Attachment A

CITY OF OAKLAND

# MEMORANDUM

**TO:** PAC

**FROM:** Sgt. Y. Zhou
OPD, Criminal Investigation Division

**SUBJECT:** Annual Report – Cellebrite / Mobile Forensic Extraction Device

**DATE:** **MAY 13, 2025**

## Background

Oakland Municipal Code (OMC) 9.64.040: Oversight Following City Council Approval requires that for each approved surveillance technology item, city staff must present a written annual surveillance report for the Privacy Advisory Commission (PAC). After review by PAC, city staff shall submit the annual surveillance report to City Council. The PAC shall recommend to City Council that:

- The benefits to the community of the surveillance technology outweigh the costs, and civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

Sgt. Y. Zhou is currently the program coordinator for OPD's mobile device extraction.

## 2024 Annual Report Details

A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

Cellebrite Premium (current version being used by OPD) is used to extract data from a mobile device. The tool supports both logical and physical extractions, allowing access to data including call logs, SMS/MMS, contacts, browser history, application data (e.g., WhatsApp, Facebook, Signal), emails, GPS/location data, and deleted content when available. The amount and type of data gathered depends on the device model, operating system, and encryption level. The Cellebrite tool does not conduct live surveillance; it performs a one-time data extraction from a seized device.

OPD has owned and used an old Cellebrite UFED device prior to bringing the mobile forensic extraction policy to PAC. OPD began the required data collection in February 2024 when the policy was passed. However, OPD did not acquire the updated Cellebrite device until July 2024. The difference between these two devices is significant. Prior to the acquiring the updated Cellebrite device in July 2024, OPD has no real capability to extract data from a locked device without the passcode.

OPD utilizes the Cellebrite tools in both administrative and criminal investigations. Administratively, OPD is required to conduct random quarterly audits of work phones belonging to OPD members. OPD Internal investigations will also download and examine member work phones pertaining to internal investigations. Given the nature of these investigations, the program coordinator can only facilitate the extraction of OPD work

phones and do not know whether these phones were selected as a random audit or as part of an investigation. From February 2024 to December 2024, OPD has conducted 30 internal work phone searches. OPD members are required to provide a passcode to IAD for these extractions, as such, they are equally as successful on the older Cellebrite or the newer Cellebrite device.

For criminal investigations, OPD is allowed to conduct consent, exigency, and search warrant searches of mobile devices / tablets. From February 2024 to December of 2024, OPD has conducted 1 consent search of a mobile device and 271 searches of a mobile device pursuant to a search warrant.

From February to June of 2024, when OPD was utilizing the older Cellebrite UFED device, OPD extracted or attempted to extract data from 35 devices as pertaining to a criminal investigation. After acquiring the updated Cellebrite device, 237 devices were extracted or attempted to be extracted by OPD as pertaining to a criminal investigation. Out of those devices, 39 devices were unable to be extracted by OPD.

Extractions by Investigation Type (February – June 2024)

| **Investigation Type** | **Number of Extractions** |
|---|---|
| IAD (Internal Affairs) | 26 |
| Homicide | 25 |
| Robbery | 7 |
| Felony Assault (Shooting, stabbing, non-fatal) | 3 |

All non-IAD related devices were accessed and extracted pursuant to a search warrant.

Extractions by Investigation Type (July – December 2024)

| **Investigation Type** | **Number of Extractions** |
|---|---|
| Homicide | 110 |
| Robbery | 46 |
| Felony Assault (Shooting, stabbing, non-fatal) | 40 |
| Firearm-related (Brandishing, illegal possession) | 18 |
| Sexual Assault | 13 |
| Burglary | 6 |
| IAD (Internal Affairs) | 4 |
| Human Trafficking | 3 |
| Hit and Run | 1 |

Only one device was downloaded with the consent of the owner in a robbery investigation; the owner of the device was a suspect in the robbery and provided consent to search his / her device during a recorded interview with OPD investigators. All other non-IAD related devices were accessed pursuant to a search warrant.

B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

OPD shares mobile device extraction data obtained through Cellebrite with prosecutorial agencies as part of ongoing criminal prosecutions. The data is shared with agencies such as the Alameda County District Attorney's Office and federal prosecutorial office as part of the routine discovery process. These disclosures are made at the request of the prosecuting attorney and are standard practice during the course of prosecution. OPD does not maintain separate records of each instance in which data is shared for discovery, as these requests are part of the broader prosecution effort and not tracked independently by OPD. OPD has not shared any Cellebrite extraction data with U.S. Immigration and Customs Enforcement (ICE), the Department of Homeland Security (DHS), or U.S. Customs and Border Protection (CBP).

C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

The Cellebrite Premium phone extraction tool is located within the OPD CID office and connected to a computer that access the OPD network. It is not taken into the field. The tool is used on mobile devices or tablets (both Android and iOS) either as part of a criminal investigation or OPD internal audit / investigation. It extracts data stored on the device, including internal memory, SIM cards, and SD cards when present. It is not connecting to any live data feeds or external surveillance sources.

D. Where applicable, a breakdown of where the surveillance technology was deployed geographically by each police area in the relevant year:

N/A. The device is not deployed in the field.

E. A summary of community complaints or concerns about the surveillance technology and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

No community complaints or concerns were communicated to staff in 2024.

No racial data was gathered for internal OPD work phone searches.

Extractions Conducted as Part of a Criminal Investigation by Race

| | |
|---|---|
| Black | 176 |
| Hispanic | 65 |
| White | 13 |
| Asian | 9 |
| Unknown | 9 |

The racial data for nine devices being unknown is due to the identity of the owner is unknown, or the data was not gathered. Only one search as part of a criminal investigation was not pursuant to a search warrant, the race of the owner of the device was identified as Black.

OPD's use policy allows OPD to conduct forensic extraction of these devices in a criminal investigation either pursuant to a search warrant, via consent, or life / death exigency. In 2024, only one consent search was conducted. The search was sought during a recording interview, the manner in which the consent was sought and given was recorded. All other searches were done via search warrants authorized and signed by judges. Officers would have to articulate to judges, under penalty of perjury, the facts in which relevant evidence exists on these devices relating to the crime(s) they are investigating. Given these safeguards, OPD's adopted use policy is adequate in protecting the civil rights and civil liberties of the individuals whom the department is using the technology on.

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

One internal audit was conducted in November of 2024. The program coordinator compared the usage log automatically generated by the Cellebrite device to the audit usage log maintained by OPD. All usage of the device correlated to an entry in the OPD usage log. There was no unauthorized or undocumented usage of the Cellebrite device.

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response:

There were no known data breaches or known unauthorized access during 2024.

H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

Homicide
During the investigation of a 2025 homicide, a suspect was identified. A search warrant was authored for the suspect's wireless account, but it was submitted outside of the window for specialized location records. Because of this, the investigation had to rely on limited location data generated only by calls and text messages. When the suspect was arrested, his phone was seized and a Cellebrite download was conducted pursuant to a search warrant. The report documented additional location data that was not captured by

the wireless company. The new location data pinpointed the suspect’s location before and after the murder and provided important evidence in the case.

Robbery Series #1
In the second quarter of 2024, a series of eight armed robberies including two where victims were struck by gunfire occurred. A suspect was taken into custody and the Cellebrite was used to extract data from the suspect’s electronic device. The data extracted included data connections, media and messages that led to the suspect being charged for the entire series of robberies.

Robbery Series #2
From September 2024 to October 2024, at least four major robbery series occurred within the City of Oakland. These series all had major commonalities between them, targeting mostly Hispanic day laborers in the early morning hours. The robberies were committed in quick succession as the driver would stay in the vehicle, and multiple suspects would exit, armed with firearms and demand money. The suspects would often pistol-whip the victims if any resistance was encountered. During these incidents, up to nine victims would be robbed at a time.

Multiple suspects were taken into custody during the course of the series. Multiple cellular phones were extracted by use of the Cellebrite. The data on these phones included communications, media, data connections and cellular connections between the suspects. The data was critical in charging three suspects in the series and led directly to their prosecution.

Robbery Series #3
In January 2024, a series of an armed carjacking and seven armed robberies occurred in the City of Oakland. One suspect was taken into custody the following day and his cellular device was extracted via Cellebrite. The information within the device led to investigators identifying four other suspects within the series. The information would not have been obtained via any other source during the investigation and proved invaluable when one suspect later committed a shooting prior to his arrest. The data was used for both the robbery cases as well as the attempted homicide case.

Robbery Series #4
In June 2024, a robbery series involving two carjackings and two commercial business takeovers with rifles occurred in the City of Oakland. Data from the suspects' devices was later used to identify them both as suspects of a separate human trafficking case as well as a separate robbery and kidnapping.

Robbery Shooting
In April 2024, a robbery and attempted homicide occurred in the City of Oakland. One suspect was taken into custody and his device was processed by Cellebrite. Media, communication, and data logs from the device led to the positive identification of two other suspects. The data from the other two suspects' devices assisted in the prosecution of the two. One suspect was charged due to the key evidence on his device, which was recovered from a forensic extraction.

Attempted Homicide
In July 2024, an attempted homicide occurred in the City of Oakland. Two victims were shot, and one was paralyzed permanently. Cellebrite was used to extract both suspects' electronic devices. The media, log files, communications, and device connections were used as evidence to charge the suspects with the shooting.

I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

There are no existing or newly opened public records requests relating to the technology.

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

The cost to acquire and operate Cellebrite Premium for June 2024 to June 2025 was $96,688.95.

The renewal for Cellebrite Premium from June 2025 to June 2026 has increased to $107,769.38

The expected renewal cost for Cellebrite from June 2026 to June 2027 will be $130,095, and is subject to change.

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

1. OPD is requesting to transition from referring to the tool by its trademark name when the policy was first developed, Cellebrite UFED, to referring to the tool as its purpose, a mobile forensic extraction tool. This is to avoid confusion as the company renames the service provided to OPD. For context, this tool was named Cellebrite UFED, to now Cellebrite Premium and soon to be renamed Cellebrite Inseyets. This would not change the legal and policy requirement that OPD has to follow to use this tool, it would only facilitate ease of future reporting.

2. OPD is also requesting additional funding for the renewal of Cellebrite, given the expected increase in cost for the June 2026 to June 2027 renewal.

   When OPD was still using the older Cellebrite UFED device from February to June of 2024, it was only utilized 35 times in a criminal investigation. Mostly in homicides. After upgrading in July, the usage increased to 237 times and involving other serious crimes. This significant increase reflects the device's value in terms of capability and the need for digital evidence in criminal investigations. Additional funding to maintain this digital evidence capability of OPD is essential for its investigative capability.

3. OPD requests that future data gathered regarding the race of each person subject to the technology's use be limited to extractions not done pursuant to a search warrant—i.e., consent or exigent circumstance searches.

   In warrant-based extractions, the search is authorized by a judge based on a sworn affidavit establishing probable cause. The race of the individual is not a factor in the legal standard or the judge's decision to issue the warrant. Because of that, there is no clear probative value in tracking race data for these cases when evaluating potential impacts on civil rights or civil liberties.

   Collecting and verifying race data for all warrant-based extractions also creates an administrative burden, particularly in cases where the phone owner is unknown,

there are multiple subjects, or race data was not otherwise collected during the investigation. Trying to gather this information can be intrusive in itself.

Given these concerns, OPD recommends limiting race tracking to consent and exigent searches, where officer discretion plays a more direct role and where the data may be more meaningful in identifying potential disparities.