



Privacy Advisory Commission
November 2, 2023 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Meeting Agenda

Commission Members: District 1 Representative: Reem Suleiman, District 2 Representative: Chloe Brown, District 3 Representative: Brian Hofer, Chair, District 4 Representative: Lou Katz, District 5 Representative: Vacant, District 6 Representative: Gina Tomlinson, District 7 Representative: Robert Oliver, Council At-Large Representative: Henry Gage III, Vice Chair, Mayoral Representative: Jessica Leavitt

Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.

1. Call to Order, determination of quorum
2. Review and approval of the draft September 7 and October 5 meeting minutes
3. Open Forum/Public Comment
4. Surveillance Technology Ordinance – OPD – Cellebrite Cellphone Data Extraction Technology
 - a. Review impact report and take possible action on a proposed use policy

Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.

Members of the public can view the meeting live on KTOP or on the City's website at <https://www.oaklandca.gov/topics/ktop-tv-10>.

Comment in advance. To send your comment directly to the Privacy Commission and staff BEFORE the meeting starts, please send your comment, along with your full name and agenda item number you are commenting on, to Felicia Verdin at fverdin@oaklandca.gov. Please note that eComment submissions close one (1) hour before posted meeting time. All submitted public comment will be provided to the Privacy Commission prior to the meeting.

Each person wishing to speak on items must fill out and submit a speaker's card to staff prior to the meeting. Members of the public can address the Privacy Advisory Commission in-person only and shall state their names and the organization they are representing, if any.

To observe the meeting via Zoom, go to: <https://us02web.zoom.us/j/85817209915>
Or One tap mobile: +1 669 900 9128



Privacy Advisory Commission
September 7, 2023 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
DRAFT Meeting Minutes

Commission Members: District 1 Representative: Reem Suleiman, District 2 Representative: Chloe Brown, District 3 Representative: Brian Hofer, Chair, District 4 Representative: Lou Katz, District 5 Representative: Vacant, District 6 Representative: Gina Tomlinson, District 7 Representative: Robert Oliver, Council At-Large Representative: Henry Gage III, Vice Chair, Mayoral Representative: Jessica Leavitt

Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.

1. Call to Order, determination of quorum

In attendance: Commissioner Suleiman, Chair Hofer, Commissioner Katz, Commissioner Tomlinson, Commissioner Gage, Commissioner Leavitt

Absent: Commissioner Oliver, Chloe Brown

2. Review and approval of the draft May meeting minute

Chair Hofer moved to approve the minutes and seconded by Commissioner Gage

Approved unanimously.

3. Open Forum/Public Comment

Ms. Assata Olugbala commented on her driver's license regarding federal limits apply. She provided background on the process and documents needed.

4. Surveillance Technology Ordinance – Department of Transportation (DOT) – Mobile Parking Payment System

- a. Review and take possible action on the proposed use policy

Chair Hofer introduced the item and provided background information including the work completed by the Cleveland law students and Commissioner Leavitt.

Michael Ford provided a staff update. He shared a summary including some clarification of terms in the use policy and impact analysis to help facilitate the discussion.

Chair Hofer further indicated the document includes clarification on terms regarding the data flow who would have raw data, anonymized data and aggregated data and those issues have been resolved. The retention periods are reasonable. Its subject to the ordinance and including these terms in the municipal contracts so the vendors take it seriously and honor our use policy terms and data security practices that the Privacy Advisory Commission (PAC) favors. The City Attorney's Office was also engaged in the process of negotiating the contracts.

Commissioner Tomlinson raised questions about the data protection section under number 5. This section states that the DOT will rely on each provider to securely store, transmit information and audit transactions, etc. So does that mean there were six different methodologies and protocols or did the DOT provide a framework for the six (6) providers? Mr. Ford indicated that DOT made changes to the system security plan that each vendor is responsible for following. He stated that each vendor will have their own system and their own terms and conditions, each will be responsible for implementing the system security protocol.

Commissioner Suleiman requested clarification on the attachment A addendum and indicated that this is what the vendor is responsible for following in the security protocol. Mr. Ford stated that part of the effort was to hold staff accountable for the surveillance technology ordinance, but to also bring it forward and include it in the professional services agreement. This will be a part of the negotiations with the contractors. The goal of the PAC has been to include this at the RFP process and Commissioner Suleiman indicated that she would like to hear feedback from the vendors and hopes that this could be a new standard for other departments to use going forward. Chair Hofer stated that this is an aspect of Privacy by Design which includes communicating with the designers in the procurement process.

The Commissioners proceeded to discuss clarification on ownership of the data between the individual and the contractor. The contract language was referenced in the motion.

Public Comment: Assata Olugbala stated information shared in the park mobile app including your license plate, phone and vehicle number, credit card number and other information could be at risk.

Chair Hofer clarified that the vendor cannot repurpose or sell data.

Motion: Commissioner Hofer moved that the PAC forward this to city council with a favorable recommendation to adopt the use policy and we also encourage the city attorney and DOT to address the individuals data ownership rights with possible clarification needed to the definitions in section 3 of the data addendum. Commissioner Leavitt seconded.

Commissioner Suleiman – yes
Commissioner Brown – absent
Chair Hofer – yes
Commissioner Katz - yes
Commissioner Tomlinson - yes
Commissioner Gage – yes
Commissioner Leavitt – yes
Commissioner Oliver - absent

Motion passed.

5. Surveillance Technology Ordinance – OPD – Fixed Wing Aircraft (with surveillance technology)
 - a. Review and take possible action on a proposed use policy

Chair Hofer provided an overview on this item. Commissioner Leavitt and Chair Hofer served on the ad hoc for this item and met with the vendor and discussed the capacity of the Fixed Wing Aircraft and they were able to see the flight plan and hear about the various restrictions. There were concerns about the retention policy and it was adjusted from two years to 6 months.

Officer Brandon Mart with OPD in the Air Support Unit made a brief presentation. He provided an update from the meeting in July when this item was last heard by the PAC. Changes were made to the use policy and impact report to alleviate concerns during that meeting. The vendor was in attendance to address questions as needed. The goal is to transition from the OPD helicopter to a fixed wing aircraft. The fixed wing camera will be activated to capture the overall nature of the scene. Body worn cameras are activated when officers are on scene.

Commissioner Gage recommended defining what the OPD means by “actively conducting” since it is mentioned throughout the document. As Officer Mart explained it, the definition is that members are on the scene on the ground, which is different from once the officers are dispatched. This needs to be defined more clearly and could be covered in section A3 under specific discretionary activations.

Mr. Joe DeVries recommended change to the document in sentence 1, under B2 which remains the same up to the semi-colon and then add and/or where a subject as been observed as being actively violent towards community members or officers.

Commissioners emphasized the need to state specific authorized uses, which could include fire suppression and investigation. Authorized uses are listed under B2. This could also include reckless drivers or natural disasters.

Chair Hofer stated with the edits, suggested amendments previously discussed on video and to be confirmed between members of the PAC and staff at a subsequent time before the Public Safety Committee. Chair Hofer moved that the PAC forward this with a favorable recommendation to the City Council. Seconded by Commissioner Gage.

Commissioner Suleiman – yes

Chair Hofer – yes

Commissioner Katz - yes

Commissioner Tomlinson - yes

Vice Chair Gage - yes

Commissioner Leavitt – yes

The item passed.

The meeting was adjourned.



Privacy Advisory Commission
October 5, 2023 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
DRAFT Meeting Minutes

Commission Members: District 1 Representative: Reem Suleiman, District 2 Representative: Chloe Brown, District 3 Representative: Brian Hofer, Chair, District 4 Representative: Lou Katz, District 5 Representative: Vacant, District 6 Representative: Gina Tomlinson, District 7 Representative: Robert Oliver, Council At-Large Representative: Henry Gage III, Vice Chair, Mayoral Representative: Jessica Leavitt

Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.

1. Call to Order, determination of quorum

In attendance: Chair Hofer, Vice Chair Gage, Commissioner Suleiman, Commissioner Brown, Commissioner Katz, Commissioner Oliver

Absent: Commissioners Tomlinson and Leavitt

2. Review and approval of the draft June 8, July 6 meeting minutes

Draft Meeting Minutes for June 8.

motion to approve by Chair Hofer, seconded by Henry Gage III.

Approved unanimously.

Draft Meeting Minutes for July 6.

Chair Hofer reminded staff that Dela Cruz resigned from the Commission and to remove him from the meeting roster for both June and July. On July 6 add Commissioner Oliver as present not absent.

Chair Hofer moved to accept, second by Commissioner Gage

Approved unanimously.

3. Open Forum/Public Comment

No public comment.

4. Surveillance Technology Ordinance – OPD – Automated License Plate Readers
 - a. Review and take possible action on a proposed use policy

Chair Hofer recused himself due to the proposed settlement agreement and left the meeting. Vice Chair Gage took over running the meeting.

Lt. Omar Daza-Quiroz made a presentation on ALPR, Department General Order I12. A couple of items that were agreed to were the retention schedule of ALPR from 6 months to 30 days. The other discussion included creating an auditing tool and look at how other nearby agencies managed this process. OPD explored the surrounding agencies usage of the Flock Camera system, including BART, San Leandro and Alameda. The ease of their auditing system creates transparency and accountability. There is a transparency report through Flock where the community can look at the number of cameras, the number of searches by officers and what was the reason. The policy also addresses making sure that data is only shared in the State of California. These were the primary areas covered. OPD chose Flock because they have a proven track record of working with other agencies.

Public Comment:

Jim Donet, Representing the Lakeshore Homes Association

He attended a public safety meeting on Lakeshore and following a discussion with Deputy Chief Beere he began researching Flock cameras and indicated that his HOA has purchased Flock cameras and will provide access to OPD.

Vice Chair Gage provided an overview and indicated that the draft policy which resulted from an ad-hoc with the Vice Chair and Commissioner Leavitt. They met with members of OPD to discuss the amendments proposed by the department.

Commissioner Katz raised a question about Flocks statewide and nationwide networks. He also commented on Flock services audio detection and requested clarification. Josh Thomas from Flock Safety responded. He indicated that the audio network is a separate product line that is not a part of this ALPR policy. Flock does have customers in 4,000 cities across the country, however, in this policy access could only be allowed in the State of California.

Mr. Joe DeVries clarified under SB34 state law, the city cannot share data or allow federal agencies or other agencies to query our system. This is also stated in the use policy.

Commissioner Brown raised a question about any remaining concerns or were they all addressed by the ad hoc. VC Gage explained that when handing over a new investigative tool to law enforcement there will always be concerns about how it is used. He further explained that the PAC's role is advisory, we look at a policy, craft language to meet the base needs and give law enforcement an opportunity to prove that it

works. An annual report is required in a year and the auditing capabilities will provide a better sense of efficacy. Privacy concerns are ongoing, but license plates are publicly viewable and prominently displayed so the privacy issues are a bit more limited.

Commissioner Brown requested a map or list of cameras.

Vice Chair Gage made a motion that the PAC approve the DGO as presented and forward to Council with a recommendation for adoption. Seconded by Commissioner Suleiman.

Roll call:

Commissioner Suleiman, yes

Commissioner Brown, yes

Commissioner Katz, abstain

Commissioner Oliver, yes

Commissioner Gage, yes

The motion carries.

The meeting was adjourned.



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:
 - o 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.
 - o 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 may utilize 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 of 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:

DRAFT

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 *intentionally or inadvertently* 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.

DRAFT