

## 2021 Surveillance Impact Report

# Callyo

Seattle Police Department

DRAFT

<b>Surveillance Impact Report (“SIR”) overview.....</b>	<b>3</b>
<b>Privacy Impact Assessment .....</b>	<b>4</b>
<b>Financial Information .....</b>	<b>18</b>
<b>Expertise and References.....</b>	<b>20</b>
<b>Racial Equity Toolkit (“RET”) and engagement for public comment worksheet. </b>	<b>21</b>
<b>Privacy and Civil Liberties Assessment.....</b>	<b>27</b>
<b>Submitting Department Response .....</b>	<b>28</b>
<b>Appendix A: Glossary.....</b>	<b>29</b>

**DRAFT**

# Surveillance Impact Report (“SIR”) overview

## About the Surveillance Ordinance

The Seattle City Council passed Ordinance [125376](#), also referred to as the “Surveillance Ordinance,” on September 1, 2017. SMC 14.18.020.b.1 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”.

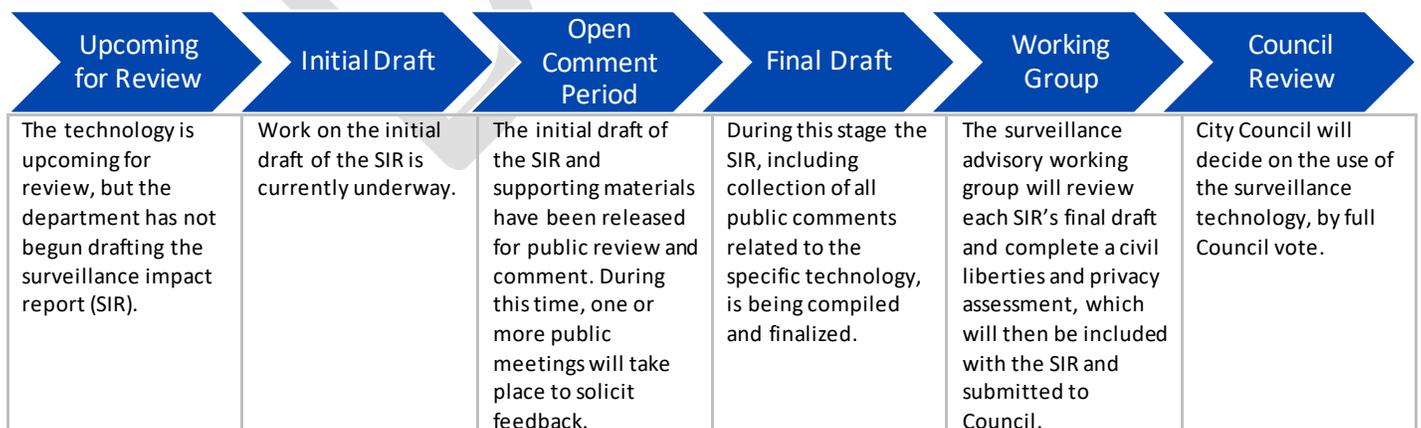
## How this Document is Completed

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.

DRAFT

## 1.0 Abstract

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

Motorola Solutions' Callyo, a software as a service (SaaS), is a cell phone identification masking and recording technology. The technology masks the phone number assigned to an existing phone, displaying a different local number to recipients of calls from the phone. Additionally, the technology can record all calls made to/from the masked phone, covertly record audio, as well as GPS locate the phone of a caller. When Seattle Police Department (SPD) utilizes Callyo to records conversations, the technology is used only with search warrant. Callyo is a subset of the SPD audio recording systems explained in the SIR titled "Audio Recording Systems 'Wires'."

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

Callyo has the ability to disguise the identity of a willing participant by masking a phone number, record phone conversations, covert recording device, and GPS locate identifiable individuals, who are unaware of the operation. Without appropriate safeguards, this raises significant privacy concerns. Recognizing this potential, SPD utilizes Callyo in a limited fashion, and only subject to 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.**

Callyo allows SPD to pursue resolution of criminal investigations expeditiously, by masking the identify of an officer in an undercover investigation, recording conversations and location of suspects, only after a court magistrate has determined that sufficient probable cause exists and an order has issued. Without this technology, SPD would be unable to 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.**

Callyo is installed on a SPD Department cell phone and has the ability to disguise the identity of an officer by masking a phone number, record phone conversations, and GPS locate identifiable individuals, who are unaware of the operation. When Seattle Police Department (SPD) utilizes Callyo to records conversations, the technology is used only with a search warrant.

### **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 and phone number masking 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 to record audio with a warrant.

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

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.

For all other Callyo deployments, once an Officer/Detective has obtained a court order to utilize Callyo, having established probable cause, s/he makes a verbal request to the TESU for deployment of Callyo. TESU documents the equipment requested, the legal authority, and the case number. TESU then deploys the equipment to the requesting Officer/Detective to engage within the scope of the court order.

If no data was collected by the device that assists in the pursuit of the criminal investigation or falls within the scope of the 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.

Callyo is managed and maintained by staff within the Technical and Electronic Support Unit (TESU) and the High Risk Victims Unit.

Staff within the High Risk Victims Unit deploy Callyo for investigations related to cases assigned to that unit and maintain records of each Callyo deployment. The High Risk Victims Unit uses Callyo to mask phone numbers but does not utilize the recording features of Callyo.

For all other Callyo deployments, once an Officer/Detective has obtained a court order to utilize Callyo, having established probable cause, 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 court order. Each request is screened by the TESU Supervisor prior to deployment.

TESU detectives then install Callyo on a SPD cellphone and use Callyo to connect into a willing participant's phone conversation with a 3<sup>rd</sup> party.

Each deployment is logged, and all request forms (including 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.

The recording features of Callyo are utilized only after legal standards of the 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. Callyo may only be issued/deployed by TESU and High Risk Victims Unit detectives. All TESU and High Risk Victims Unit staff that deploy Callyo are trained in its use. Staff within the High Risk Victims Unit deploy Callyo for investigations related to cases assigned to that unit and maintain records of each Callyo deployment. The High Risk Victims Unit uses Callyo to mask phone numbers but does not utilize the recording features of Callyo.

For all other Callyo deployments, once an Officer/Detective has obtained a court order, having established probable cause, to utilize Callyo, 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 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 in Callyo collects conversations, sounds, and location information of individuals related to a criminal investigation. The information is extracted onto a thumb drive from Callyo and stored utilizing SPD policies regarding evidence. [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.

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

Deployment of audio recording devices, including Callyo, is constrained to the conditions stipulated by 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 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.

### 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?

Callyo is managed and maintained by staff within the Technical and Electronic Support Unit (TESU) and the High Risk Victims Unit.

Staff within the High Risk Victims Unit deploy Callyo for investigations related to cases assigned to that unit and maintain records of each Callyo deployment. The High Risk Victims Unit uses Callyo to mask phone numbers but does not utilize the recording features of Callyo.

For all other Callyo deployments, once an Officer/Detective has obtained a court order to utilize Callyo, having established probable cause, 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 court order. Each request is screened by the TESU Supervisor prior to deployment.

Each deployment is logged, and all request forms (including warrant number) are maintained within TESU.

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

The High Risk Victims Unit uses Callyo to mask phone numbers but does not utilize the recording features of Callyo. Each deployment of this technology is logged within the HRVU. Court ordered warrants determine the scope of each deployment where audio recording is attempted utilizing Callyo. Callyo is generally used to meet the needs of a criminal investigation, and the scope is specifically limited to the stipulations of the court-ordered warrants providing authorization of use.

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

Once a warrant has been issued, TESU detectives uses Callyo to connect into a willing participant's phone conversation with a 3<sup>rd</sup> party. Callyo connections must be accepted by a participant. After a warrant has expired SPD does not initiate this connection.

#### 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?

Callyo is not a physical object and there are no visible markings indicating when it is in use.

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

Data collected with Callyo is 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, including Callyo, 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 court-ordered warrant to utilize Callyo's recording features. The data is accessed in the course of a criminal investigation.

#### 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.)?

Data collected utilizing Callyo is stored as evidence. [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.

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 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?

Data collected utilizing Callyo is stored as evidence on physical media such as a thumb drive. [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.

### 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 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 court-ordered warrants. Any data that is collected outside the established scope is purged by the investigating detective.

[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, including Callyo. No person, outside of SPD, has direct access to Callyo 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 executed 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.

Callyo capture sounds as they are happening in the moment and the location information of individuals. The software does not interpret or otherwise, analyze any data it collects.

## 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 Callyo is governed at the state level by the [Washington Privacy Act](#). Callyo is utilized only with a 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 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 warrants) that allow for any auditor, including the Office of Inspector General and the federal monitor, to inspect use and deployment and use of Callyo. The potential of privacy risk is mitigated by the requirement of a 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:

The initial acquisition costs for Callyo occurred prior to 2012.

#### 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
Annual Licensing Basic System and Additional Callyo Lines of Service \$7650				

Notes:

\$4200/yr High Risk Victims Unit, \$3450 TESU

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

Callyo recording is used with a search warrant to resolve investigations. It provides 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

DRAFT

## 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>

# 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 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 a 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 checked="" 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?

Callyo is used exclusively during the investigation of crimes and only records information within the bounds of a 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 Callyo 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 Callyo 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 Callyo is the possibility that the civil rights of individuals may be compromised by unlawful surveillance. SPD mitigates this risk by requiring a court-ordered warrant, having established probable cause, prior to the utilization of any recording capabilities of these technologies.

**2.0 Public Outreach**

**2.1 Organizations who received a personal invitation to participate.**

Please include a list of all organizations specifically invited to provide feedback on this technology.

1.	2.	3.
----	----	----

**2.1 Scheduled public meeting(s).**

Meeting notes, sign-in sheets, all comments received, and questions from the public will be included in Appendix B, C, D, E, F, G, H and I. Comment analysis will be summarized in section 3.0 Public Comment Analysis.

<b>Location</b>	
<b>Time</b>	
<b>Capacity</b>	
<b>Link to URL Invite</b>	

**2.2 Scheduled focus Group Meeting(s)**

Meeting 1

<b>Community Engaged</b>	
<b>Date</b>	

Meeting 2

<b>Community Engaged</b>	
<b>Date</b>	

### 3.0 Public Comment Analysis

This section will be completed after the public comment period has been completed on [DATE] by Privacy Office staff.

#### 3.1 Summary of Response Volume

Dashboard of respondent demographics.

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

Dashboard of respondent demographics.

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

Dashboard of respondent demographics.

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

Dashboard of respondent demographics.

#### 3.5 Question Four: General response to the technology.

Dashboard of respondent demographics.

#### 3.5 General Surveillance Comments

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

Dashboard of respondent demographics.

### 4.0 Response to Public Comments

This section will be completed after the public comment period has been completed on [DATE].

**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.

DRAFT

# 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

Respond here.

## Submitting Department Response

### Description

Provide the high-level description of the technology, including whether software or hardware, who uses it and where/when.

### Purpose

State the reasons for the use cases for this technology; how it helps meet the departmental mission; benefits to personnel and the public; under what ordinance or law it is used/mandated or required; risks to mission or public if this technology were not available.

### Benefits to the Public

Provide technology benefit information, including those that affect departmental personnel, members of the public and the City in general.

### Privacy and Civil Liberties Considerations

Provide an overview of the privacy and civil liberties concerns that have been raised over the use or potential mis-use of the technology; include real and perceived concerns.

### Summary

Provide summary of reasons for technology use; benefits; and privacy considerations and how we are incorporating those concerns into our operational plans.

## 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.

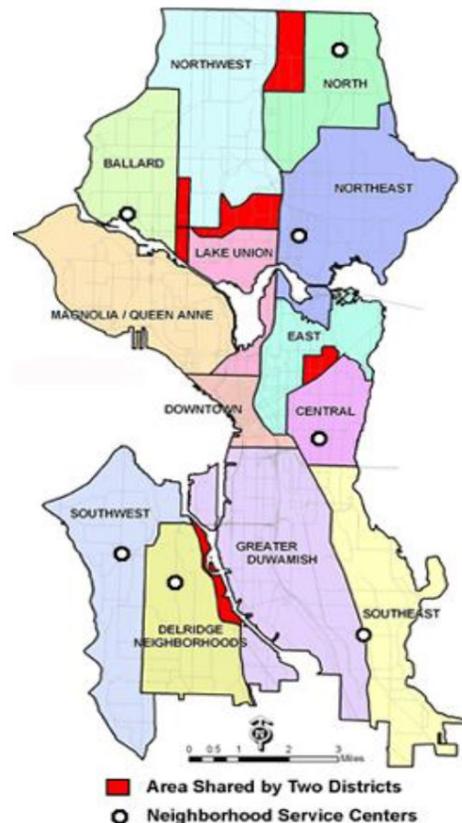
**Stakeholders:** (taken from the racial equity toolkit.) Those impacted by proposed policy, program, or budget issue who have potential concerns or issue expertise. Examples might include: specific racial/ethnic groups, other institutions like Seattle housing authority, schools, community-based organizations,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



DRAFT