Seattle Office of Inspector General

Callyo Report 2024

As Required by Seattle Municipal Code 14.18.060

September 30, 2025

Office of Inspector General
City of Seattle
PO Box 94764
Seattle, WA 98124-7064

206.684.3663
oig@seattle.gov

Acknowledgement

We would like to thank Technical and Electronic Support Unit (TESU) personnel for their participation in this review. TESU staff made themselves available to answer questions and directed us to key personnel throughout the course of this review. The unit's desire to collaborate with the Seattle Office of Inspector General (OIG) to provide transparency throughout the oversight process is notable and appreciated.

Technology Description

Callyo refers to a bundle of Motorola Solutions software applications for investigative recording purposes. Callyo provides a variety of applications, each requiring an individual subscription. The Seattle Police Department (SPD) uses three applications: a virtual investigative phone, an audio recording software, and a software that tracks an officer's live location. Callyo has multiple capabilities, but SPD only has access to the three paid subscriptions. Using additional Callyo capabilities, outside of these subscriptions, could require a material change to the Surveillance Impact Report (SIR).

The SIR Inaccurately Describes the Current Managers and Capabilities of this Technology

SPD has two units that manage access to Callyo; the Technical and Electronic Support Unit (TESU) and the Internet Crimes Against Children (ICAC) unit. The SIR identifies the "High-Risk Victims Unit" (HRVU) as a unit with distinct processes for using Callyo, however SPD reported that this is no longer accurate.

TESU manages requests for most surveillance technologies used by other units in the department. They approve technology deployment, assist in deployment, extract data, and provide data to investigating officers. ICAC investigates Child Sexual Exploitation (CSE) cases that might involve the production, distribution, or possession of CSE materials or where Electronic Service Provider systems have been used for CSE crimes. CSE crimes often involve the use of computers, cellular phones, tablets or other electronic devices. Due to the nature of ICAC's work, they have slightly different approval processes for some surveillance technologies, including Callyo.

The *virtual investigative phone* functions similarly to a "burner phone," a physical phone used by officers while they conduct undercover investigations. Instead of using a separate cellphone, officers can use a mobile application or computer for the same purposes. Since the virtual investigative phone does not have audio or video record capabilities and relies on a suspect to willfully engage in communication, the use of the technology does not require a warrant.

The *audio recording software* is similar to audio recording devices, also known as "wires," but does not require any physical equipment. Since

this software records audio, any use must adhere to the Washington Privacy Act, Chapter 9.73, which generally requires two-party consent. Two-party consent is not required if a warrant is obtained. There are also warrant exceptions. RCW 9.73.210 allows law enforcement officers to intercept, transmit, or record a private conversation or communication concerning the sale of controlled substances or a person(s) engaging or promoting the commercial sexual abuse of a minor. Law enforcement do not have to obtain two party consent or a warrant in these situations if at least one-party consents to the recording and there is reasonable suspicion that the consenting party is in danger.

The *software that records an officer's live location* is used to monitor officer safety in potentially dangerous situations. While there are multiple sections of the SIR stating that SPD can use Callyo to track a suspect's location, SPD reports that they only use a Callyo software that tracks an officer's location while the officer is using the technology.

Recommendation 1: Update the SIR

In collaboration with the unit specific technology expert(s), SPD should update the Callyo Surveillance Impact Report to ensure that it accurately identifies and describes the multiple Callyo applications, their capabilities, and the units that use them.

Reporting Limitations

The efficacy of Callyo and safety of those who use it is highly dependent on maintaining confidentiality of this technology and the manner of use. To complete this assessment, SPD has provided all information and access deemed necessary by OIG for appropriate oversight. This report is intended to provide information necessary to demonstrate there is proper oversight and knowledge about the use of Callyo, while maintaining confidentiality of certain information for safety considerations.

SECTION A Frequency and Patterns of Use

SMC 14.18.060, § A: How surveillance technology has been used, how frequently, and whether usage patterns are changing over time.

Patterns of Use

In 2024, Callyo was rarely used, and all uses were authorized in compliance with state law. Callyo technology can be used in a case multiple times. Callyo was used a total of ten times in eight cases in 2024.

Purpose of Use

ICAC accounted for about 80% of all Callyo deployments. As a result, in 2024, most of the deployments of Callyo were for cases involving child exploitation. Outside of ICAC deployments, Callyo was used in an Intelligence investigation involving the illegal sale of goods. In the remaining case, TESU approved Callyo for a Community Response Group (CRG) case involving the sale of a controlled substance.

The SIR documents community concerns that SPD may use voice recognition or authentication technologies in conjunction with Callyo. TESU staff asserted that SPD does not use or approve use of voice recognition technologies.

SECTION B

Data Sharing with External Partners and Other Entities

SMC 14.18.060, § B: How often surveillance technology or its data are being shared with other entities, including other governments in particular.

TESU only shares data with the investigative officer. Once an investigation has concluded, TESU extracts data onto a disc for evidence purposes, in a secure facility where all access is logged. After extraction, TESU reports that all data are removed from the software. While TESU does not share or retain any records, records may be shared with other external entities throughout the investigation process by case officers. ICAC shares evidentiary data with prosecutors as part of the criminal justice process.

Records created by this technology may be shared with the following entities:

- 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

SECTION C

Data Management and Safeguarding of Individual Information

SMC 14.18.060, § C: How well data management protocols are safeguarding individual information.

SPD Process for Accessing Callyo

Personnel who can grant access to Callyo are limited, providing a control to decrease the likelihood of unauthorized access to or use of the technology. To access Callyo, a virtual telephone line must be created in the Callyo system, which generates a unique phone number. Virtual telephone lines can only be created by the TESU officer who manages Callyo, so all units, including ICAC, must submit a request form to TESU to request the creation of a line. The TESU officer who manages Callyo access is responsible for reviewing and verifying that officers have satisfied the authorization requirements. After a request is approved TESU logs the authorization and creates the telephone line in the Callyo system.

Once a line is created, all officers, except for ICAC, must physically meet with the TESU manager to register to use the software. Once the software is downloaded, the officer must log into Callyo through a secure pin provided by TESU. While ICAC officers must submit a request form to gain a telephone line, they do not need to meet with TESU to gain a secure pin to log in. Instead, ICAC has one manager who can grant other ICAC officers a secure pin. This can only be done after the ICAC manager has been authorized by TESU to use the technology in the process described above.

Data Retention

TESU personnel report that they delete all Callyo records once evidence has been extracted and preserved, as described in Section B. This includes deleting the virtual telephone line, so that the telephone number created by Callyo is no longer active. TESU reported that the vendor uses cloud storage and retains individual data indefinitely, unless the department requests that the data be deleted. TESU reported that once data is deleted on their interface at the end of an investigation, the vendor also deletes the corresponding data from their cloud server.

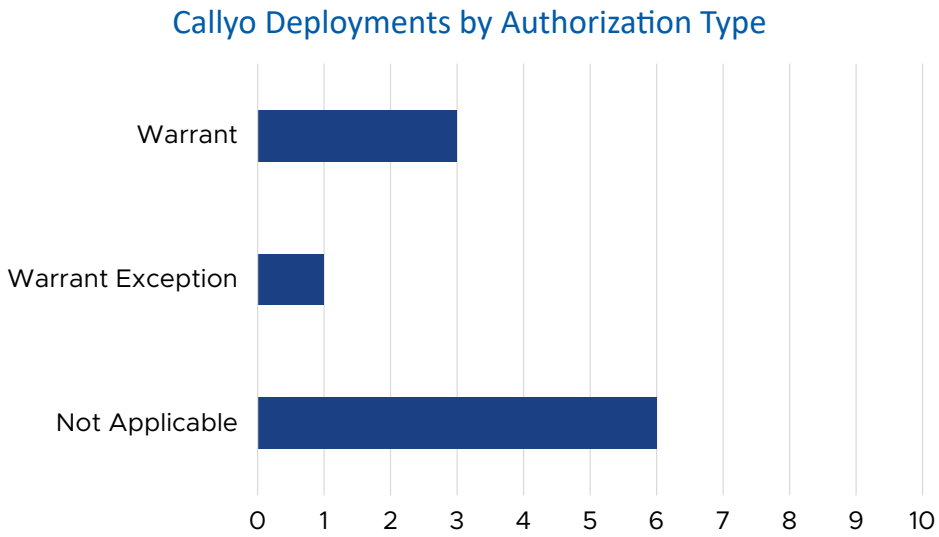
SECTION D

Impact on Civil Liberties and Disproportionate Effects on Disadvantaged Populations

SMC 14.18.060, § D: How deployment of surveillance technologies impacted or could impact civil liberties or have disproportionate effects on disadvantaged populations (…).

As stated in the Technology Description, the authorization required to use Callyo depends on the application used. The authorization requirements for each software are not clearly articulated in the SIR. For example, SIR Section 1.2 states that Callyo is only used when subject to a court order, but there is a Callyo software application that does not require a warrant or warrant exception to be deployed—The investigative phone does not require a warrant or warrant exception because law enforcement relies on the suspect willingly engaging in conversation.

As a result of deploying the virtual investigative phone, the majority of Callyo deployments in 2024 did not require authorization. Three deployments were authorized by a warrant, and one case was authorized by a warrant exception. TESU's authorization log did not contain records for the use of the software that tracks an officer's location.



*One Callyo application does not require an authorization type because it relies on a suspect's willingness to participate in conversations and does not record audio.

Provided that this technology is used as reported—In compliance with state law, rarely deployed, and primarily deployed in cases involving child exploitation, OIG does not expect use of this technology to improperly impact civil liberties or have a disproportionate effect on disadvantaged populations.

Callyo SIR Inaccuracies

While OIG found that all documented Callyo approvals were in compliance with state law, there are inconsistencies in the SIR surrounding Callyo's use and approval. Multiple sections of the SIR state that HRVU does not use Callyo audio recording technology, however, OIG reviewed logs that document ICAC's use of both the investigative phone and the audio recording software. The SIR states that HRVU logs all uses of Callyo, however, as explained in Section C of this report, all Callyo deployments are logged by TESU- including the use of the investigative phone.

Multiple sections of the SIR also assert that Callyo is only used pursuant to a court order or warrant. While the description could reasonably include recognized warrant exceptions, it does not accurately address use of the investigative phone.

Recommendation 2: Update the SIR

In collaboration with the unit specific technology expert(s), SPD should update the Callyo Surveillance Impact Report to ensure that it accurately identifies and describes the multiple Callyo applications, their capabilities, and the units that use them.

SECTION E Complaints, Concerns and Other Assessments

SMC 14.18.060, § E: A summary of any complaints or concerns received by or known by departments about their surveillance technology and results of any internal audits or other assessments of code compliance.

Customer Service Board Comments

In 2024, there were no relevant Customer Service Board (CSB) complaints filed pertaining to this surveillance technology.

Office of Police Accountability Complaints

In 2024, there were no relevant Office of Police Accountability (OPA) complaints filed pertaining to this surveillance technology.

Internal Audits/Assessments

No internal audits or assessments of this surveillance technology were conducted in 2024.

SECTION F Total Annual Costs

SMC 14.18.060, § F: How surveillance technology has been used, how frequently, and whether usage patterns are changing over time.

TESU purchased a 3-year contract for Callyo in 2022 totaling $22,027.95 that includes cost of the technology for all SPD units. This contract expires in 2025, as a result, there were no direct costs for Callyo in 2024.

Non-Audit Statement This review was not conducted under Generally Accepted Government Auditing Standards (GAGAS); however, OIG has followed GAGAS standards regarding the sufficiency and appropriateness of evidence.

Appendix A SPD Management Recommendations Response

1. In collaboration with the unit specific technology expert(s), SPD should update the Callyo Surveillance Impact Report to ensure that it accurately identifies and describes the multiple Callyo applications, their capabilities, and the units that use them.

SPD Management Response

■ Concur ☐ Do Not Concur

Estimated Date of Implementation: 11/15/2025

Proposed Implementation Plan: SPD's understanding is that the requested clarification will not require a material change and can be completed with notice to City Council and City Clerk updating the SIR.

2. In collaboration with unit specific technology expert(s), SPD should update the Callyo Surveillence Impact Report to clearly documentthe authorization requirements for each Callyo application SPD uses.

SPD Management Response

■ Concur ☐ Do Not Concur

Estimated Date of Implementation: 11/15/2025

Proposed Implementation Plan: SPD's understanding is that the requested clarification will not require a material change and can be completed with notice to City Council and City Clerk updating the SIR.