Surveillance Use Policy

Covert Cloud-Based Mobile Application
San Diego Police Department

PURPOSE

The San Diego Police Department utilizes a covert cloud-based mobile application (CBMA) and software for audiovisual recording, audio recording, GPS location, and recording of text/multimedia messages. The current vendor used by the SDPD is Callyo. A CBMA is designed to create objective, real-time recordings and documentation to develop and further investigations, and to protect undercover operators at-risk during sensitive investigations.

USE

The CBMA can be used for audio recordings of law enforcement personnel, undercover operators, victims, and witnesses who engage with persons suspected of engaging in criminal activity. This also includes real-time audio monitoring and GPS location by law enforcement officers, which provides additional security and safety to undercover operators.

CBMA shall only be used for official law enforcement business. No personal use is authorized.

The CBMA can be used for audiovisual recordings of law enforcement personnel, undercover operators, victims, and witnesses who engage with persons suspected of engaging in criminal activity. This also includes real-time audiovisual monitoring by law enforcement officials, which provides additional security and safety to the undercover operators.

The device may be housed in such a way that the identity of the device is not immediately recognizable or is hidden or otherwise concealed.

Before the CBMA is used in a specific investigation, a new case is started in the data management platform. This is for tracking and for later retrieval and downloading of the recorded material.

The SDPD member who is assigned access to the CBMA is required to download the necessary audiovisual and/or audio recordings, collect the recordings and categorize the recordings as evidence per D.P. 3.02 Impound, Release, and Disposal of Property Evidence and D.P. 3.26 Media Evidence Recovery and Impounding / Preserving Procedures.

Department procedures associated with vehicle tracking devices are:

- 3.02 - Impound, Release, and Disposal of Property Evidence
- 3.26 - Media Evidence Recovery and Impounding / Preserving Procedures.

DATA COLLECTION

CBMA is a mobile application that can record audio, audiovisual, and text conversations including photos and video attachments. It can also provide GPS locations of the undercover operator when an application is in use but does not record the GPS locations. The devices do not have any filtering capabilities and the data files are saved as complete and whole to provide to the District Attorney and used in the discovery process, as detailed in the California Evidence Code.

All data gathered by the CBMA are for the official use of SDPD.

CBMA can only be operated on a device where the owner of the device has control of it and must manually start the recording process.

Once the recording and the investigative operation are complete, the recorded files will be downloaded from the data management platform to an external media device for impound per D.P. 3.02 Impound, Release, and Disposal of Property Evidence and D.P. 3.26 Media Evidence Recovery and Impounding / Preserving Procedures.

DATA ACCESS

Personnel authorized to use CBMA, the data management platform, or access the real-time monitoring through the use of such equipment shall be specifically trained in such technology and authorized by the Chief of Police, or designee. Such personnel shall be limited to designated captains, lieutenants, sergeants, officers, detectives, and police department personnel unless otherwise authorized.

Those who are administrators for the CBMA have access to all recorded data for auditing, requested deletions, and assistance to authorized users.

DATA PROTECTION

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment, selecting and approving technology solutions. Cyber security and technology risks are also assessed by the Department of IT. For additional details related to IT governance processes, refer to the information at the following link:

- https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf

The recorded files collected using CBMA are stored via encrypted technology in the Amazon government-classified domain and not on the device. Once the investigation is complete, the recorded files are to be downloaded from the data management platform and physically impounded. All such evidence is controlled and regulated per D.P. 3.02 Impound, Release, and Disposal of Property Evidence and D.P. 3.26 Media Evidence Recovery and Impounding / Preserving Procedures.

Those authorized to have access to CMBA can view the data on the data management platform of only the cases they created. All other authorized users of CMBA can monitor recordings in real-time and cannot access previously recorded data on the platform of other law enforcement officials' cases.

The data management platform is only accessible via a username/password and two-factor authentication. To monitor the recordings in real-time, it is protected by username/password security credentials.

DATA RETENTION

After the case is completed, the recorded files are downloaded from the data management platform and physically impounded for evidence. Once the authorized user has impounded the recorded files physically, the authorized user will request the recorded files be deleted from the data management platform and select "completed case" as the reason. The request will be sent to the Robbery

Administrator who will know that "case completed" signifies the evidence was downloaded and retained for evidence. The recorded files will then be deleted.

PUBLIC ACCESS

The general public has no access to CBMA or any data collected by the device.

Once the authorized user has impounded the recorded file physically, evidence retention and access are the responsibility of the SDPD Property Unit and all such evidence is controlled and regulated by SDPD Procedure 3.02 – Impound, Release, and Disposal of Property, Evidence and Articles Missing Identification marks.

THIRD PARTY DATA SHARING

Recorded files may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes, which includes criminal investigations and prosecution as allowed by law. The recorded files will not be used in immigration enforcement.

TRAINING

Individualized or group training is provided by Robbery Unit personnel before access is granted to CBMA. This training shall include a review of the Use Policy for this technology. Familiarity with the operation, data management and real-time monitoring are also included in the training. Authorized users also have access to on-demand training videos to review operations and data management.

AUDITING AND OVERSIGHT

Personnel who are authorized to use CBMA shall ensure their access and use of the device complies with the Surveillance Use Policy. As with all uses of Department or City Computer Systems, the use of CBMA must be in accordance with DP 1.45 – Use of City or Department Computer Systems.

A log shall be maintained of personnel who required access and use of CBMA during an investigation. The log shall be available for presentation for all required internal and external audits, and oversight will be maintained by the system Program Manager or their designee.

The Robbery Unit shall maintain CBMA. The Special Equipment Officers assigned to the Robbery Unit shall work with the vendor to ensure the technology's security features are updated. 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.

MAINTENANCE

SDPD shall maintain robust security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect the covert audiovisual information from unauthorized access, destruction, use, modification, or disclosure.

The Robbery Unit shall maintain CBMA. The Special Equipment Officers assigned to the Robbery Unit shall work with the vendor to ensure the security features of the technology are updated. 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.