OAKLAND POLICE DEPARTMENT

Surveillance Impact Report: Universal Forensic Extraction Device (UFED)

A. **Description:** *Information describing the Universal Forensic Extraction Device (UFED) and how they work, including product descriptions and manuals from manufacturers.*

A UFED 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.

B. **Purpose:** *How OPD intends to use UFED Technology*

UFEDs are currently produced by Cellebrite, a 3rd 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. The Oakland Police Department (OPD) uses UFEDs for two separate purposes:

1. UFEDs may be used to investigate the contents of OPD-issued phones, used by OPD personnel; and
2. UFEDs may be used for extracting data from suspects related to criminal investigations (not relating to OPD-issued phone devices).

OPD's Internal Affairs Division (IAD) must investigate situations where there is reason to believe that personnel are using their phones to communicate messages that do not comport with the rules governing employment and/or OPD telephonic device-specific policies. Department General Order (DGO) I-30: Universal Forensic Extraction Device explains that DGO I-19 "Electronic Communication Devices" enumerates the situations in which OPD's Internal Affairs Division (IAD) and/or Bureau of Risk Management (BORM) may search OPD-issued phones to ensure their proper use.

DGO I-19: "Electronic Communication Devices," Section D "Inspection And Auditing Of Department Cellular Phones And Electronic Devices," explains, in part that:

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.*

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.*

More commonly, OPD UFED Coordinator(s) use UFEDs in support of criminal investigations where existing evidence points to a probable cause to support a search warrant – UFEDs can be used without the permission of the phone's user or owner in conjunction with a judge-approved search warrant (for cases not related to OPD-issued phones). In general, OPD most often seeks to use UFEDs with a search warrant in investigations of human trafficking or violent crime investigations.

The use of UFEDs for both internal IAD use as well as for external criminal investigations is considered a best practice is a contemporary best practice for law enforcement. UFEDs provide forensically sound evidence which is necessary for documentation, evidence discovery, criminal investigation and prosecution, and for internal investigations. Forensically sound refers to a process that collects data or metadata from an electronic device without any alteration or destruction from the source device.

C. Location: *The Locations and situations in which UFED Technology may be deployed or utilized.*

The use of UFED is not generally constrained by geographic location. Officers may use UFEDs where officers have jurisdiction to operate as sworn officers. However, DGO I:30 prohibits the use except for conditions allowed under Section D "Authorized Use."

D. Privacy Impact: *How is the UFED Surveillance Use Policy Adequate in Protecting Civil Rights and Liberties and whether UFEDs are used or deployed, intentionally or inadvertently, in a manner that is discriminatory, viewpoint-based, or biased via algorithm.*

Mobile phone use has become ubiquitous in the 21st Century and people both depend on these devices for communication but also allow great amounts of personally identifiable information (PII) on these phones as numerous phone-based applications connect phones and their users to people and platforms everywhere. Therefore, UFED technology holds the potential for massive privacy impacts should they be allowed for use without strict guidelines and use barriers.

OPD recognizes that privacy impacts from UFED usage are entirely dependent on the ways they can be used, as well as under what circumstances. Staff appreciate that UFEDs are not available to the public, and that OPD will only use UFEDs for specific law enforcement purposes articulated in DGO I:30 Authorized Use Section.

Data hacking and the unauthorized release of these phone extractions poses another potential impact from the use of UFEDs. Phone extractions from UFED – just like from other means of data acquisition – could cause negative impacts to the privacy rights and expectations of phone users. People expect that their phone extractions will remain private. UFED use must therefore comply with security procedures to mitigate against the unauthorized release of phone extractions.

OPD will only use UFEDs for non-OPD issued phones from members of the public in specific cases as related investigations, outlined in the Authorized Use Section of DGO I:30. OPD's use of UFEDs therefore will not be deployed in a manner that i*ntentionally or inadv*ertently causes bias.

E. Mitigations: *Specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each of the impacts.*

UFEDs may be used by IAD for the investigation of OPD-issued telephonic devices. Generally, OPD's Internal Affairs Division (IAD) can request the use of UFEDs without restriction to investigate OPD-issued phones operated by OPD personnel. OPD's Ceasefire Division, Criminal Investigations Division (CID) and Violent Crimes Operations Center (VCOC) staff can request the use of UFEDs only with a judge-approved search warrant. The request for a search warrant must first be approved by an OPD Commander of rank of lieutenant or higher. Part 3 of Section the Authorized Use Section of DGO I:30 explains that OPD staff do not need a search warrant if the possessor of the phone gives verbal or written consent, and that the UFED Coordinator creates a report explaining the scenario of the UFED use and documents the consent for the phone search in a report, maintained with other UFED uses.

OPD maintains security protocols explained in part G "Security" below that provide numerous mitigations against negative privacy impacts. Furthermore, DGO Part K, "Training" stipulates that OPD UFED Coordinators shall be trained by Cellebrite as Certified Operators and Certified Physical Analysts. These courses help to ensure that personnel with access to UFEDs use them as designed and take steps to ensure all data is downloaded correctly and only shared via prescribed protocols.

F. **Data Types and Sources*****:*** *A list of all types and sources of data to be collected, analyzed, or processed by the surveillance technology, including "open source" data, scores, reports, logic or algorithm used, and any additional information derived therefrom.*

Data generated from the use of UFED is preserved onto hard drives in the original file formats from the mobile phones. Once a phone is connected, the UFED tool initiates a command and sends it to the device, which is then interpreted by the device processor; the data is requested as a result of the use of proprietary protocols and queries. Data is then received from the phone's memory and sent back to the UFED and stored on an external hard drive as articulated in DGO I:30, Part G "Data Protection." For example, Short Messaging Service (SMS) messages, commonly referred to as 'texts,' can be imported and saved into an SMS file type; Multimedia Messaging Service (MMS) messages can be stored and saved as MMS files. Images are similarly extracted and stored in the same image file types (e.g., jpeg, png file types). Voice mail is commonly stored and saves as an M4A file or .wav file. Phone log files show geolocation data.

G. Data Security: *Information about the steps that will be taken to ensure that adequate security measures are used to safeguard the data collected or generated by the technology from unauthorized access or disclosure.*

DGO I:30, Part G "Data Protection" articulates the procedures OPD employs for the

security of data obtained from the use of UFEDs. 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. 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 can only be directly viewed from a physical analyzer program (PA) that is loaded onto a Windows operating system (OS) as part of a contract with Cellebrite. The data is never transmitted online via a cloud environment where the data could be possibly open to capture by a third party. The data itself is not stored on an actual computer connected to the internet; the data is kept on hard drives that are not connected to the internet.

Trained personnel can then view the parsed phone data by connecting the data on the external drive to a computer temporarily and running the PA program. The data can then be shared. 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 Evidence Section, non-attached to a computer.

H. **Fiscal Cost:** *The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding.*

OPD currently possess two UFEDs and one physical analyzer that are approximately eight years old. OPD will seek a new contract with Cellebrite should the City Council adopt a resolution to accept the UFED Use Policy in addition to a sole source contract with Cellebrite for new UFEDs. Cellebrite now offers software as a service (SAAS)-type contract. OPD is proposing a SAAS contract at approximately $90,000 per year. This type of contract will provide OPD with three devices (one for CID, one for Ceasefire, and one for IAD) with unlimited number of allowed extractions or uses.

I. **Third Party Dependence:** *Whether use or maintenance of UFED technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis.*

OPD is reliant upon Cellebrite, the sole provider of the UFED technology. There is no other 3rd party provider creating a similar product that can be used to extract phone data in a manner that have been found by courts to be forensically sound. This threshold is crucial to ensuring that evidence found on phones through procedurally just use of search warrants can be used as evidence in a court of law.

J. **Alternatives Considered:** *A summary of all alternative methods considered in-lieu of UFED, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate*

OPD officers and investigators rely primarily on traditional policing techniques to gather evidence related to criminal investigations such as speaking to witnesses and suspects. There are many cases where a suspect connected to violent crimes and/or human trafficking may not want to provide any information. At the same time,

the mobile phone used by the suspect may contain evidence that connects them to crimes OPD is tasked with trying to investigate. UFEDs provide a connection to the data on the phone where no other connection exists in the case of unwillingness to share the phone data by the phone user. In these situations, the alternative to UFED use would be to not access the data. The inability to access the phone data in some situations may result in an inability to successfully investigate violent crimes and human trafficking – a situation that negatively impacts all Oakland residents and visitors.

UFEDs also help IAD in its mandate to ensure that OPD-issued phones are used as intended according to DGO I.19. IAD and BORM need to access at times the digital content of phones to ensure compliance.

In situation where suspects or crime victims voluntarily offer the contents of their phone in the context of investigations UFEDs may be able to expedite and even find data where the phone user otherwise could not provide the data. More importantly, UFEDs allow for the phone data transfer in court-admissible forensically sound manner that is crucial for the admissibility of evidence for legal prosecutions.