Memo

Date:

To: Seattle City Council

From: Jim Loter, Interim Chief Technology Officer

Subject: CTO Response to the Surveillance Working Group Callyo 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 Callyo.

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

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, and 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'."

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: Callyo

Concern: Additional policy language is necessary to define a specific and restricted purpose of use.

CTO Assessment: The SIR outlines the purpose and conditions under which Callyo is used. Data obtained are processed in accordance with SPD's policies and other applicable laws as described below.

SIR Response:

Section 2.5

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.

Section 3.1

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 installs Callyo on a SPD cellphone and uses Callyo to connect into a willing participant's phone conversation with a 3rd party.

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

SIR 3.2

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.

Concern: Inadequate policies regarding data collection and unclear policies regarding data storage, protection, and sharing.

CTO Assessment: The SIR contains discrete sections addressing the policies around each of these areas of concern. Additionally, policies governing the use are defined in the SPD manual and may be governed by various state laws as detailed in the SIR.

SIR Response:

Section 4.2

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. 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.

Section 4.7

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."

Section 5.1:

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."

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 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 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.

Section 6.1

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."

Concern: Inadequate oversight policies restricting Callyo technologies' additional surveillance features.

CTO Assessment: The SIR details the use of Callyo. Any additional features or use outside of the scope of the SIR-defined functionality, will be evaluated as a material change to the SIR, under City Surveillance Policy PR-02, and as prescribed by law.

Concern: It is unclear what specific Callyo technologies or applications SPD uses.

CTO Assessment: The solution in use is described in the defined SIR section below.

SIR Response:

Section 1.1

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'."

Concern: There is lack of clarity around requirements for a warrant.

CTO Assessment: Callyo is 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 court-ordered warrant to utilize Callyo's recording features. The data is accessed in the course of a criminal investigation.

Concern: It is unclear how Callyo technologies may be used and by whom.

CTO Assessment: The SIR states how Callyo is used and by whom. Callyo is managed by staff within the Technical and Electronic Support Unit and High Risk Victims Unit. These staff may deploy the technology to

support investigations assigned to that unit. Further detail on the use of the audio recording features by the units are described in the SIR.

SIR Response:

Section 3.1

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 installs Callyo on a SPD cellphone and uses Callyo to connect into a willing participant's phone conversation with a 3rd party.

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

Concern: It is unclear if and how Motorola Solutions collects or retains data.

CTO Assessment: Any data collection and sharing has been defined within the SIR and is scoped within the use and sharing outlined below.

SIR Response:

Section 6.1

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.

Concern: There are inadequate data retention policies.

CTO Assessment: The SIR contains discrete sections addressing the policies around each of these areas of concern. Additionally, policies governing the use are defined in the SPD manual and may be governed by various state laws as detailed in the report.

SIR Response:

Section 4.7

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.

Section 5.1

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.

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 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 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.

Section 5.4

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.