Surveillance Use Policy

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

PURPOSE

Cellebrite Universal Forensics Extraction Device (UFED) is used to extract cell phone data by the Forensic Technology Unit (FTU).

Cellebrite makes UFED software available on two different platforms:

- The UFED 4PC: Extraction software installed on department computers and is secured the same way as any other PC-based software
- The UFED Touch: Standalone proprietary hardware with UFED software installed

The UFED Touch and 4PC perform the same function.

Once the data is extracted, the UFED Physical analyzer, part of the Touch and 4PC software, is used to categorize extracted data into readable reports for assigned investigators.

- Additional information can be found in the Laboratory Ops Manual 2020

USE

When proper authority, such as a search warrant or consent form, is obtained, cell phones are connected to the Cellebrite tool, and the data is extracted from the phone. Cellebrite is designed to complete the extraction without altering any of the data or adding data to the phone.

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

DATA COLLECTION

Cellebrite can extract call logs, text messages, emails, photos, videos, contacts, browsing history, app data, and location data. Cellebrite can also extract data from some social media apps on the phone.

Cellebrite's software 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 data systems. Only investigators with a search warrant can access the data controlled by Data Systems.

DATA ACCESS

Only Criminalists in the FTU, police officers, and detectives that have been trained and certificated by Cellebrite and have been authorized by the Quality Manager to perform extractions may use Cellebrite software.

All new users must be manually entered into the Cellebrite software by FTU before being given access to the system.

Trained investigators are authorized to use Cellebrite to conduct an extraction. However, if an investigator is not certified to use the technology, they may submit a laboratory request to have the device extracted in the lab.

DATA PROTECTION

Cellebrite software and equipment are stored and maintained 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 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 have no internet access and 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 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 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 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

Training via Success Factors is required prior to an officer or detective getting a unique log-in and username from FTU to use the Cellebrite Software. Criminalists in FTU who use the Cellebrite software must complete and pass an extensive training program outlined in the FTU manual prior to using the software.

AUDITING AND OVERSIGHT

FTU maintains a log of all authorized Cellebrite users that tracks how many times the software was accessed by the user. FTU is also responsible for all Cellebrite software and granting access to the system.

Data is only extracted via legal authority, such as an active warrant. Department policies, State of California laws, and laboratory policies outline how extracted data is maintained. Misuse of the system

would be reported to and investigated by the Department's Internal Affairs unit. 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 is controlled and maintained by the vendor and FTU, following laboratory quality policies and department policies. FTU criminalists are responsible for monitoring and updating software when new versions are released. A log documenting all software updates is maintained by the FTU.