DEPARTMENTAL GENERAL ORDER

I-30: UNIVERSAL FORENSIC EXTRACTION DEVICE

Effective Date:

Coordinator: UFED Coordinator, Criminal Investigations Division

---

UNIVERSAL FORENSIC EXTRACTION DEVICE OR UFED

The purpose of this order is to establish Departmental policy and procedures for the use of Universal Forensic Extraction Devices (UFED).

A. VALUE STATEMENT

The purpose of this policy is to establish guidelines for the Oakland Police Department's use of UFEDs, for the extraction and analysis of data from mobile devices.

B. Purpose of the Technology: *The specific purpose(s) that the surveillance technology is intended to advance*

UFEDs are currently produced by Cellebrite, a third-party private company. UFEDs are designed to extract data from mobile phone devices to access data related to investigations. OPD investigations are supported by extracted phone data related to criminal activity and/or internal police misconduct involving OPD-issued mobile phones. OPD seeks to use UFEDs to extract and preserve mobile phone data in a forensically sound condition so that the data can later be presented in court as admissible evidence.

C. DESCRIPTION OF THE TECHNOLOGY

A UFED is consists of (1) physical ports that connect to common mobile phones (e.g., Apple and Android operating system phones); (2) a computer memory storage and transfer module to extract phone data to upload to a computer; and (3) software language "Cellebrite Physical Analyzer" or "PA" that communicates with the phone to gain digital access to phone data; and physical analyzer software that parses and indexes the data so it's searchable and more comprehensible for investigators. The software automates a physical extraction and indexing of data from mobile devices.

D. Authorized Use: *the specific uses that are authorized, and the rules and processes required prior to such use*

1. UFEDs may be used to investigate the contents of OPD-issued phones, used by OPD personnel, without a search warrant and without permission by the user of the phone, in accordance with DGO I-19: "Electronic Communication Devices.
   a. DGO I-19, Section D "Inspection And Auditing Of Department Cellular Phones And Electronic Devices," explains, in part that:
      i. ***Audit*** *– audits of work cell phones include using a digital forensic tool to extract the entirety of the data stored on the phone, including deleted data, for the purpose of reviewing the device for policy compliance. Audits involve an expanded scope and significantly more intensity than inspections and will typically have a planned review to significantly sample and examine the data extracted from the device.*
      ii. ***Search*** *– searches are a focused attempt to find something (e.g. evidence of misconduct or criminal activity, or specific communication that could prove or disprove an allegation of misconduct) that could reasonably exist on the device. The scope and intensity of a search, and the use of digital forensic tools will depend on what is being searched for.*
   b. DGO I-19 Section D.2, "Right of Department to Inspect Work Cell Phones and Electronic Devices at Any Time," explains that OPD may inspect, audit, or search work OPD-issued work phones and electronic devices at any time.
   c. DGO I-19 Section D.3 explains that the OPD Bureau of Risk Management (BRM) will develop an inspection plan for random OPD-issued mobile phone inspections.
   d. Any investigation of OPD-issued phones and/or telephonic devices shall only occur with approval from a Commander (rank of Lieutenant or higher) of the Internal Affairs Division (IAD), or BRM.
   e. Use of OPD-issued phones is governed by all relevant OPD mobile phone and telephonic device policies.
   f. Only OPD sworn personnel designated as an OPD IAD UFED Coordinator and/or personnel designated by the IAD UFED Coordinator (see Training Section below for training requirements) may utilize the UFED technology.

2. UFEDs are sanctioned for use, without the verbal or written consent of the owner of the phone, as part of criminal investigations only when the following conditions have been met:
   a. Only OPD sworn personnel designated as an OPD UFED Coordinator and/or personnel designated by the UFED Coordinator (see Training Section below for training requirements) may utilize the UFED technology.
   b. An OPD Commander (lieutenant or above rank) must first authorize the search warrant to utilize UFED for a phone search. The request for a search warrant to utilize UFED must be part of an active criminal investigation
   c. The search warrant to access personal electronic information from a mobile telephone must be authorized by a judge pursuant to Chapter 3 (Search Warrant) of the California Penal Code

e. A search warrant must be approved in accordance with (PC 1546.1(c)(6)) as part of the California Electronic Communications Privacy Act ("CalECPA")[1] The Search Warrant must demonstrate probable cause to target someone's digital information and show "with particularity the information to be seized by specifying the time periods covered and, as appropriate and reasonable, the target individuals or accounts, the applications or services covered, and the types of information sought."

f. CalECPA (PC 1546.1(c)(6)) provides that OPD personnel, otherwise following the procedures listed here for authorized use, may use UFED to access the contents of a phone without a search warrant, if personnel, in good faith, believe that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information.

i. The UFED Coordinator shall create a report explaining the nature of the exigent emergency circumstance justifying the use of UFED. This report shall be maintained with other UFED uses.

3. UFEDs are sanctioned for use, without the verbal or written consent of the owner of the phone, if the authorized possessor of the phone is confirmed to be on parole or probation with a valid electronic device search cause, in compliance with OPD Policy DGO R-02, only when the following conditions have been met:
   - Only OPD sworn personnel designated as an OPD UFED Coordinator and/or personnel designated by the UFED Coordinator (see Training Section below for training requirements) may utilize the UFED technology.
   - The probation or parole search to utilize UFED must be part of an active criminal investigation.

4. UFEDs are sanctioned for use in alignment with CalECPA rules, with the verbal or written consent of the owner of the phone, as part of investigations, only when the following conditions have been met:

   a. Only OPD sworn personnel that have completed UFED training requirements and/or personnel designated by the UFED Coordinator may utilize the UFED technology.
   b. The request for a search warrant to utilize UFED must be part of a criminal investigation.
   c. The UFED Coordinator shall create a report explaining the reasons for the phone search and describing the nature of the consent given for the search in a report. It is highly preferred that OPD obtain and maintain a record of written consent prior to conducting a consent search of an electronic device. This report shall be maintained with other UFED uses.

[1] (PC 1546.1(c)(6)) was established with the passage of Senate Bill (SB) 178, also known as the California Electronic Communications Privacy Act ("CalECPA") which went into effect on January 1, 2016.

E. ***Data Collection:*** *The information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data;*

UFEDs specifically collect phone content that is stored on the mobile device (not in a cloud server environment accessed by a phone), including:

- Geo-location meta data (that is stored on the phone device; some phones are configured to not store this data);
- Short Message Service (SMS) content data (including sender and receiver phone numbers) and images contained in SMS data;
- Voice Mail and phone numbers from phone call logs;
- Phone contacts data;
- Social Media application messenger data (e.g., Facebook Messenger Application or SnapChat data that is stored on the phone); UFEDs do not allow personnel to access social media platforms and access data stored on the platform;
- Phone numbers from call logs;
- Photographs, videos, notes, or other application, audio, image, and/or data stored on a phone;
- Phone browser search data (stored on the phone device)

The UFED cannot pull data stored in a cloud computer environment not physically stored in the phone.

F. ***Data Access:*** *The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information*

Only sworn personnel may utilize UFEDs in the possession of OPD as defined in the "Authorized Use" Section above. Authorized personnel in may utilized UFEDs, according to Authorized Use, for crime investigations. IAD personnel may utilize UFEDs for IAD investigations. The UFED Coordinator can provide the downloaded phone data via a physical medium (e.g., hard-drive) or via a cloud-based law enforcement evidence storage service for an OPD investigator to review the data.

UFED downloaded data shall be accessed only by the assigned investigators and/or designees as well as the assigned personnel conducting the UFED phone download.

The approved request is retained on file.

G. ***Data Protection:*** *The safeguards that protect information from unauthorized access, including encryption and access control mechanisms:*

UFEDs store data on standard external computer hard drives – either rotary hard disk drives (HDD) with spinning machine-recordable platters, solid-state hard drives (SSD) or smaller flash or jump drive SSDs; UFED data may also be stored on a law enforcement evidence management storage system. UFEDs have universal serial bus and/or other standard ports to connect these storage devices. The data from a phone that is transferred to a computer hard drive storage device that can only be directly viewed from a physical analyzer program (PA) that is loaded onto a computer operating system (OS) as part of a contract with Cellebrite. Trained personnel can then view the parsed phone data. The phone data and report (two files) can then be shared via a professional document file (PDF), UFED-reader file, or HTML-type readable format via computer browser.

All hard drives from UFED phone extractions are stored with the OPD Property Section.

H. ***Data Retention*** *The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;*

Any data generated from the use of the UFED for the purpose of lawful investigations will be stored while the legal proceedings associated with the investigation is adjudicated. Any data generated from the use of the UFED shall not longer be stored following the adjudication of a court proceeding, in accordance with the statute of limitations for the particular case. Data will not be retained beyond the statute of limitations if there are no court proceedings or criminal charges filed.

I. **Public Access**: *how collected information can be accessed or used by members of the public, including criminal defendants.*

Data which is collected and retained under subsection B of this section is considered a "law enforcement investigatory file" pursuant to Government Code § 6254 and shall be exempt from public disclosure. Members of the public may request data via public records request pursuant to applicable law regarding Public Records Requests as soon as the criminal or administrative investigations has concluded and/or adjudicated.

J. Third Party Data Sharing: *if and how other city departments, bureaus, divisions, or non-city entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information.*

OPD personnel may share UFED data with other law enforcement agencies and/or a prosecuting agency at the local, state or federal level. as part of connected investigations and/or legal prosecutions. OPD personnel shall follow the same data file sharing procedures outlined above in "Data Protection." OPD personnel must provide the physical hard drive with PDF file format or UFED reader format – UFED data shall not be sent via unsecured electronic communications (e.g., email).

K. Training: *the training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, and the category of staff that will provide the training*

Cellebrite offers several levels of training for investigators to identify mobile device hardware and understand the general forensic process for the analysis of extracted device data and to generate reports using Cellebrite Reader software. OPD UFED Coordinators receive training via Cellebrite in (at least) the following two areas:

Cellebrite Certified Operator Class; upon completion of this course, trainees will be able to:

- Install and configure UFED Touch and Physical Analyzer software.
- Exhibit how to open extractions using Physical Analyzer.
- Summarize how to conduct basic searches using Cellebrite Physical Analyzer.
- Outline how to create reports using Cellebrite Physical Analyzer.
- Demonstrate proficiency of the above learning objectives by passing a knowledge test and practical skills assessment with a score or 80% or better.
- Explain the best practices for the on-scene identification, collection, packaging, transporting, examination and storage of digital evidence data and devices.
- Display best practice when conducting cell phone extractions.
- Identify functions used within UFED Touch to perform supported data extractions.

Cellebrite Certified Physical Analyst; upon completion of this course, trainees will be able to:

- Conduct advanced mobile device forensic analysis using the UFED Physical Analyzer software.
- Recall techniques used for authentication and validation of data parsed and collected as evidence.

- Identify functions within Physical Analyzer software which allow examination of various types of data.
- Recognize Physical Analyzer's capabilities to generate custom reports in an organized manner.
- Demonstrate proficiency of the above learning objectives by passing a knowledge test and practical skills assessment.

L. Auditing and Oversight: *the mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy.*

Only Cellebrite-certified officers and/or designated personnel may be considered as an OPD UFED Coordinator. Only these staff shall have Physical Analyzer software on their OPD computer.

The UFED Coordinator shall track all OPD requests and use of UFEDs for OPD investigations in their department. There may be more than one UFED Coordinator in Ceasefire, IAD and VCOC in addition to the main Coordinator in CID. The CID-based UFED Coordinator shall ultimately be responsible for ensuring that all UFED uses are tracked in on document along with investigation information so that this information will be centrally organized.

The UFED Coordinator(s) shall be responsible for reviewing all UFED uses and that each use is connected to a court-approved search warrant. Publicly releasable data (e.g., number of uses, types of investigations) shall be made available in the annual surveillance technology report which is required for presentation to the City's Privacy Advisory Commission (PAC) as well as the City Council per Oakland Municipal Code 9.64.

M. Maintenance: *The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.*

The UFED Coordinator shall ensure that OPD UFEDs are stored in a secure location with controlled access by OPD.

The UFED Coordinator shall also ensure that each UFED is maintained in working order; the OPD Cellebrite contract covers maintenance and repair; Cellebrite is responsible for hardware support if and when such support is needed. Cellebrite is also responsible for providing secure links to their servers for any Physical Analyzer software updates and UFED firmware updates.

By Order of

Darren Allison

Interim Chief of Police

Date Signed: