Surveillance Impact Report

Data Extraction Tool for Computers and Cell Phones
San Francisco Police Department

As required by San Francisco Administrative Code, Section 19B, departments must submit a Surveillance Impact Report for each surveillance technology to the Committee on Information Technology ("COIT") and the Board of Supervisors.

The Surveillance Impact Report details the benefits, costs, and potential impacts associated with the Department's use of a data extraction tool for computers and mobile devices.

PURPOSE OF THE TECHNOLOGY

Pursuant to the San Francisco Charter, the Police Department is required to preserve the public peace, prevent, and detect crime, and protect the rights of persons and property by enforcing the laws of the United States, the State of California, and the City and County. The Department's mission is to protect life and property, prevent crime and reduce the fear of crime by providing service with understanding, response with compassion, performance with integrity and law enforcement with vision.

The surveillance technology supports the Department's mission and provides important operational value in the following ways:

These technologies forensically examine computers and mobile devices associated with a crime and help determine whether a subject is associated or can be exonerated from their alleged participation in a crime.

The Department shall use the surveillance technology only for the following authorized purposes:

Authorized Use(s):

To conduct forensic/evidence examination of computers and/or mobile devices received under the provisions of CA Penal Code §1546.1, including, but not limited to via a search warrant or specific consent. Examinations are performed by the SFPD CSI-Multimedia Evidence Unit.

Surveillance technology may be deployed in the following locations, based on use case:

SFPD Digital Forensics Lab (Multimedia Evidence Unit).

Description of Technology
This is a product description of the technology and how they work:

All of the Cellebrite tools are utilized in the digital forensic lab space or in the field by members of the digital forensics lab. Evidence items such as computers, mobile devices, digital media, etc. are submitted to the lab for examination. The Cellebrite tools listed below are located on forensic workstations and only accessible by digital forensic examiners.

- Cellebrite Inspector (formerly known as BlackBag's "BlackLight") is used worldwide by examiners in the digital forensics community. It quickly analyzes computer volumes and mobile devices and allows for fast searching, filtering, and sifting through large data sets. With its easy-to-use graphical interface you can quickly find internet history, downloads, recent searches top sites, locations, media, messages, and more. (BlackBag was recently procured by Cellebrite and this tool is now known as Cellebrite Inspector.)

- Cellebrite Digital Collector (formerly known as BlackBag's "MacQuisition") is a unique forensic imaging and acquisition tool capable of booting various MacOS systems, as well as acquiring live targeted data. Digital Collector is a forensic solution that runs within a native MacOS boot environment. Digital Collector is the first and only solution to create physical images of Macs with the Apple T2 chip. Tested and used by experienced examiners for over a decade, Digital Collector runs on the MacOS operating system and safely boots and acquires data from different Macintosh computer models in their native environment – even Fusion Drives. (BlackBag was recently procured by Cellebrite and this tool is now known as Cellebrite Digital Collector.)

- Cellebrite UFED 4PC can bypass locks and passcodes on many mobile devices, as well as perform multiple types of digital extractions from them. Cellebrite Physical Analyzer can parse more data than what is possible through other tools and do so in a forensic means. Cellebrite can gain access to 3rd party app data, chat conversations, downloaded emails and email attachments, deleted content and more, increasing the chances of finding inculpatory (as well as exculpatory) evidence.

Third-Party Vendor Access to Data

Data collected or processed by the surveillance technology will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Records.

IMPACT ASSESSMENT

The impact assessment addresses the conditions for surveillance technology approval, as outlined by the Standards of Approval in San Francisco Administrative Code, Section 19B:

1. The benefits of the surveillance technology outweigh the costs.
2. The Department's Policy safeguards civil liberties and civil rights.
3. The uses and deployments of the surveillance technology are not based upon discriminatory or viewpoint-based factors and do not have a disparate impact on any community or Protected Class.

The Department's use of the surveillance technology is intended to support and benefit the residents of San Francisco while minimizing and mitigating all costs and potential civil rights and liberties impacts of residents.

A. Benefits

The Department's use of the surveillance technology has the following benefits for the residents of the City and County of San Francisco:

	Benefit	Description
▪	Education	
▪	Community Development	
▪	Health	
▪	Environment	
X	Criminal Justice	Forensic computer analysis can be used to discover and document evidence in criminal investigations.
▪	Jobs	
▪	Housing	
▪	Other	

B. Civil Rights Impacts and Safeguards

The Department has considered the potential impacts and has identified the technical, administrative, and physical protections as mitigating measures:

Administrative Safeguards:
The administrative safeguards are use of the technologies are limited to members of Forensic Services Division (FSD) who have documented training in the technologies. The digital forensics lab has procedures that must be followed when using these tools. Following these procedures safeguards the data obtained during analysis and ensures protection and confidentiality,

These standard operating procedures (SOPs) are based on Digital Forensic standards that the lab voluntarily abides by. These standards are provided by the Organization of Scientific Area Committees (OSAC) – Digital Forensics and the Scientific Working Group on Digital Evidence (SWGDE).

OSAC is a Federal project, administered by the National Institute of Standards and Technology. The SFPD Digital Forensics Lab is a voluntary adopter of OSAC standards and will adopt these standards as they are released. This ensures that all the best practices are continually followed, even as the field progresses. OSAC standards deal with training, examination procedures and correct terminology.

Along with OSAC, the digital forensics lab, voluntarily follows and adopts the SWGDE recommended procedures and policies. SWGDE is a working group of practitioners, lawyers, and academia and are tasked with issuing best practices for the digital forensics community. The digital forensics lab has voluntarily committed to adopting SWGDE best practices.

Since OSAC and SWGDE are adopted and added to the lab's procedure manuals, they will be reviewed and assessed during internal audits, demonstrating, a multilayer approach to ensuring administrative

safeguards are in place, maintained and followed. The goal of the Digital Forensics Lab is to achieve accreditation through the American Association for Lab Accreditation, further enhancing the administrative safeguards in place.

Technical Safeguards:

These technologies are only used in the Forensic Services Division and are highly restricted. Technologies only brought to bear on evidence submitted in the course of a criminal investigation. Data access is restricted to Digital Forensics Lab unit personnel and stored on an internal forensic network. The SFPD internal network is password protected and controlled by FSD. Employees must be a part of the unit to access these tools. The physical access to the unit is restricted to unit personnel.

Results of the examination are provided by the Digital Forensics Lab to the investigator in the format of a working copy or result copy report which is the requested data governed by the legal authority of the investigation. The investigator is provided the report for them to store with their casefile. Raw data is not provided. Investigators access is limited to working or results copy data.

Privacy and the confidentiality of investigatory information is of prime concern when using Cellebrite tools. Any devices that are analyzed are collected through legal search warrants or voluntarily submitted for examination. The tools are only used by qualified digital forensic examiners while working at the Digital Forensics Lab. The digital forensics lab has their own internal network that does not communicate outside the Digital Forensics Lab. Any information from the devices is protected and unauthorized release mitigated.

Sharing of data is prohibited by lab accreditation standards unless ordered to do so by the court for discovery purposes.

OSAC, SWGDE and international standards stress the importance of privacy and confidentiality of forensic work and these standards that must be followed reflect it. Strict adherence to the procedural manuals is enforced at the Digital Forensics Lab and confirmed internally and externally through review of casework and auditing of lab systems.

Physical Safeguards:

The Digital Forensics Lab is only accessible by staff who gain access through an RFID badge. The building access is managed by SFPD Facilities Unit. The Digital Forensics Lab is not accessible to the public due to the nature of the work performed and accreditation standards. Additionally, Digital Forensics Lab access is restricted to staff as staff is only able to access their assigned workspaces. The staff may only access lab spaces in which they are authorized to perform work. If a member of the public needs access then they must sign in and be fully escorted during the course of their visit.

C. Fiscal Analysis of Costs and Benefits

The Department's use of the surveillance technology yields the following business and operations benefits:

	Benefit	Description
x	Financial Savings	Forensic computer analysis can document and discover relevant files on devices quickly, reducing investigator hours examining devices.
x	Time Savings	Forensic computer analysis can document and discover relevant files on devices quickly, reducing investigator hours examining devices.
-	Staff Safety	
x	Data Quality	Forensic computer analysis provides investigators with specific and relevant documents from devices in criminal investigations.
-	Other	

The fiscal cost, such as initial purchase, personnel and other ongoing costs, include:

Number of Budgeted FTE (new & existing) & Classification	Q2-Q4, Police Officer Q50-Q-52, Sergeant Q60-Q62, LT also currently have an oversight role. 8252-8254 Forensic Examiner 8259-8262 Criminalists 0955 Forensic Services Director~~3~~	
	Annual Cost	***One-Time Cost***
Total Salary & Fringe	~~$650,000~~	
Software	$~~35,000~~35,520	
Hardware/Equipment		
Professional Services		
Training		
Other		

Total Cost	~~***$685,000***~~ ***35,520***	***None***

The Department funds its use and maintenance of the surveillance technology through the SFPD Operating Budget.

COMPARISON TO OTHER JURISDICTIONS

The technology is currently utilized by other governmental entities for similar purposes.

Other government entities have used the technology in the following way: Retrieve and analyze digital evidence for use in investigations and court proceedings.

The effectiveness of the technology while used by government entities is determined to be the following: These tools are currently the standard in the field of digital forensics in order to effectively conduct forensic analysis on technology that is rapidly growing and changing.

The adverse effects of the technology while it has been used by other government entities are: Forensic data extraction tools must be used in a controlled environment by trained forensic analysts to ensure that the right inferences are made from the extracted data to be used as evidence. Conclusions made by an unskilled individual could put the reliability of the extracted data into question.

These tools are used by most Law Enforcement Agencies (LEA) – including the Federal Bureau of Investigation and the United States Secret Service, among others. Most LEA performing digital forensics are using Cellebrite as part of their suite of forensic tools.