Surveillance Use Policy

Cellebrite ~~Universal Forensics Extraction Device (UFED)~~Inseyets
San Diego Police Department

PURPOSE

Cellebrite Inseyets is a suite of ~~'s~~ mobile device ~~extraction~~ forensics tools, ~~currently~~ previously referred to as the Universal Forensics Extraction Device (UFED) platform.~~,~~ Cellebrite Inseyets tools are used to extract data from evidentiary mobile devices, analyze that data, and generate reports for review in a criminal investigation.

Cellebrite~~'s tools~~ Inseyets has~~ve~~ two primary functions:

- Forensic data extraction from mobile devices via software installed on department computers ~~or standalone proprietary hardware, and is secured the same way as any other PC based software~~
- Data extraction analysis via software installed on department computers, and is used to categorize extracted data into readable reports for assigned investigators.

USE

When proper legal authority, as defined by the California Electronic Communications Privacy Act [ECPA; SB 178 (2016) codified in Penal Code 1546.1], is obtained, cell phones are connected to one of the Cellebrite tools, and the data is extracted from the phone. ~~The~~ Cellebrite ~~tools~~ Inseyets is~~are~~ designed to complete extractions without altering any of the data or adding data to the phone. Most of the time, there is no way to limit what data is extracted using the Cellebrite technology; extractions are usually all-or-nothing. However, a limited number of devices with specific operating systems may be eligible for limited extractions if the passcode to unlock the device is known, or no passcode is enabled on the device.

Due to the large variety of cell phone models and manufacturers, not all cell phones can be extracted. Only phones that the vendor supports can have data extracted.

DATA COLLECTION

Cellebrite Inseyets can extract call logs, text messages, emails, photos, videos, contacts, browsing history, app data, location data, and more. Cellebrite Inseyets can also extract data from many social media apps, such as Facebook Messenger, Instagram, and Snapchat, on the phone. The applications that can be extracted depend on a number of factors, including the device's make, model, operating system, and security updates.

Cellebrite~~'s software~~ Inseyets can also analyze deleted data and hidden files on a device, and can recover data that has been deleted.

The extracted data is then stored on the department's Network Attached Storage (NAS) in D~~d~~ata ~~s~~Systems. Only investigators with ~~a search warrant~~proper legal authority can access the data controlled by Data Systems.

DATA ACCESS

Only ~~Criminalists in the FTU that have been trained and authorized by the Quality Manager to perform extractions, as well as police officers/detectives that have been trained by FTU,~~trained and authorized

users may use Cellebrite software. FTU issues each trained officer/detective a personal log-in and secure folder on the network for them to store their extracted data and reports. The secure folder is accessible only by the user's personal log-in; no other user may access it.

If an investigator is not certified to use the technology, they may submit a laboratory request to have the device extracted in the lab.

Extracted data is accessible only by the ~~extraction trained officer/detective/FTU criminalist~~extractor and the requesting investigator. Extracted data is stored on SDPD networks which are managed by the FTU and IT/Data Systems analysts.

The resulting report(s) generated from extracted data are only reviewed when proper legal authority has been obtained to review those report(s).

DATA PROTECTION

Cellebrite ~~software and equipment are~~Inseyets is stored, secured, and maintained at~~in the FTU, a secured office within~~ Police Headquarters. Only authorized users have access to the technology. Each user is required to use a unique login and password to access the software and conduct data extractions.

~~The~~ Cellebrite ~~software~~ Inseyets is not located on department network computers and can only be accessed by logging in to a computer with the software installed inside the building. ~~-~~ These computers are not accessible by the vendor. Additionally, the software can only be installed through a specific process. It cannot be moved, and the user must be an authorized user with a valid software license. ~~The~~ Cellebrite Inseyets~~software~~ cannot be accessed outside of the Department.

DATA RETENTION

Other than homicides and violent sexual assaults, where extracted data is kept indefinitely, extracted data is retained based on the statute of limitations for the associated crime or if the case has been adjudicated. Data is purged from the NAS at the end of its retention period.

PUBLIC ACCESS

The data extracted using Cellebrite ~~technology~~ Inseyets is only used in criminal investigations and is not available to the public. ~~-~~Copies of the data can only be obtained with a court order or the discovery process.

THIRD PARTY DATA SHARING

Data that has been extracted using Cellebrite ~~technology~~ Inseyets is not shared without a court order or other legal proceedings such as discovery. ~~-~~The extracted data is considered confidential, and there is no third-party access or sharing. Cellebrite does not have access to the extracted data.

TRAINING

Surveillance Use Policy

Cellebrite ~~Universal Forensics Extraction Device (UFED)~~Inseyets
San Diego Police Department

Authorized users in the FTU ~~criminalists~~ must successfully complete an in-house extensive training program comprised of: literature review; lectures; practical exercises; shadowing; passing a written test, practical tests, and moot court; and completing supervised casework. The training program, which is outlined in the FTU manual,~~-~~ complies with the American National Standards Institute (ANSI) National Accreditation Board's (ANAB) International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17025 Forensic Testing Laboratory standards. To satisfy the on-going requirements of ANAB accreditation, ~~FTU criminalists~~authorized FTU users are also required to pass annual proficiency tests for each technology utilized.

~~Officers/detectives must complete the~~ FTU's Cellebrite training course must be completed before access to ~~the~~ Cellebrite ~~tool~~ Inseyets is authorized to any other individual.

AUDITING AND OVERSIGHT

As an ANAB-accredited forensic testing laboratory, FTU is extensively audited annually to ensure that all policies and procedures are followed, and in accordance with the standards set by ANAB. One portion of this is specifically dedicated to auditing a random sampling of each FTU ~~criminalist's~~ user's usage of the tools. Prior to its initial usage in casework, the tool's capabilities and limitations were assessed in a comprehensive validation study. It was approved for casework by the FTU Technical Lead and Crime Laboratory Quality Assurance (QA) Manager. All updates to the software are verified prior to use in casework by FTU analysts. FTU ~~criminalists~~ users also must annually pass a proficiency exam utilizing the Cellebrite technology. All qualification records are maintained by the Crime Laboratory's QA Manager.

The Crime Lab's Administrative Support Unit and the FTU supervisor (or designee) ensure that legal authority to search each device is valid. The FTU supervisor authorizes the use of the tools each time a device is assigned to an FTU ~~criminalist~~ user for extraction/analysis. The performance of each tool is monitored by each FTU ~~criminalist~~user, and oversight of the performance of all tools is maintained by the FTU Technical Lead. Every tool usage by an FTU ~~criminalist~~ user is audited by another qualified FTU ~~criminalist~~ user and the FTU supervisor (or designee).

SDPD's Research and Planning Unit audits equipment utilized by FTU annually.

~~The~~ Cellebrite ~~technology~~ Inseyets resides in the FTU and in a mobile device extraction room for authorized SDPD ~~officers/detectives~~personnel. Both rooms are inside the SDPD Headquarters building and can only be accessed via key card. Key card access logs are audited annually.

~~Officers/detectives~~ Non-FTU SDPD personnel ~~who are trained and~~are authorized to use ~~the~~ Cellebrite ~~technology~~ Inseyets ~~have received~~after they obtain approval from the Crime Laboratory's Commanding Officer and ~~after~~ training is completed by ~~the~~ FTU. Key card access is then granted to the mobile device extraction room ~~for SDPD officers/detectives~~. FTU is responsible for maintenance of all Cellebrite software, as well as granting access to the Cellebrite system. FTU maintains a log of all authorized Cellebrite users that tracks how many times the software was accessed by the user. Every tool usage by a trained ~~officer/detective~~user is audited by ~~an~~ the FTU ~~criminalist~~.

FTU and IT/Data Systems are the administrators of the mobile device extraction networks. Network security is monitored on a daily basis for unauthorized activity, and regular maintenance is performed.

Data is only extracted with proper legal authority. Department policies, State of California laws, and laboratory policies outline how extracted data is maintained. Misuse of the system, data, or resulting reports must be reported to and investigated by the Department. Violations of the laws, Departments policies or user agreement terms would subject the department member to discipline and/or criminal proceedings or civil processes.

MAINTENANCE

~~The~~ Cellebrite ~~software~~ Inseyets is controlled and maintained by the vendor and FTU, following laboratory quality policies and department policies. FTU ~~criminalists are~~ is responsible for monitoring and updating software when new versions are released. A log documenting all software updates is maintained by the FTU.