City of Seattle

## 2023 Surveillance Impact Report Executive Overview

# Callyo

## 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 Callyo. 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

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 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'."

# 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. 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.

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.

# 3.0 Data Collection and Use

**Operational Policy: 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.**

Audio recording in Callyo collects conversations, sounds, and location information of individuals related to a criminal investigation. The information is extracted onto digital media from Callyo and stored utilizing SPD policies regarding evidence. SPD Policy 7.010governs 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.

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 is kept on file with SPD. Each request is screened by the TESU Supervisor prior to deployment. TESU detectives then provide access to Callyo on a SPD cellphone for the requesting detective, who 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.

# 4.0 Data Minimization & Retention

**Operational Policy: 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.**

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 system 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 data created for the case in question 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). 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.

# 5.0 Access & Security

**Operational Policy: 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.**

**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

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 .140Officers/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.

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.

### Security

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.

## 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 Callyo must also comply with SPD Policy 12.050 – Criminal Justice Information Systems and may only be used for legitimate criminal investigative purposes.**

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.