SPD personnel via password-protected login credentials. All user activity within the iBase system generates a log that is auditable.

Data is securely input and used on SPD’s password-protected network with access limited to authorized users.

The entire system is located on the SPD network that is protect by industry standard firewalls. ITD performs routine monitoring of the SPD network.

The CAD system is CJIS compliant. More information on CJIS compliance may be found at the CJIS Security Policy website.

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.

SPD’s Audit, Policy and Research Section (APRS) can conduct an audit of the 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.

ITD client services interaction with SPD systems is governed by the terms of the 2017 Management Control Agreement between ITD and SPD, which states that: “Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBI’s Criminal Justice Information Services, (CJIS) Security Policy.”

### Section 5.1

“All of the data in the iBase system are held in SPD/ITD servers, located on City premises on SPD networks. Access to these networks is as specified in 4.1. All data that goes to mobile clients are encrypted to FIP 140-2 standards and is therefore CJIS compliant.

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.

Network Diagrams - Network diagrams, i.e. topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the “big picture” – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest.”

### Section 5.3

If improperly collected data is found during an audit log review (or through other means), it will be deleted from the server (includes a soft delete and purging of deleted records). The user responsible for the improper collection will be dealt with on a case-by-case basis, to include limiting their access to data or removal of their access to the system altogether. SPD policy contains multiple provisions to avoid improperly collecting data. SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a GO Report. SPD Policy 7.090 specifically governs the collection and submission of photographic evidence. Evidence is submitted to the Evidence Unit and associated with a specific GO Number and investigation. And, SPD Policy 7.110 governs the collection and submission of audio recorded statements. It requires that officers state their name, the Department name, the General Offense number, date and time of recording, the name of the interviewee, and all persons present at the beginning of the recording. Additionally, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures. All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002. Per the CJIS Security Policy: “5.8.3 Digital Media Sanitization and Disposal The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. 5.8.4 Disposal of Physical Media Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.”

## Section 6.1

“No person, outside of SPD and Seattle IT, has direct access to the application or the data.

As Seattle IT supports the iBase system on behalf of SPD, a Management Control Agreement exists between SPD and Seattle IT. The agreement outlines the specifications for compliance, and enforcement related to supporting the iBase system through inter-departmental partnership. The MCA can be found in the appendices of this SIR.

Because all the data used in this project relates to criminal investigations, any information shared will follow standard policing practices and CJIS compliance.”

## 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 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 items    [Home](#)    [About](#)    [Help](#)    [Privacy](#)    [Contact](#)

[<< Previous](#)

[Next >>](#)

## **Appendix C: All Comments Received from Members of the Public**

**ID:** 12841230225

**Submitted Through:** Online Comment

**Date:** 7/23/2021 3:55:46 PM

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

SPD: i2 iBase

**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 iBase 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 i2 iBase. (2) SPD has not been transparent with the public regarding the data sources to SPD's iBase system. (3) The potential incorporation of information from data brokers (i.e. Corelogic, LexisNexis, Experian, etc) into SPD's iBase system. (4) The potential incorporation of information gleaned via SPD officer's using their own "sock puppet" accounts on social media platforms (Facebook, etc). (5) Excessive SPD RMS data pulled into SPD'S iBase (such as the entirety/majority of the SPD RMS (Mark43) as opposed to only "surgically" pulling in case-by-case data from the RMS about specific incidents). (6) SPD is likely using iBase to conduct dragnet surveillance of Seattle residents by analyzing their geolocation history/patterns via incorporating SPD's Automated License Plate Reader (ALPR) data into iBase. (7) Weaken security by the likely lack of Security Classification Codes (SCC) per each item in a record in iBase. (8) Unvalidated and excessive external data incorporated into SPD's iBase via IBM Security i2 Connect, IBM i2 Enterprise Insight Analysis, and/or the Premium version of IBM i2 Analyst's Notebook. (9) Inaccurate/incomplete iBase SIR since SPD did not provide complete information regarding their data sharing partners. In iBase SIR item 6.1, SPD did not answer regarding who they indirectly share data with. Given SPD provided an answer as to why data sharing is justified (SIR item 6.2), it can only be safely assumed that SPD has withheld information from the public regarding who they indirectly share iBase data with. (10) Missing information due to SPD not specifying in the SIR the data retention period for data inside iBase. One can again only safely assume that the data retention period is excessive, otherwise why hide it. (11) No safeguards in place to prevent or quickly remedy the retention of data in iBase of individuals who are not suspects nor found guilty of a crime (i.e. a suspect's younger brother, or girlfriend, or mother). Nothing prevents SPD from using iBase on innocent members of the public. Nothing ensures that data collected accidentally on innocent individuals is deleted in a timely manner. (12) Potential security weakness due to iBase having write access to the SPD RMS. Thus if SPD's iBase system is compromised, an attacker could leverage this inappropriate scoping in the access control to modify, create, or delete arbitrary records in the SPD RMS (Mark43). (13) Too many employees with access to the system. There may also be an additional security weakness via rotting of the access control list, if employees who change teams are not promptly revoked access and/or if terminated employee accounts continue to persist post-termination. (14) Lack of transparency by SPD to the public regarding what contract language governs SPD's use of iBase. (15) Nothing prevents an SPD employee from accessing the data of an investigation they are not involved in. That is, it assumes that the access granted to iBase is all-or-nothing (not granular access control). Thus, nothing would prevent an SPD employee who is assisting in investigation A from seeing the details of unrelated investigation B in iBase (i.e. arson vs kidnapping vs stolen car, etc)? (16) Potential lack of a sufficient audit trail due to too low of an audit log level setting. (17) Lack of clarity from SPD in the iBase SIR items 5.2 &

8.2 regarding who fills the role of the "Seattle Intelligence Ordinance Auditor". This is especially unclear given multiple rolls/teams inside Seattle and federally can conduct audits of certain aspects of SPD (and in some cases overlapping role powers regarding who can audit what). (18) SPD did not disclose to the public when the last audit of iBase was conducted or where such an audit report might be found. (19) Lack of clarity regarding the magnitude of the use of iBase by SPD. SPD has not specified how many incidents per year they use iBase for. (20) Lack of clarity regarding if the use of iBase is always disclosed to the legal representative of someone facing charges for which iBase was used in SPD's investigation. (21) Finally (and most importantly) it's concerning that SPD has yet another tool to 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.

**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?**

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 funding 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 iBase may be used. (3) Require SPD to disclose all of their data sources to iBase (such as, any data brokers: Corelogic, LexisNexis, Experian, etc.; use of any non-public details from social media platforms: Facebook, Twitter, etc). (4) Require SPD to disclose if any data they add to iBase has been attained via deception (such as via the use of sock puppet accounts). (5) Require SPD to only "surgically" pull in data to iBase from their RMS (Mark43) on a case-by-case basis about specific incidents. (6) Ban the incorporation of Automated License Plate Reader (ALPR) data into iBase (such as via IBM's iBase Plate Analysis). (7) Require SPD use Security Classification Codes (SCC) per each item in a record in iBase. (8) Due to the unvalidated and excessive external data potentially incorporated into SPD's iBase via these 3 tools, City Leadership should disallow SPD use of: IBM Security i2 Connect, IBM i2 Enterprise Insight Analysis, and/or the Premium version of IBM's i2 Analyst's Notebook. (9) Disallow SPD from indirectly sharing data from iBase. (10) Require that data that is part of an investigation be retained in iBase for at most until the investigation is closed (if not deleted sooner). (11) Ban SPD from retaining in iBase the data of individuals who are not suspects nor found guilty of a crime (i.e. a suspect's younger brother, girlfriend, mother, neighbor, or a stranger like a shopkeeper, etc). (12) Improve security by requiring that SPD's iBase system only has read access (no write access - cannot create/delete/modify records) to the SPD RMS (Mark43). (13) Reduce the number of employees with access to iBase. (14) Improve security by requiring that access to iBase is promptly revoked for employees that change teams or when they no longer work for the City. (15) Require that SPD post publicly the contract that governs their use of IBM i2 iBase. (16) Require that employee access is assigned per record in iBase (that is, prevent an SPD employee who is assisting in investigation A from seeing the details of unrelated investigation B in SPD's iBase, i.e. arson vs kidnapping vs stolen car, etc). (17) Require that the audit log level of SPD's iBase system is set to level '5' (and that sufficient disk space is allocated for the records). This would allow those auditing the system to review all access to the system and look for anomalies [see: <https://www.ibm.com/docs/en/i2-ibase/9.0.3?topic=database-controlling-what-is-audited> ] (18) Require SPD to update iBase SIR items 5.2 & 8.2 to clarify who can/does fill the roll of the "Seattle Intelligence Ordinance Auditor" (19) Require SPD to publicly provide the date and report from the most recent audit of SPD's iBase. (20) Require SPD to disclose how many incidents per year they use iBase for. (21) Require that the use of iBase is always disclosed to the legal representative of someone facing charges for which iBase 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 iBase? (2) What are all of SPD's data sources to iBase - specifically what are the data sources meant by the wording in the SIR "information gathered during criminal investigation"? (3) Is SPD using information from data brokers (i.e. Corelogic, LexisNexis, Experian, etc)? (4) Is SPD using information found via officers' Facebook (or other social media) profiles? (5) Does all data in the SPD RMS get automatically imported into iBase? If not, what segments of RMS data are auto-imported to iBase? (6) Does SPD have licenses for iBase Plate Analysis? (7) Does SPD use Security Classification Codes (SCC) per each item in a record in iBase? (8) Is SPD's licenses for i2 Analyst's Notebook the basic version or the Premium version, which includes "i2 Analyze"? (9) Does SPD have licenses for IBM's "Security i2 Connect"? (10) Does SPD have licenses for IBM's "Security i2 Enterprise Insight Analysis"? (11) The iBase SIR 6.1 asks which entities are data sharing partners. SPD only answered regarding who has direct access. Which entities (if any) does SPD share iBase data with indirectly? If there are entities that SPD indirectly shares iBase data with, then will iBase SIR 6.1 and 6.3.1 be updated to accurately reflect that? If there is no indirect iBase data sharing, then why did SPD provide a supposed data sharing justification in iBase SIR 6.2? (12) How long is data retained in iBase? (13) What (if anything) prevents the retention of data in iBase of individuals who are not suspects nor found guilty of a crime (i.e. a suspect's younger brother, or girlfriend, or mother)? What ensures their information is deleted from iBase in a timely manner? (14) Does iBase have write access to the SPD RMS (i.e. can it create/delete/edit records in the RMS)? (15) How many employees are in the RTCC? How many employees are in the Investigations Unit? How many employees from IT have access to iBase? (16) Is SPD directly contracted with IBM or is there a third-party contracted company involved in provisioning/managing iBase? (17) Say an SPD employee is assisting in investigation A. What (if anything) prevents them from seeing the details of unrelated investigation B in iBase (i.e. arson vs kidnapping vs stolen car, etc)? (18) What is SPD's iBase audit log level set to? [Levels 1-5: <https://www.ibm.com/docs/en/i2-ibase/9.0.3?topic=database-controlling-what-is-audited>] (19) Who fills the role of "Seattle Intelligence Ordinance Auditor" (from items 5.2 & 8.2 in the iBase SIR)?...OIG? (20) When was the last audit of iBase conducted? (21) Roughly how many incidents per year does SPD use iBase for? (22) Is the use of iBase always disclosed to the legal representative of someone facing charges for which iBase was used in SPD's investigation?

---



**ID:** 12746737080

**Submitted Through:** Online Comment

**Date:** 6/15/2021 6:44:20 PM

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

SPD: i2 iBase

**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 iBase? 2) What are all of SPD's data sources to iBase - specifically what are the data sources meant by the wording in the SIR "information gathered during criminal investigation"? 3) Is SPD using information from data brokers (i.e. Corelogic, LexisNexis, Experian, etc)? 4) Is SPD using information found via officers' Facebook (or other social media) profiles? 5) Does all data in the SPD RMS get automatically imported into iBase? If not, what segments of RMS data are auto-imported to iBase? 6) Does SPD have licenses for iBase Plate Analysis? 7) Does SPD use Security Classification Codes (SCC) per each item in a record in iBase? 8) Is SPD's licenses for i2 Analyst's Notebook the basic version or the Premium version, which includes "i2 Analyze"? 9) Does SPD have licenses for IBM's "Security i2 Connect"? 10) Does SPD have licenses for IBM's "Security i2 Enterprise Insight Analysis"? 11) The iBase SIR 6.1 asks which entities are data sharing partners. SPD only answered regarding who has direct access. Which entities (if any) does SPD share iBase data with indirectly? If there are entities that SPD indirectly shares iBase data with, then will iBase SIR 6.1 and 6.3.1 be updated to accurately reflect that? If there is no indirect iBase data sharing, then why did SPD provide a supposed data sharing justification in iBase SIR 6.2? 12) How long is data retained in iBase? 13) What (if anything) prevents the retention of data in iBase of individuals who are not suspects nor found guilty of a crime (i.e. a suspect's younger brother, or girlfriend, or mother)? What ensures their information is deleted from iBase in a timely manner? 14) Does iBase have write access to the SPD RMS (i.e. can it create/delete/edit records in the RMS)? 15) How many employees are in the RTCC? How many employees are in the Investigations Unit? How many employees from IT have access to iBase? 16) Is SPD directly contracted with IBM or is there a third-party contracted company involved in provisioning/managing iBase? 17) Say an SPD employee is assisting in investigation A. What (if anything) prevents them from seeing the details of unrelated investigation B in iBase (i.e. arson vs kidnapping vs stolen car, etc)? 18) What is SPD's iBase audit log level set to? [Levels 1-5: <https://www.ibm.com/docs/en/i2-ibase/9.0.3?topic=database-controlling-what-is-audited>] 19) Who fills the roll of "Seattle Intelligence Ordinance Auditor" (from 3.1 in the iBase SIR)?...OIG? 20) When was the last audit of iBase conducted? Where can that audit report be found? 21) Roughly how many incidents per year does SPD use iBase for? 22) Is the use of iBase always disclosed to the legal representative of someone facing charges for which iBase was used in SPD's investigation?

---

**ID:** 12698224918

**Submitted Through:** Online Comment

**Date:** 5/28/2021 2:24:35 PM

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

SPD: i2 iBase

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

Bias. AI may seem unbiased, but it is not. The training sets are based on historically biased data furthering the 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?**

There is way too much bias in the police. Let's not aggravate it even more under the guise of impartial data.

**Do you have any other comments or questions?**

---

## **Appendix D: Letters from Organizations or Commissions**

July 23, 2021

Seattle Information Technology  
700 5<sup>th</sup> 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.

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 contain inaccuracies and built-in race and gender biases.<sup>1</sup> Such audio could be later input into a voice recognition or biometrics database, which may further enable both corporate and government surveillance.<sup>2</sup>

---

<sup>1</sup> 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>.

<sup>2</sup> 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/interpol-s-new-automated-platform-will-recognize-criminals-by-their-voice>.



P.O. Box 2728  
Seattle, WA 98111-2728  
(206) 624-2184  
[aclu-wa.org](http://aclu-wa.org)

Michele Storms  
*Executive Director*

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,<sup>3</sup> the Surveillance Impact Report (SIR) states that Callyo is used to GPS locate individuals.<sup>4</sup> 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.<sup>5</sup> 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.<sup>6</sup> Elsewhere, the SIR states that Callyo's call recording functions may only be used with a search warrant.<sup>7</sup> However, the city's webpage states, "Callyo may be used with consent or search warrant."<sup>8</sup> Comments at the June 10<sup>th</sup> and July 20<sup>th</sup> 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

<sup>3</sup> "Speaker Identification" *GoViva.com*, Accessed June 10, 2021, <https://www.goviva.com/products/speaker-identification/>; "Voice Authentication," *Awars Biometrics*, Accessed June 10, 2021, <https://www.awars.com/voice-authentication/>; "Forensic Voice Analysis," *Sestek.com*, Accessed June 10, 2021, <https://www.sestek.com/forensic-voice-analysis/>; "Voice Inspector for Forensic Experts," *Phonocia.com*, Accessed June 10, 2021, <https://www.phonocia.com/en/use-case/au/fo-forensic-software/>.

<sup>4</sup> 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=10FVHt2oyv8>.

<sup>5</sup> Seattle Police Department, "2021 Surveillance Impact Report: Callyo," Accessed June 7, 2021, <https://www.seattle.gov/Documents/Departments/Tech/Privacy/Public%20Engagement%20SIR%200%20Callyo.pdf>, 5-7.

<sup>6</sup> "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/>.

<sup>7</sup> SPD, "Callyo," 5.

<sup>8</sup> *Ibid.*, 7, 10, and 11.

<sup>9</sup> "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.<sup>9</sup> 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,<sup>10</sup> despite HRVU's larger share of the annual Callyo budget.<sup>11</sup> 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,"<sup>12</sup> 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.<sup>13</sup> 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.<sup>14</sup> When asked about possible Motorola collection of Callyo data during the July 20<sup>th</sup> 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

<sup>9</sup> SPD, "Callyo," 10, 11, 13, and 17.

<sup>10</sup> *Ibid.*, 7-11.

<sup>11</sup> *Ibid.*, 18.

<sup>12</sup> *Ibid.*, 14.

<sup>13</sup> "Investigative Solutions," *Callyo.com*, Accessed June 16, 2021, <https://callyo.com/investigations/investigative-solutions>.

<sup>14</sup> "Callyo," *Amazon Web Services*,

<https://partners.amazonaws.com/partners/0010f1d00001pBHaCQA/W/Callyo>; "10-21 Video" *Callyo.com*, Accessed June 7, 2021, <https://callyo.com/public-safety/10-21-video>.

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.<sup>15</sup> 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.<sup>16</sup> 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.<sup>17</sup> 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.<sup>18</sup> 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 its surveillance capabilities more forceful.<sup>19</sup> Callyo also includes numerous additional surveillance features, such as video recording and live-streaming<sup>20</sup> and “10-

<sup>15</sup> SPD, “Callyo,” 14-16.

<sup>16</sup> *Ibid.*, 7 and 10.

<sup>17</sup> See “Supervisors and commanding officers are responsible for ensuring compliance with policies,” at SPD, “Callyo,” 9.

<sup>18</sup> “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-1p2PRKAl5Tmm0y37/>.

<sup>19</sup> 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/>.

<sup>20</sup> “Police Body Camera App,” *10-21 Video.com*, Accessed June 16, 2021, <https://10-21.com/>; “10-21 Video,” *Callyo.com*.



21 Flight,<sup>21</sup> which allows officers to perform surveillance using drones.<sup>21</sup> 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.<sup>22</sup> Flight-based video tools can be and have been<sup>23</sup> 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:

<sup>21</sup> "10-21 Flight," *Callyo.com*, Accessed June 7, 2021, <https://callyo.com/public-safety/10-21-flight>.

<sup>22</sup> 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/>.

<sup>23</sup> "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.<sup>24</sup> SPD uses i2 iBase in partnership with a second IBM application, i2 Analyst's Notebook,<sup>25</sup> 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."<sup>26</sup> 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.<sup>27</sup>

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

<sup>24</sup> "IBM Security i2 iBase: FAQs," *IBM.com*, Accessed June 10, 2021, <https://www.ibm.com/products/i2-ibase>.

<sup>25</sup> 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-%20i2%20iBase-IBM%20%20i2%20iBase.pdf>.

<sup>26</sup> "IBM Security i2 Analyst's Notebook," *IBM.com*, Accessed June 10, 2021, <https://www.ibm.com/products/i2-analysts-notebook>.

<sup>27</sup> "IBM Security i2 iBase: Details," *IBM.com*, Accessed July 23, 2021, <https://www.ibm.com/products/i2-ibase>.

Connected Network<sup>27</sup> tool, which identifies a network that “directly or indirectly” connects several entities of interest.<sup>28</sup>

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.<sup>29</sup> The RTCC is a “centralized data and logistics hubs” that allows analysts to provide data to officers on the street.<sup>30</sup> Second, investigating officers use iBase to collect and organize timeline and relationship data for cases in progress.<sup>31</sup>

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.<sup>32</sup> 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.”<sup>33</sup> 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.<sup>34</sup> The SIR does not describe any SPD policy that would prevent additional data from being added to iBase. During the July 20<sup>th</sup> 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.<sup>35</sup> 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

<sup>28</sup> “IBM Security i2 Analyst’s Notebook: Feature Spotlights,” IBM.com, Accessed June 10, 2021, <https://www.ibm.com/products/i2-analysts-notebook/details>.

<sup>29</sup> SPD, “IBM i2 iBase,” 5.

<sup>30</sup> 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/>.

<sup>31</sup> SPD, “i2 iBase,” 5-6.

<sup>32</sup> “Digital Dragnet: How Data Became a Cop’s Best Weapon,” *GCM*, November 29, 2011, <https://gcn.com/Articles/2011/12/05/Predictive-policing-tech-feature.aspx?Page=2>.

<sup>33</sup> “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/>.

<sup>34</sup> “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/>.

<sup>35</sup> Timothy Crocker, “The Power of Social Network Analysis,” *Police Chief Magazine*, Accessed June 11, 2021, <https://www.policechiefmagazine.org/power-social-network-analysis/>.

Indigenous<sup>36</sup> – 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).<sup>37</sup> SNA is a problematic mode of analysis, in part because it is often used for predictive policing via “heat-mapping.” iBase advertises such features.<sup>38</sup> 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.<sup>39</sup>

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<sup>40</sup> – 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

<sup>36</sup> 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.oia.nim.nih.gov/pmc/articles/PMC3868476/>;

<sup>37</sup> SPD “IBM i2 iBase,” 6.

<sup>38</sup> “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>.

<sup>39</sup> 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-a-new-crime-analytics-program-threatens-perpetuate-racism-policing>.

<sup>40</sup> Andrew Papachristos and Michael Sierra-Arevalo, “Policing the Connected World,” *Department of Justice: Community Oriented Policing Services*, 2018, <https://www.hsdj.org/view/8d1d-014313>; Reichart, et al. “Focused Deterrence: A Policing Strategy to Combat Gun Violence,” *ICJLA Research Hub*, Accessed July 23, 2021, <https://icjla.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."<sup>41</sup> However, that claim conflicts with assertions that iBase's automated processing will "create[e] relevant intelligence from large amounts of data,"<sup>42</sup> and will create new "efficiencies" by avoiding manual data management.<sup>43</sup> 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"<sup>44</sup> 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.

---

<sup>41</sup> SPD, "IBM i2 iBase," 27.

<sup>42</sup> *Ibid.*, 7.

<sup>43</sup> *Ibid.*, 6, 21, and 27.

<sup>44</sup> *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.<sup>45</sup> 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<sup>46</sup> and suggests that officers would manually input only single “piece[s] of data.”<sup>47</sup> 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.

---

<sup>45</sup> Ibid., 7.

<sup>46</sup> Ibid.

<sup>47</sup> Ibid., 6.

- i. **Data Deletion.** The SIR states that manually entered data will be automatically deleted after five years.<sup>48</sup> 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.”<sup>49</sup> 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”<sup>50</sup> 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?

---

<sup>48</sup> Ibid., 10.

<sup>49</sup> Ibid., 11.

<sup>50</sup> 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.<sup>51</sup> The SIR does not specify the particular audio recording technology

---

<sup>51</sup> Seattle Police Department, “2021 Surveillance Impact Report: Audio Recording Systems (“Wires”),” accessed June 4, 2021, <https://www.seattle.gov/Departments/Departments/Tech/Privacy/Transparency/2021Engagement/2021SIR/01-30-Audio%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.<sup>32</sup> Although the SIR is unclear about the type or model of devices used, at the July 20<sup>th</sup> 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.<sup>33</sup> 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.<sup>34</sup> 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.<sup>35</sup> 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.

<sup>32</sup> Ibid., 6.

<sup>33</sup> Wendy Ridenman, “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-privacy-protection.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>.

<sup>34</sup> 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/interpol-new-automated-platform-will-recognize-criminals-by-their-voice>; “Speaker Identification” *GoVoice.com*, Accessed June 10, 2021, <https://www.govoice.com/products/speaker-identification/>; “Voice Authentication,” *Awave Biometrics*, Accessed June 10, 2021, <https://www.awave.com/voice-authentication/>; “Forensic Voice Analysis,” *Sivtek.com*, Accessed June 10, 2021, <https://www.sivtek.com/forensic-voice-analysis/>; “Voice Inspector for Forensic Experts,” *Phonoxia.com*, Accessed June 10, 2021, <https://www.phonoxia.com/en/use-cases/audio-forensics-software/>.

<sup>35</sup> SPD, “Audio Recording Systems (“Wires”),”<sup>12</sup>.

## 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.”<sup>56</sup> 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.<sup>57</sup> However, neither the SIR nor the June 10<sup>th</sup> or July 20<sup>th</sup> 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.

---

<sup>56</sup> Ibid., 4.

<sup>57</sup> Ibid.

- d. **Lack of Clarity on Types of Devices Used.** The SIR does not specify the manufacturer or function of devices used.<sup>58</sup> 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."<sup>59</sup> 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,<sup>60</sup> but also that the investigating officer is responsible for the purge.<sup>61</sup> 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 4<sup>th</sup> amendment rights and Washington consent laws.
- g. **Security Risks Associated with Third Party Data Sharing.** The SIR describes third-party data sharing only vaguely.<sup>62</sup> 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<sup>63</sup> but elsewhere states that TESU does so.<sup>64</sup> 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.

---

<sup>58</sup> Ibid., 5 and 16.

<sup>59</sup> Ibid., 8.

<sup>60</sup> Ibid., 6.

<sup>61</sup> Ibid., 11.

<sup>62</sup> Ibid., 12.

<sup>63</sup> Ibid., 10.

<sup>64</sup> 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.

- 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.”<sup>65</sup> There are multiple versions of Maltego that include different functions and data packages.<sup>66</sup> SPD states that they use the free, community version to assess information which is already publicly available online, primarily in the course of cybercrime investigations.<sup>67</sup>

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

<sup>65</sup> “Law Enforcement,” *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/law-enforcement/>.

<sup>66</sup> “Pricing,” *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/pricing-plans/>.

<sup>67</sup> “Products,” *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/products/>.

<sup>68</sup> Seattle Police Department, 2021 Surveillance Impact Report: Link Analysis Software - Maltego,” Accessed June 4, 2021,

<https://www.seattle.gov/Documents/Departments/Tech/Privacy/Public/620Engagement%20SIF-%20in%20Analysis-Maltego.pdf>, 5 and 11.

<sup>69</sup> “The Five Pillars of the Maltego Officer,” *Maltego.com*, Accessed June 4, 2021, <https://www.maltego.com/blog/the-five-pillars-of-the-maltego-officer/>.

<sup>70</sup> “Transform Hub,” *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/transform-hub/>.

<sup>71</sup> “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>.

<sup>72</sup> “Social Links CE,” *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/transform-hub/social-links-ce/>.

pieces of data.<sup>72</sup> 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.<sup>73</sup> Although the SIR identifies some types of data that SPD does collect, such as web domain ownership information,<sup>74</sup> 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,<sup>75</sup> 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.<sup>76</sup> Notably, Maltego includes a free integration from “Have I Been Pwned,” which may be used to search for such “public” hacked data.<sup>77</sup> 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.<sup>78</sup> 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.<sup>79</sup> 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

<sup>72</sup> 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/>.

<sup>73</sup> “Wayback Machine,” *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/transform-hub/wayback-machine/>.

<sup>74</sup> SPD, “Maltego,” 6.

<sup>75</sup> *Ibid.*, 5.

<sup>76</sup> Joseph Cox, “Police are Buying Access to Hacked Website Data,” *Vice.com*, July 8, 2020, <https://www.vice.com/en/article/3atvey/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-services-15-websites-offering>.

<sup>77</sup> “Have I Been Pwned,” *Maltego.com*, Accessed June 15, 2021, <https://www.maltego.com/transform-hub/haveibeen-pwned/>.

<sup>78</sup> Jeremy Kirk, “Who Is Tweeting from the NSA’s Parking Lot?” *Computer World*, October 17, 2012, <https://www.computerworld.com/article/2402504/who-is-tweeting-from-the-nsa-s-parking-lot.html>.

<sup>79</sup> 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/88651/2016-law-enforcement-use-of-social-media-survey\\_5.pdf](https://www.urban.org/sites/default/files/publication/88651/2016-law-enforcement-use-of-social-media-survey_5.pdf).

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

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.<sup>85</sup> 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,<sup>86</sup> 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.<sup>87</sup> During the July 20<sup>th</sup> 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.”<sup>88</sup> 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

<sup>80</sup> Rachel Levinson-Waldman, “Government Access to and Manipulation of Social Media: Legal and Police Challenges,” *Howard Law Journal* (61.3, 2018), [https://www.humanrightscenter.org/sites/default/files/maliciousness/images/RLW\\_HowardLJ\\_Article.pdf](https://www.humanrightscenter.org/sites/default/files/maliciousness/images/RLW_HowardLJ_Article.pdf), 529.

<sup>81</sup> “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>.

<sup>82</sup> 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.

<sup>83</sup> Lau, “Predictive Policing Explained,” Friend, “Seattle’s New Crime Analytics Program.”

<sup>84</sup> Levinson-Waldman, “Government Access,” 530.

<sup>85</sup> *Ibid.*, 528.

<sup>86</sup> SPD, “Maltego,” 5.

<sup>87</sup> *Ibid.*, 8 and 10.

<sup>88</sup> *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.”<sup>89</sup> 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,”<sup>90</sup> 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.”<sup>91</sup> The SIR indicates that SPD exports Maltego charts back into SPD’s system<sup>92</sup> and suggests that data from Maltego might be used for “defensive” purposes.<sup>93</sup> 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.
- c. **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.”<sup>94</sup> 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,”<sup>95</sup> and thereby “help in identifying unknown relationship[s].”<sup>96</sup>

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.<sup>97</sup>

---

<sup>89</sup> Ibid., 6.  
<sup>90</sup> SPD, “Maltego,” 20.  
<sup>91</sup> Law Enforcement,” *Maltego.com*.  
<sup>92</sup> SPD, “Maltego,” 9.  
<sup>93</sup> Ibid., 6.  
<sup>94</sup> Ibid., 6 and 14.  
<sup>95</sup> Ibid., 6.  
<sup>96</sup> Ibid.  
<sup>97</sup> 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.<sup>98</sup> 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.<sup>99</sup> 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,”<sup>100</sup> but elsewhere says that private information gathered via search warrant can be input into Maltego.<sup>101</sup> The SIR does not describe measures to keep that private data secure nor outlines Paterva’s or Maltego Technologies’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.<sup>102</sup> 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?

---

<sup>98</sup> Ibid., 9.

<sup>99</sup> Ibid., 10.

<sup>100</sup> Ibid., 9.

<sup>101</sup> Ibid., 6.

<sup>102</sup> 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



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



### **Callyo (Police)**

1. Data from this application is stored on Amazon Web Services<sup>1</sup>. Will any SPD generated data 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 Motorola 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?

---

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



### **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?



## 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<sup>2</sup>. 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?

---

<sup>2</sup> <https://gspp.berkeley.edu/assets/uploads/research/pdf/SpencerCharbonneauGlaser.Compass.2016.pdf>



## **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 non-profits, 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?



### *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 Maltego 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?



## 2021 Surveillance Impact Report Executive Overview

# IBM i2 iBase

## Seattle Police Department

## Overview

**The Operational Policy statements in this document represent the only allowable uses of the equipment and data collected by this technology.**

This Executive Overview documents information about the collection, use, sharing, security and access controls for data that is gathered through SPD's I2 iBase. All information provided here is contained in the body of the full Surveillance Impact Review (SIR) document but is provided in a condensed format for easier access and consideration.

### 1.0 Technology Description

The iBase software is a SQL server that imports a portion of the data from SPD's Records Management System (RMS) and Computer Aided Dispatch (CAD) systems, allowing users to visualize the data in a link chart (rather than the standard textual display in RMS/CAD). The iBase server is an on-premise security encrypted server housed and managed by Seattle IT meeting CJIS approved requirements. The client i2 Analyst's Notebook software is locally installed on Real Time Crime Center (RTCC) analysts' workstations. An automated electronic data transfer allows information located within SPD's RMS and CAD systems to be imported into the iBase system via a one-way transfer of data from the source systems to iBase. 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. IBM i2 Analyst's Notebook is the worldwide standard software solution for operational crime analysis and visualization, with the purpose of creating relevant intelligence from large amounts of data. Various types of structured data are compared and visualized through a variety of heatmaps, relationships, and diagrams.

### 2.0 Purpose

Prior to the implementation of the iBase software, investigators were required to re-type all criminal information from RMS onto visualization charts, which was a time-consuming and redundant process. Implementing iBase gave users direct access to that information without having to re-type it. This software is used exclusively for ongoing criminal investigations and therefore necessarily includes personal information about subjects of those investigations.

The utilization of the IBM Security i2 iBase system increases efficiency of investigations, availability of data, awareness of situational information, and timeliness of actionable information to officers on the street.

### 3.0 Data Collection and Use

**Operational Policy: All use of the i2 iBase system must also comply with [SPD Policy 12.050 – Criminal Justice Information Systems](#) and may only be used for legitimate criminal investigative purposes.**

**Use of the iBase system is governed by the [City of Seattle Intelligence Ordinance \(SMC 14.12\), 28 CFR Part 23](#), CJIS requirements, and any future applicable requirements.**

The only information pulled into iBase automatically comes from SPD's Records Management System (RMS) and Computer Aided Dispatch (CAD) system. Users may manually add additional information that they have collected during the course of a criminal investigation. All manually added information is deleted after five years, in accordance with 28 CFR Part 23. No data outside SPD's RMS/CAD (e.g. commercial data aggregators, publicly available data, or other city departments) is automatically collected.

IBM i2 iBase is currently in use by the RTCC to assist with criminal investigations and to provide actionable information to units in the field. SPD employees in the RTCC and Investigations Unit utilize the i2 Analyst's Notebook software and information stored in the i2 iBase system. It may also be used in compliance with the City of Seattle Intelligence Ordinance.

## 4.0 Data Minimization & Retention

**Operational Policy:** All manually added information is deleted after five years, in accordance with [28 CFR Part 23](#).

All data changes are logged in the software's audit log, which is reviewed periodically. In addition, when manually adding information, a user must provide the source description, source reliability, and content certainty.

No data outside SPD's RMS/CAD (e.g. commercial data aggregators, publicly available data, or other city departments) is automatically collected.

The software automatically alerts users of data that must be deleted under legal deletion requirements such as 28 CFR Part 23.

## 5.0 Access & Security

**Operational Policy:** All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions:

- [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.

### Access

Data stored in the i2 iBase system is accessed by SPD employees assigned to the Real Time Crime Center and Investigations Unit. Access to the application requires SPD personnel to log in with password-protected login credentials which are granted to employees with business needs to access CAD. These employees are ACCESS and CJIS certified.

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

ITD client services interaction with SPD systems is governed by the terms of the 2017 Management Control Agreement between ITD and SPD, which states that: “Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBI’s Criminal Justice Information Services, (CJIS) Security Policy.”

## Security

Only authorized SPD users can access the system, technology, or the data. Access to the application is limited to SPD personnel via password-protected login credentials. All user activity within the iBase system generates a log that is auditable.

Data is securely input and used on SPD’s password-protected network with access limited to authorized users.

The entire system is located on the SPD network that is protect by industry standard firewalls. ITD performs routine monitoring of the SPD network.

The CAD system is CJIS compliant. More information on CJIS compliance may be found at the CJIS Security Policy website.

All data that goes to mobile clients are encrypted to FIP 140-2 standards and is therefore CJIS compliant.

## 6.0 Data Sharing and Accuracy

**Operational Policy: No person, outside of SPD and Seattle IT, has direct access to the application or the data.**

**Because all the data used in this project relates to criminal investigations, any information shared will follow standard policing practices and CJIS compliance.**

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. For example, an investigator may send out a photo or description of a homicide suspect in order to find out if another LE agency knows their identity.

Products developed using this information may be shared with other law enforcement agencies. All products created with the information used in this project will be classified as Law Enforcement Sensitive. Any bulletins will be marked with the following restrictions: LAW ENFORCEMENT SENSITIVE — DO NOT LEAVE PRINTED COPIES UNATTENDED — DISPOSE OF IN SHREDDER ONLY – NOT FOR PUBLIC DISPLAY OR DISTRIBUTION — DO NOT FORWARD OR COPY.

## 7.0 Equity Concerns

**Operational Policy: To mitigate against any potential algorithmic bias or ethnic bias to emerge in the use of link analysis software such as the iBase system, SPD employees are responsible for gathering, creating, and disseminating information 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.**

IBM Security i2 iBase system is used during the investigation of crimes by the SPD Real Time Crime Center and information collected and stored in the system 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 the i2 iBase system must also comply with SPD Policy 12.050 – Criminal Justice Information Systems and may only be used for legitimate criminal investigative purposes.

## SUMMARY and FISCAL NOTE\*

<b>Department:</b>	<b>Dept. Contact/Phone:</b>	<b>CBO Contact/Phone:</b>
SPD / ITD	Rebecca Boatwright Vinh Tang/206-684-7640	Neal Capapas/206-684-5292

*\* Note that the Summary and Fiscal Note describes the version of the bill or resolution as introduced; final legislation including amendments may not be fully described.*

### **1. BILL SUMMARY**

**Legislation Title:** AN ORDINANCE relating to surveillance technology implementation; authorizing approval of uses and accepting the 2021 surveillance impact report and 2021 executive overview for the Seattle Police Department’s use of IBM i2 iBase.

**Summary and background of the Legislation:** Per SMC Chapter 14.18 (also known as the Surveillance Ordinance), authorizing the approval of the surveillance impact reports for Seattle Police Department’s continued use of I2 iBase.

### **2. CAPITAL IMPROVEMENT PROGRAM**

**Does this legislation create, fund, or amend a CIP Project?**            \_\_\_ Yes  X  No

### **3. SUMMARY OF FINANCIAL IMPLICATIONS**

**Does this legislation amend the Adopted Budget?**                            \_\_\_ Yes  X  No

**Does the legislation have other financial impacts to The City of Seattle that are not reflected in the above, including direct or indirect, short-term or long-term costs?**

This technology is currently in use by the Seattle Police Department and no additional costs, either direct or indirect, will be incurred based on the continued use of the technology. However, should it be determined, that SPD should cease use of the technology, there would be costs associated with decommissioning the technologies. Additionally, there may be potential financial penalty related to breach of contract with the technology vendors.

**Is there financial cost or other impacts of *not* implementing the legislation?**

Per the Surveillance Ordinance, the City department may continue use of the technology until legislation is implemented. As such, there are no financial costs or other impacts that would result from not implementing the legislation.

### **4. OTHER IMPLICATIONS**

**a. Does this legislation affect any departments besides the originating department?**

This legislation does not affect other departments. The technology under review is used exclusively by the Seattle Police Department.

**b. Is a public hearing required for this legislation?**

A public hearing is not required for this legislation.

**c. Is publication of notice with The Daily Journal of Commerce and/or The Seattle Times required for this legislation?**

No publication of notice is required for this legislation.

**d. Does this legislation affect a piece of property?**

This legislation does not affect a piece of property.

**e. Please describe any perceived implication for the principles of the Race and Social Justice Initiative. Does this legislation impact vulnerable or historically disadvantaged communities? What is the Language Access plan for any communications to the public?**

The Surveillance Ordinance in general is designed to address civil liberties and disparate community impacts of surveillance technologies. Each Surveillance Impact Review included in the attachments, as required by the Surveillance Ordinance, include a Racial Equity Toolkit review adapted for this purpose.

**f. Climate Change Implications**

**1. Emissions: Is this legislation likely to increase or decrease carbon emissions in a material way?**

No.

**2. Resiliency: Will the action(s) proposed by this legislation increase or decrease Seattle's resiliency (or ability to adapt) to climate change in a material way? If so, explain. If it is likely to decrease resiliency in a material way, describe what will or could be done to mitigate the effects.**

No.

**g. If this legislation includes a new initiative or a major programmatic expansion: What are the specific long-term and measurable goal(s) of the program? How will this legislation help achieve the program's desired goal(s)?**

There is no new initiative or programmatic expansion associated with this legislation. It approves the continuation of use for the specific technologies under review.

**List attachments/exhibits below:**

April 19, 2022

## MEMORANDUM

**To:** Economic Development, Technology and City Light Committee  
**From:** Lise Kaye, Analyst  
**Subject:** Council Bill 120309 - Authorizing approval of uses and accepting the surveillance impact report for the Seattle Police Department's use of IBM's i2 iBase Link Analysis Software

---

On Wednesday, April 27, 2022, the Economic Development, Technology and City Light Committee will discuss [Council Bill 120309](#). This Council Bill would approve the Seattle Police Department's (SPD's) continued use of IBM's i2 iBase Link Analysis Software and accept the Surveillance Impact Report (SIR) and an Executive Overview for this technology. The bill is intended to meet the requirements of [Seattle Municipal Code Chapter 14.18](#), Acquisition and Use of Surveillance Technologies, which requires City of Seattle departments intending to acquire surveillance technology to obtain advance Council approval of that acquisition and of a surveillance impact report (SIR).<sup>1</sup> Departments must also submit a SIR for surveillance technology in use when [Ordinance 125376](#) was adopted in 2017 (referred to in the ordinance as "retroactive technologies"), but failure to approve an ordinance for a retroactive technology does not require SPD to discontinue its use. Councilmembers may choose to amend the ordinance to request additional information or to request that SPD develop new and/or revised operational policies, which, if implemented, could restrict or modify the application of certain technologies.

This memo describes IBM's i2 iBase Link Analysis Software, summarizes recommendations from the Community Surveillance Working Group, describes whether and how each recommendation is addressed in the SIR and/or by current law, and summarizes responses by the Chief Technology Officer (CTO) and/or SPD. Finally, the memo identifies policy issues for Council consideration.

### **IBM's i2 iBase Link Analysis Software**

IBM's i2 iBase Link Analysis Software (iBase) is a relational database that SPD uses to combine and analyze different types of data associated with police investigations. Specifically, SPD's "Real Time Crime Center" (RTCC) uses this software to combine data from its Records Management System (RMS) and the Computer Aided Dispatch (CAD) system with information gathered during criminal investigations and then to portray that information visually on a chart or other display<sup>2</sup>. The visual displays help analysts and investigators see connections between known entities, vehicles, locations, and other data. SPD uses these analyses to assist ongoing criminal investigations and to provide information to officers in the field. The SIR identifies the risk of erroneous links between individuals not related to criminal investigations as the most important unintended civil liberties consequence from this technology. According to SPD, that risk is mitigated because iBase makes it

---

<sup>1</sup> The Executive Overview summarizes SPD's allowable uses of IBM i2 iBase. See also the [memo](#) summarizing process for developing a Surveillance Impact Report (SIR), consistent with [Ordinances 125376](#) and [125679](#) and [Ordinance 108333](#), Seattle's "Intelligence Ordinance," adopted in 1979 and amended in 1982 via adoption of [Ordinance 100572](#).

<sup>2</sup> Displays include heatmaps (per [Wikipedia](#), a data visualization technique that shows magnitude of a phenomenon as color in two dimensions), relationships and diagrams.



easier for users to identify erroneous linkages in existing data. SPD mitigates other risks, such as acquisition of private data about individuals, potential algorithmic bias or ethnic bias, and potential racial or ethnicity-based bias in data sharing, storage and retention by only entering information into iBase related to the investigation of a crime and/or collected in accordance with the City’s Intelligence Ordinance ([SMC 14.12](#)). SPD provides additional mitigation through its evidence procedures, anti-bias policies and warrant parameters. The RET does not identify metrics to be used as part of the CTO’s required annual equity assessments.

**Surveillance Working Group Recommendations and CTO Response**

The Community Surveillance Working Group’s Impact Assessment for iBase makes 15 recommendations to Council. The CTO’s response finds that the “policy, training and technology limitations enacted by SPD provide adequate mitigation for the potential privacy and civil liberties concerns raised by the Working Group.” The CTO’s response does not specifically address the Working Group’s recommendations, but it identifies relevant citations from the SIR for each of the “key concerns” raised by the Working Group. **Table 1** describes whether the SIR as drafted or current law addresses the Working Group’s recommendations, as well as relevant responses from the CTO and/or SPD.

*Table 1. Working Group Recommendations*

Working Group Recommendation	Whether/How Addressed by SIR, CTO or SPD and/or Current Law
<p>1. The purpose and allowable uses of i2 iBase must be clearly defined, and any SPD use of i2 iBase must be limited to that specific purpose and those allowable uses. The specific incident types for which i2 iBase may be used must be clearly stated. The use limits must restrict when someone’s relationship network may be assembled in i2 iBase.</p>	<p><b>Executive Overview.</b> Operational Policies represent the only allowable uses of the equipment and data collected by this technology.</p> <p><b>SIR §3.2</b> ... iBase system is only used during the investigation of crimes by the SPD Real Time Crime Center and information collected and stored in the system is related to these criminal investigations.</p> <p><b>SIR §4.3</b> ... iBase is used to assist with criminal investigations and to provide actionable information to units in the field.</p> <p><i>SMC 14.12 (the “Intelligence Ordinance) governs the collection of data for a criminal investigation.</i></p> <p><i>The SIR does not limit the use of iBase to specific incident types or define when an individual’s network may be assembled.</i></p>
<p>2. If SPD’s use of i2 iBase is governed by a contract, it must be made publicly available.</p>	<p>Not addressed in the SIR.</p> <p><i>Seattle’s Information and Technology Department (ITD) has a contract with IBM for its two annual licenses.</i></p>
<p>3. SPD must publicly disclose all of its data sources, such as data brokers (e.g., LexisNexis, CoreLogic) and any use of non-public details from social media platforms (e.g., Facebook, Twitter).</p>	<p><b>SIR §4.1</b> ... information pulled into iBase automatically comes from SPD’s Records Management System (RMS), Computer Aided Dispatch (CAD) system, and information ... collected during the course of a criminal investigation....</p> <p><i>According to SPD, the department does not enter data from any data brokers into iBase. Open source information obtained during the course of a criminal investigation may be entered into iBase. No social media data that is not open source/publicly available is entered into iBase, even if it was obtained during the course of a criminal investigation.</i></p>

Working Group Recommendation	Whether/How Addressed by SIR, CTO or SPD and/or Current Law
4. SPD must not be permitted to share i2 iBase data with third parties	<b>SIR §6.1</b> No person, outside of SPD and Seattle IT, has direct access to the application or the data.... Because all the data used in this project relates to criminal investigations, any information shared will follow standard policing practices and CJIS compliance.
5. There must be a regular audit to assess for biases in the data imported into i2 iBase and in the analyses generated by i2 iBase. There must be technical mechanisms in place to enable robust auditing to occur (e.g., detailed logs).	<b>SIR §8.2</b> SPD’s Audit, Policy and Research Section is authorized to conduct audits of all investigative data collection software and systems, and the Office of Inspector General for Public Safety and the federal monitor can conduct audits of the software and its use at any time.  <i>According to SPD, the audit log tracks every action a user takes (e.g., searching, accessing data, adding data, editing data).</i>
6. There must be limits on the kinds of data that may be inputted both manually and automatically into i2 iBase, ensuring that additional pools of public or private information are not added in the future.	Not addressed in the SIR.  <i>According to SPD, iBase users may manually add data to iBase that has already been obtained during the course of a criminal investigation. Information collection is governed by <a href="#">SMC 14.12</a> (the “Intelligence Ordinance) and federal regulations (<a href="#">28 CFR Part 23</a> and Criminal Justice Information System requirements).</i>
7. There must be a shortened data retention period that does not exceed the time necessary to conduct a criminal investigation.	<b>SIR §4.0</b> All manually added information is deleted from the system after five years.  <i>The State Law Enforcement Records Retention Schedule for Intelligence Files requires retention “until no longer needed for agency business.” However, federal law allows for a retention period of up to five years, so SPD applies that period to all manually entered data.<sup>3</sup></i>
8. There must be a clear deletion oversight process to ensure that manually added data are deleted after the specified retention period.	<b>SIR §1.2</b> SPD conducts regular reviews of audit logs to ensure proper use and retention of data.  <i>According to SPD, iBase has an automated query that alerts users that manually entered data is approaching its 5-year limit (at 4 years, 9 months and again at 4 years, 11 months), at which point users purge the data from the system through the “batch delete” feature.</i>
9. There must be a requirement that limits employee access to i2 iBase records.	Not addressed in the SIR.  <i>According to SPD, two civilian SPD analysts and one civilian Seattle IT employee currently have access to iBase. Only the two civilian analysts are currently able to produce such visualizations for detectives, but multiple detectives might request such assistance.</i>

<sup>3</sup> Section 8.2 of the [State Law Enforcement Records Retention Schedule](#) establishes different retention periods for different types of Intelligence records. [28 CFR Part 23.20\(h\)](#) establishes a retention period not to exceed five years.

Working Group Recommendation	Whether/How Addressed by SIR, CTO or SPD and/or Current Law
10. There must be a manual relationships analysis process that includes clear checkpoints designed to ensure erroneous data and inaccurate linkages generated by i2 iBase are detected and corrected before they are actively investigated.	<p><b>SIR §4.2</b> ... when manually adding information, a user must provide the source description, source reliability, and content certainty...</p> <p><b>SIR §5.3</b> provides for deletion of improperly collected data found during an audit log review</p>
11. There must be limits on usage of potentially erroneous i2 iBase analyses and search data in rapid-response settings where manual analysis is not possible.	<p>Not addressed in the SIR.</p> <p><i>SPD's use of data from an iBase analysis is an operations issue is governed by the SMC 14.12 (the "Intelligence Ordinance), which governs SPD's collection of data for a criminal investigation.</i></p> <p><i>According to SPD, the department primarily uses iBase for long-term criminal investigations; during time-sensitive investigations, iBase data may be searched, along with searches of RMS, CAD, and relevant files.</i></p>
12. There must be a requirement for SPD to disclose for how many incidents per year they use i2 iBase.	<p>Not addressed in the SIR.</p> <p><i>According to SPD, it would not be possible to track this information, as a single search may result in dozens or more incidents laid out on a chart for analysis.</i></p>
13. There must be a requirement that the use of i2 iBase is always disclosed to the individual or the legal representative of an individual facing charges for which i2 iBase was used in an SPD investigation.	<p><b>SIR §6.6</b> As per RCW 10.97, individuals who are subject to a criminal investigation will not be party to the information collection process...<sup>4</sup></p>
14. There must be a regulation prohibiting the use of i2 iBase for predictive policing.	<p>Not addressed in the SIR.</p> <p><i>According to SPD, data compiled via iBase is never used for predictive purposes. It is a tool to assist in investigation of crimes that have already occurred.</i></p>
15. There must be a contract with IBM that ensures IBM never possesses, uses, or accesses SPD data.	<p>Not addressed in the SIR.</p> <p><i>According to SPD, Seattle's Information and Technology Department (ITD) has a contract with IBM for its two annual licenses and IBM does not have access to SPD's iBase data.</i></p>

<sup>4</sup> RCW 10.97.080 – "... The individual's right to access and review of criminal history record information shall not extend to data contained in intelligence, investigative, or other related files....

## Policy Considerations

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

1. Annual equity assessment metrics. SPD has not yet finalized metrics to be used in evaluating use of i2 iBase as part of the CTO's annual equity assessments. These assessments are intended to play a key role in determining whether the City's surveillance legislation is meeting the goals of the Race and Social Justice Initiative. In the absence of such metrics, it is unclear how SPD and/or the CTO could identify disproportionate impacts from the use of i2 iBase, such as the frequency of specific populations appearing on i2 iBase displays.

### Options:

- A. Council may wish to request a report on the proposed metrics by a date certain.
  - B. Take no action.
2. Response to Public Comments. The SIR does not provide a response to question 4.1 "How will you address the concerns that have been identified by the public."

### Options:

- A. Request that SPD provide a written response to public comments associated with the SIR public engagement process by a date certain.
  - B. Take no action.
3. Mitigation of civil liberties impacts. The SIR flags the risk of erroneous links between individuals not related to criminal investigations as the most important unintended consequence from the use of this technology. The SIR also identifies data sharing, storage and retention as having the potential to contribute to structural racism and/or disparate impacts on historically targeted communities. An expanded evaluation of these risks and related concerns could reveal whether more direct policies and protocols would better protect against errors, potential bias in baseline data, and/or disproportionate over-surveillance.

### Options:

- A. Obtain an independent evaluation of the civil liberties risks associated with the use of iBase, including potential bias in its baseline data sources, the data manually input into iBase, data validation and accuracy of analyses, and demographic information about the individuals and groups associated with each iBase visualization.
- B. Take no action.

4. Contractual Terms – Data and Security Protection. SPD reports that ITD has a contract with IBM for annual licenses for i2 iBase, which only covers the annual subscription cost. The lack of a contract and/or reliance upon a vendor-provided licensing agreement may reduce the City’s ability to restrict IBM’s access to sensitive and/or private information.<sup>5</sup>

Options:

- A. Request that SPD contractually ensures data and security protection of personally identifiable information or sensitive information generated or otherwise obtained through the use of iBase. This may require additional resources, potentially through a supplemental budget action.
- B. Take no action.

5. Retention schedule. The i2 iBase system automatically deletes manually entered data after five years. SPD uses the maximum, rather than the minimum, retention periods allowed by state and federal law. As noted above (see footnote 3), federal policies establish a retention period not to exceed five years. Extended records retention could result in maintaining inaccurate and/or out of date information.

Options:

- A. Request that SPD develop a policy for retention of iBase records that complies with the minimum retention period allowed by state and federal law and that requires regular review and validation of iBase records retained for more than one year.
- B. Take no action.

6. Data sharing with Community Safety and Communications Center. The SIR describes how the iBase system uses data from SPD’s Computer Aided Dispatch (CAD) system, however, new data sharing protocols should be developed since the CAD system is now housed within the Community Safety and Communications Center.

Options:

- A. Request that SPD develop a formal agreement with the CSCC establishing common protocols for data retention and sharing of data.
- B. Take no action.

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

---

<sup>5</sup> Data and security protection for the City’s data may not be included by vendors in their standard licensing agreements for off-the-shelf products or for “software as a service” products, in which an application is accessed via a cloud provider. ITD incorporates data and security protection requirements into its purchasing contracts, and Finance and Administration Department’s contract template for purchasing technology has similar terms.

April 19, 2022

## MEMORANDUM

**To:** Economic Development, Technology and City Light Committee  
**From:** Lise Kaye, Analyst  
**Subject:** Surveillance Impact Report Process and Related Legislation

---

This memo describes legislative history of the City’s Intelligence and Surveillance Ordinances and the process by which the Executive produces a Surveillance Impact Report (SIR).

### **Powers and Functions of Seattle Police Department’s Criminal Information Section<sup>1</sup>**

The Seattle City Council (Council) adopted [Ordinance 108333](#), often referred to as Seattle’s “Intelligence Ordinance,” in 1979 and amended it in 1982 via adoption of [Ordinance 110572](#). Section 27 of Ordinance 108333 defines Seattle Police Department’s Criminal Intelligence powers and functions, including the following authority to:

- collect, evaluate, organize, and analyze data and specific investigative information about organized criminal activity (subsequently defined by Ordinance 100572 as “a continuing enterprise engaged in solely for the purpose of obtaining monetary gain... through racketeering, vice, narcotics, gambling, fencing, or similar criminal activity”);
- collect, evaluate, and classify information about incidents of unlawful activity, confirming the degree of accuracy of the information whenever possible;
- study, detect and explain any meaningful patterns of unlawful activities;
- furnish and exchange relevant criminal intelligence information with criminal justice agencies; and
- develop methods for evaluating the effectiveness of the Criminal Intelligence Section in accomplishing its law enforcement purposes and safeguarding the constitutional rights and privacy of all individuals.

Ordinance 110572 also established policies governing the collection, recording, retention and sharing of information by SPD personnel ([SMC 14.12.020](#)), including the following directives:

- All collected information shall reasonably appear relevant to the performance of an authorized police function;
- Only information deemed relevant to present and future law enforcement activities or required by law shall be retained;
- Authorized disclosure of information, including when needed by criminal justice functions, for scientific or law enforcement research under assurance of confidentiality, and when pertinent to agencies with regulatory responsibilities.

---

<sup>1</sup> [SMC 14.12.290](#)

## Acquisition and Use of Surveillance Technologies<sup>2</sup>

[Ordinance 125376](#), passed by Council on July 31, 2017, requires City of Seattle departments intending to acquire surveillance technology to obtain advance Council approval, by ordinance, of the acquisition and of a SIR.<sup>3</sup> Departments must also submit an SIR for surveillance technology in use when Ordinance 125376 was adopted (referred to in the ordinance as “retroactive technologies”), but failure to approve an ordinance for a retroactive technology does not require a department to discontinue its use. Councilmembers may choose to amend an ordinance to request additional information or to request that the Executive develop new and/or revised operational policies, which, if implemented, could restrict or modify the application of certain technologies. As of April 1, 2021, the Council has accepted SIRs for 16 of the 28 technologies on the current Master List and extended the initial March 3, 2020 deadline to complete the retroactive SIRs to September 1, 2022.<sup>4</sup>

Either the Chief Technology Officer or the Council may determine whether a specific technology is “surveillance technology” and thus subject to the requirements of SMC 14.18. Each SIR must describe protocols for a “use and data management policy” as follows:

- How and when the surveillance technology will be deployed or used and by whom.
- How surveillance data will be securely stored.
- How surveillance data will be retained and deleted.
- How surveillance data will be accessed.
- Whether a department intends to share access to the technology or data with any other entity.
- How the department will ensure that personnel who operate the technology and/or access its data can ensure compliance with the use and data management policy.
- Any community engagement events and plans.
- How the potential impact of the surveillance on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities have been taken into account, and a mitigation plan.
- The fiscal impact of the surveillance technology.

---

<sup>2</sup> [SMC 14.18](#)

<sup>3</sup> As codified in SMC 14.18.030, Ordinance 125376 identified a number of exemptions and exceptions to the required Council approval, including information voluntarily provided, body-worn cameras and cameras installed in or on a police vehicle, cameras that record traffic violations, security cameras and technology that monitors City employees at work.

<sup>4</sup> As provided for in [Ordinance 125679](#), Council has granted five six-month extension requests: first to accommodate extended deliberation of the first two SIRs; and then four more primarily due to COVID-related delays and/or to provide additional time for public engagement.

## Community Surveillance Working Group

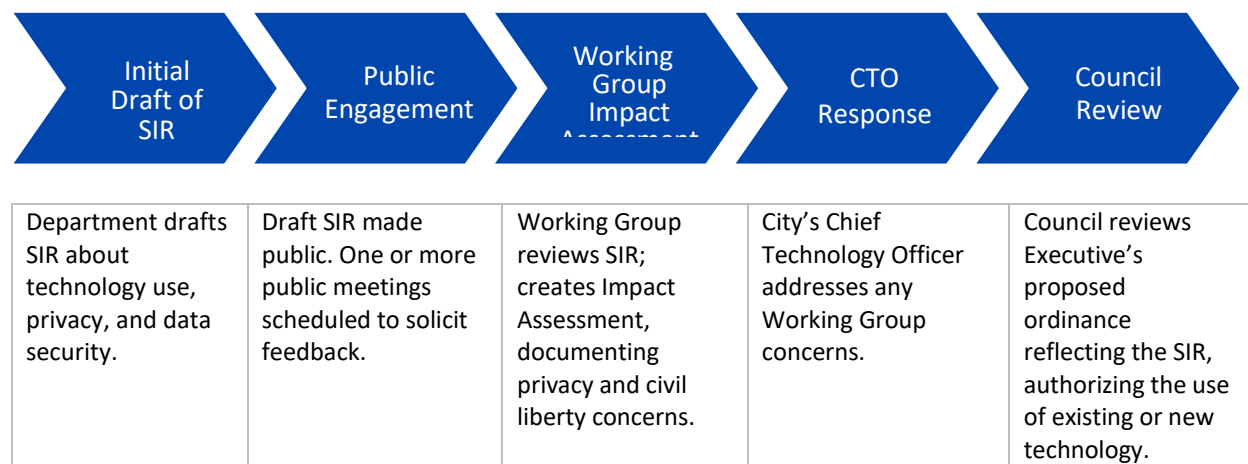
On October 5, 2018, Council passed [Ordinance 125679](#), amending SMC 14.18, creating a “community surveillance working group” charged with creating a Privacy and Civil Liberties Impact Assessment for each SIR. At least five of the seven members of the Working Group must represent groups that have historically been subject to disproportionate surveillance, including Seattle’s diverse communities of color, immigrant communities, religious minorities, and groups concerned with privacy and protest.<sup>5</sup> Each Privacy and Civil Liberties Impact Assessment must describe the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities and will be included in the SIR. Prior to submittal of a SIR to Council, the Chief Technology Officer may provide a written statement that addresses privacy rights, civil liberty or other concerns in the Working Group’s impact assessment.

## Executive Overviews

In May 2019, members of the Governance, Equity, and Technology Committee requested that the Seattle Information Technology Department staff prepare a summary section for each of the two lengthy SIR documents under review at that time. The Committee then accepted the resultant “Condensed Surveillance Impact Reports (CSIRs) together with the complete SIRs. The Executive has continued this practice with subsequent SIRs but has renamed the documents “Executive Overviews.” The Operational Policy Statements in the Executive Overview represent the only allowable uses of the subject technology.

## SIR Process

The following chart illustrates the SIR process from inception to Council Review:



cc: Aly Pennucci, Interim Director  
Brian Goodnight, Lead Analyst

<sup>5</sup> The Mayor appoints four members, and the Council appoints three members.