

MEMORANDUM

DATE: [xxx]
FROM: City of San Diego Privacy Advisory Board
TO: The Honorable Council President Elo-Rivera and Members of the San Diego City Council
RE: San Diego Police Department's Proposal for Callyo Covert Cloud-Based Mobile Application

I. RECOMMENDATION

The Privacy Advisory Board (PAB) recommends that the City Council approve the proposal with modifications as indicated below.

II. RECOMMENDED MODIFICATIONS

The PAB reviewed the San Diego Police Department's (SDPD) Callyo Surveillance Impact Report, proposed Use Policy, responses to PAB questions, policies from other jurisdictions, and court cases related to this technology. On March 7, 2024, SDPD provided written responses to PAB questions and answered follow-up questions about this technology ("SDPD Response"). The PAB recommends that content from these answers be incorporated into the Use Policy and Surveillance Impact Report to provide the City and the public additional details. Below we provide more detailed guidance, extracting information from the SDPD Response and providing recommendations about placement of information in the current Use Policy.

A. DESCRIPTION: The TRUST Ordinance requires specific information about the technology, including the manufacturer and product descriptions. These are missing from the current Surveillance Impact Report and Use Policy. The SDPD Response states that the manufacturer of the technology is Motorola subsidiary Callyo. The Surveillance Impact Report and Use Policy must be updated to provide this information.

B. PURPOSE:

1. **Legal authority:** This technology is used to covertly create audiovisual recordings as well as recordings of texts and multimedia messages. The proposed Use Policy allows for recordings of any communications related to "persons suspected of engaging in criminal activity," which is a substantially broad allowance covering minor offenses and mere suspicions. Although consent is not required under California law, other jurisdictions do require warrants prior to using Callyo, including Seattle and Massachusetts State Police;¹ Santa Clara County's use policy states that they will seek a warrant where required. The PAB recommends that Council consider a potential court order requirement prior to use of intrusive technology such as Callyo to safeguard against misuse. As SDPD notes for other technologies, "[l]egal authority [for use]

¹ See "[2021 Surveillance Impact Report Callyo](#)," Seattle Police Department. In Massachusetts, this was due to an Appeals Court ruling that a warrant was required for secretly acquired oral communications. See *Commonwealth v. Thanh Du*, [103 Mass. App. Ct. 469](#) (2023). See also "[State, Boston police caught using high-tech surveillance gadgetry without a warrant](#)," *Boston Globe*, Oct. 26, 2023.

can help mitigate privacy concerns by providing a clear legal framework for how the device can be used, who can use it, and under what circumstances. By establishing legal guidelines, law enforcement agencies can help ensure that the use of [technology] is lawful, ethical, justified and respectful of individual privacy rights.” Our recommendation goes above state requirements but is in line with practices around the country and is more protective of communication privacy. For cases where a secretly acquired oral communication is necessary, SDPD can obtain a court order if the requirement is endorsed by Council.

2. Clarification: The following should be deleted from the purpose of use: “audio [or audiovisual] recordings of law enforcement personnel, undercover operators [...] who engage with persons suspected of engaging in criminal activity ~~or are involved in policy activity.~~”
- C. **ALL SECTIONS:** As with all other use policies submitted by SDPD to date, the Use Policy must be modified in relevant sections to use limited lists. Currently, the policy uses open language. This indicates that there may be other, unlisted examples. To the maximum extent possible, the Use Policy should have exclusive lists.
 - D. **USE:** This section must be updated to provide authorized and prohibited uses. Currently, it indicates the capabilities of the technology, rather than allowable and prohibited uses. For example, the use section should specifically prohibit personal and non-law enforcement uses of the technology. A clear example can be found in the Santa Clara County Sheriff’s Use Policy for the same technology.²
 - E. **DATA ACCESS:** This section must be modified to limit access to those involved in a specific investigation or action. The section currently allows access by anyone in the police department, regardless of nexus to the particular investigation. The “unless otherwise authorized” language must also be amended to include non-law enforcement subjects who are authorized to use this technology, as referenced in the SDPD Response.
 - F. **DATA PROTECTION:** This section currently only mentions encryption of data at rest; it must be modified to include information about security of the data in transit.
 - G. **TRAINING:** The Use Policy must be modified to include training on the Policy itself.
 - H. **AUDITING AND OVERSIGHT:**
 1. The Use Policy must be modified to provide information about who does audits of SDPD uses of this technology and who has oversight of uses. The current document does not specify any auditing requirements except for logging of access.
 2. The following addition is also recommended: “Misuse of the system, data, or recordings must be reported to and investigated by the Department’s Internal Affairs unit.”
 - I. **MAINTENANCE:** The following language from the SDPD Response must be added to this section: “The Robbery Unit shall maintain the Callyo CBMA. The Special Equipment Officers assigned to the Robbery Units shall work with the vendor to ensure the

² Santa Clara County Office of the Sheriff, “Surveillance Use Policy for the Callyo Mobile Bug.”
<https://countyexec.sccgov.org/sites/g/files/exjcpb621/files/Office%20of%20the%20Sheriff%20-%20Callyo%20Mobile%20Bug%20%28August%202018%29.pdf>

technology's security features are updated as soon as they are available. The Special Equipment Officers shall also review the user lists bi-annually to ensure the accounts are still assigned appropriately to users having an investigative need for the technology."

- J. **IMPACT:** The Surveillance Impact Report is unclear whether the statement "uses and deployments of surveillance technology are not based on upon discriminatory or viewpoint-based factors" is an assurance or a statement of fact based on available data. The Report should be updated to clarify.
- K. **MITIGATIONS:** The Surveillance Impact Report must be updated to include specific mitigations in place to avoid capturing audio/video of related individuals, as noted in the SDPD Response.

For the above stated reasons, the Privacy Advisory Board respectfully recommends that the City Council **approve the proposal** with the modifications stated.

Cc: SDPD Chief Nisleit

Chloe Madison

CONFIDENTIAL DRAFT