



30-Day Posting
SEC 19B.3(b)

February 6, 2024

Pursuant to San Francisco Administrative Code 19B, a Department seeking approval under Section [19B.2](#) shall publicly post on the Department website, a Surveillance Impact Report (SIR) and a proposed Surveillance Technology Policy (STP) ordinance at least 30 days prior to the public meeting where the Board of Supervisors (BOS) will consider the STP.

The following is the Department's SIR and proposed STP relating to Data Extraction Tools for Computers and Cell Phones.

The STP and SIR were presented and discussed during the February 24, 2023, and June 29, 2023, [Privacy Surveillance Advisory Board \(PSAB\)](#) hearings.

The STP and SIR were then presented to the [Committee on Information Technology \(COIT\)](#) on September 21, 2023. On November 29, 2023, COIT issued a memo to the Members of the BOS recommending the approval of the Police Department's Data Extraction Tool for Computers and Cell Phone STP.

Next Steps:

- Legislation relating to STP will be introduced to the BOS and then will be assigned to a BOS committee.
- The BOS Committee will hold hearing(s) relating to the STP and may amend or recommend to full BOS for adoption.
- Full BOS may adopt the STP's ordinance after the 1st and 2nd readings.



Committee on Information Technology

Office of the City Administrator

To: Members of the Board of Supervisors

From: Carmen Chu, City Administrator

Jillian Johnson, Director, Committee of Information Technology

Date: November 29, 2023

Subject: Legislation introduced to approve Surveillance Technology Policy for the Police Department's Data Extraction Tool for Computers and Cell Phones

In compliance with Section 19B of the City and County of San Francisco's Administrative Code, the City Administrator's Office is pleased to submit the Surveillance Technology Policy for the Police Department's Data Extraction Tool for Computers and Cell Phones.

To engage the public in discussion on the role of government surveillance, the Committee on Information Technology (COIT) and its subcommittee the Privacy and Surveillance Advisory Board (PSAB) held 3 public meetings for Data Extraction Tool for Computers and Cell Phones between February and September 2023 to review and approve the policy. All details of these discussions are available at sf.gov/coit.

The following page provides greater detail on the review process for the Surveillance Technology Policy, and COIT's recommended course of action.

If you have questions on the review process please direct them to Jillian Johnson, Director of the Committee on Information Technology (COIT).

Data Extraction Tool for Computers and Cell Phones

Department	Authorized Uses
Police Department	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.

Data Extraction Tool for Computers and Cell Phones Public Meeting Dates

Date	Meeting
February 24, 2023	Privacy and Surveillance Advisory Board (PSAB)
June 29, 2023	Privacy and Surveillance Advisory Board (PSAB)
September 21, 2023	Committee on Information Technology (COIT)

COIT recommends the following action be taken on the policy:

- Approve the Data Extraction Tool for Computers and Cell Phones Surveillance Technology Policy for the Police Department



Surveillance Technology Policy

Data Extraction Tool for Computers and Cell Phones

San Francisco Police Department

The City and County of San Francisco values privacy and protection of San Francisco residents' civil rights and civil liberties. As required by San Francisco Administrative Code, Section 19B, the Surveillance Technology Policy aims to ensure the responsible use of Cellebrite itself as well as any associated data, and the protection of City and County of San Francisco residents' civil rights and liberties.

PURPOSE AND SCOPE

Pursuant to the San Francisco Charter, the San Francisco Police Department (SFPD) 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 Policy ("Policy") defines the manner in which a data extraction tool for computers and mobile devices will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to these data extraction tools, including employees, contractors, and volunteers. Employees, consultants, volunteers, and vendors while working on behalf of the City with the Department are required to comply with this Policy.

POLICY STATEMENT

The authorized use of the surveillance technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

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 pursuant to a relevant investigation.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Department may use information collected from technology only for legally authorized purposes and may not use that information to unlawfully discriminate against people based on race, ethnicity,

Surveillance Oversight Review Dates

PSAB Review: 2/24/2023; 6/29/2023

COIT Review: 9/21/2023

Board of Supervisors Approval: TBD

political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation, or activity, or genetic and/or biometric data.

SFPD is prohibited from seeking to extract data for purposes of enforcing prohibitions on gender-affirming health care, reproductive care, or interstate travel for gender-affirming or reproductive health care. Except as required by law, SFPD shall not share extracted data with any law enforcement agency for purposes of enforcing prohibitions on gender-affirming health care, reproductive care, or interstate travel for gender-affirming or reproductive health care.

BUSINESS JUSTIFICATION

Reason for Technology Use

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

The purpose of these technologies is to preserve the integrity and quality of information and evidence of crime by supporting the Crime Lab and Crime Scene Investigation teams with tools to examine crucial evidence collected at or connected to crime scenes. These tools forensically examine computers and mobile devices so investigators can reconstruct the elements of a crime and accurately determine the facts of the case which are then provided to the prosecution. These tools allow the Department to gather evidence that links the correct suspect to a crime and will protect individuals from consequences of being wrongly accused of a crime. The evidence is used by the District Attorney's office to determine guilt or innocence through the court system.

Description of Technology

Digital forensic tools are used for the following tasks:

- 1) To analyze computer volumes and mobile devices by filtering and sifting through data such as internet history, downloads, recent searches, locations media, messages, etc.
- 2) To extract data from digital devices.
- 3) To bypass locks and pass codes on mobile devices and computers.
- 4) To 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.
- 5) To organize results of digital forensic examinations.

As of the date of this STP, the tools in use are from the vendor Cellebrite (Inspector, Digital Collector and UFED 4PC).

Nothing herein prohibits procurement of additional data extraction/digital forensic tools provided the Department adheres to the authorized use(s) and prohibitions outlined in this STP.

Resident Benefits

The technology promises to benefit residents in the following ways:

	Benefit	Description
<input type="checkbox"/>	Education	
<input type="checkbox"/>	Community Development	
<input type="checkbox"/>	Health	
<input type="checkbox"/>	Environment	
<input checked="" type="checkbox"/>	Criminal Justice	Forensic computer analysis can be used to discover and document evidence in criminal investigations.
<input type="checkbox"/>	Jobs	
<input type="checkbox"/>	Housing	
<input type="checkbox"/>	Other	

Department Benefits

The surveillance technology will benefit the department in the following ways:

	Benefit	Description
<input checked="" type="checkbox"/>	Financial Savings	Forensic computer analysis can document and discover relevant files on devices quickly, reducing investigator hours examining devices.
<input checked="" type="checkbox"/>	Time Savings	Forensic computer analysis can document and discover relevant files on devices quickly, reducing investigator hours examining devices.
<input type="checkbox"/>	Staff Safety	
<input checked="" type="checkbox"/>	Data Quality	Forensic computer analysis provides investigators with specific and relevant documents from devices in criminal investigations.
<input type="checkbox"/>	Other	

POLICY REQUIREMENTS

This Policy defines the responsible data management processes and legally enforceable safeguards required by the Department to ensure transparency, oversight, and accountability measures.

Department use of surveillance technology and information collected, retained, processed or shared by surveillance technology must be consistent with this Policy; must comply with all City, State, and Federal laws and regulations; and must protect all state and federal Constitutional guarantees.

Specifications: The software and/or firmware used to operate the surveillance technology must be up to date and maintained.

Data Collection: Department shall only collect data required to execute the authorized use cases. All data collected by the surveillance technology, including PII, shall be classified according to the City's [Data Classification Standard](#).

The surveillance technology collects some or all of the following data type(s):

<i>Data Type(s)</i>	<i>Format(s)</i>	<i>Classification</i>
Digital Forensic Evidence	Call logs, contact lists, MMS data, SMS data, images, videos, audio, documents/notes, internet history & bookmarks, location data, app data, 3 rd -party app data, health data, device logs, various forms of metadata	Level 4

Per CA Penal Code §1546.1(d)(2), the warrant (allowing SFPD's authorized use) shall require that any information that is unrelated to the objective of the warrant shall be sealed and shall not be subject to further review, use, or disclosure except pursuant to a court order.

Access: All parties requesting access must adhere to the following rules and processes:

Only SFPD members of the digital forensics' lab has access to these technologies and must be trained prior to their use.

A. Department employees

Once collected, the following roles and job titles are authorized to access and use data collected, retained, processed, or shared by the technology:

- Q2-Q4, Police Officer
- Q50-Q-52, Sergeant

- Q60-Q62, Lieutenant
- 8252-8254 Forensic Examiner
- 8259-8262 Criminalists
- 0933 Crime Lab Manager
- 0955 Forensic Services Director

Unless assigned to Forensics Services, Q2 through Q62 data access is limited to the reports provided by the SFPD forensic practitioners or Forensic Services staff.

B. Members of the public

Department will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules.

Collected data that is classified as Level 1-Public data may be made available for public access or release via DataSF’s [Open Data](#) portal. Open Data has a Public Domain Dedication and License, and makes no warranties on the information provided. Once public on Open Data, data can be freely shared, modified, and used for any purpose without any restrictions. Any damages resulting from use of public data are disclaimed.

Members of the public may also request access by submission of a request pursuant to San Francisco’s [Sunshine Ordinance](#). No record shall be withheld from disclosure in its entirety unless all information contained in it is exempt from disclosure under express provisions of the California Public Records Act or some other statute.

Training:

To reduce the possibility that the technology or its associated data will be misused or used contrary to its authorized use, all individuals requiring access must receive training on data security policies and procedures.

At the very least, department shall require all elected officials, employees, consultants, volunteers, and vendors working with the technology on its behalf to read and formally acknowledge all authorized and prohibited uses. Department shall also require that all individuals requesting data or regularly requiring data access receive appropriate training before being granted access to systems containing PII.

All users must successfully complete documented in-house training in the technologies prior to their use. Each Cellebrite tool must be trained on prior to use. Training is composed of exercises using the tools, documented reading on the tools and mock casework prior to their use. Training results are evaluated by a supervisor and the laboratory quality system and documented authorization is required prior to use in casework. Training can be provided by outside experts, vendor provided training and Department training. Final approval and authorization are provided by the laboratory.

Data Security: Department shall secure PII against unauthorized or unlawful processing or disclosure; unwarranted access, manipulation, or misuse; and accidental loss, destruction, or damage. Surveillance technology data collected and retained by the Department shall be protected by the safeguards appropriate for its classification level(s) as defined by the National Institute of Standards and Technology (NIST) security framework 800-53, or equivalent requirements from other major cybersecurity framework selected by the department.

Department shall ensure compliance with these security standards through the following:

Data is restricted to Crime Lab unit personnel in a locked facility. The SFPD network is password protected and authentications are controlled by the SFPD Department of Technology. The physical access to the unit is restricted to unit personnel. Results of the examination are provided to the investigation teams 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, with the exception for defense discovery.

Data Storage: Data will be stored in the following location:

- x Local storage (e.g., local server, storage area network (SAN), network attached storage (NAS), backup tapes, etc.)
- x Department of Technology Data Center
- x Software as a Service Product
- x Cloud Storage Provider

All case data will be primarily stored at the local level. Some forms of search warrant production data must be downloaded from the internet (cloud). In addition, some internal case tracking and organizational software is maintained in the cloud. Processed and parsed data containing PII is maintained on local storage.

Data Sharing: For internal and externally shared data, shared data shall not be accessed, used, or processed by the recipient in a manner incompatible with the authorized use cases stated in this Policy.

Department shall ensure proper administrative, technical, and physical safeguards are in place before sharing data with other CCSF departments, outside government entities, and third-party providers or vendors. (*See Data Security*)

Department shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded from entities that do not have authorized access under this policy.

Further, in sharing data, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual person, data concerning health or data concerning an individual person's sex life or sexual orientation shall be prohibited.

Each department that believes another agency or department receives or may receive data collected from its use of surveillance technologies should consult with its assigned deputy city attorney regarding their legal obligations.

Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place:

- Confirm the purpose of the data sharing aligns with the department's mission.
- Consider alternative methods other than sharing data that can accomplish the same purpose.
- Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.
- Evaluation of what data can be permissibly shared with members of the public should a request be made in accordance with the San Francisco's [Sunshine Ordinance](#).
- Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

A. Internal Data Sharing (city agencies):

The department shares the following data with recipients within the City and County of San Francisco:

Data Type	Data Recipient
Call logs, contact lists, MMS data, SMS data, images, videos, audio, documents/notes, internet history & bookmarks, location data, app data, 3 rd -party app data, health data, device logs, various forms of metadata – only data relevant to the crime or investigation of criminal activity.	Provided to District Attorney's Office or Public Defender's Office or criminal defense attorney via the District Attorney's Office in accordance with California and federal discovery laws

Frequency - Data sharing occurs at the following frequency:

- Upon discovery request

B. External Data Sharing (non-city agencies):

The department shares the following data with recipients external to the City and County of San Francisco:

Data Type	Data Recipient
Call logs, contact lists, MMS data, SMS data, images, videos, audio, documents/notes, internet history & bookmarks, location data, app data, 3 rd -party app data, health data, device logs, various forms of metadata – only data relevant to the crime or investigation of criminal activity, or all data if provided for exculpatory purposes.	Parties to civil or criminal litigation, or other third parties, in response to a valid Defense Subpoena.

Frequency - Data sharing occurs at the following frequency:
As-needed per court order

Electronic communication data sharing shall comply with the provisions of the Electronic Communication Privacy Act, CA Penal Code §1546 – 1546.4

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose. Department data retention standards should align with how the department prepares its financial records and should be consistent with any relevant Federal Emergency Management Agency (FEMA) or California Office of Emergency Services (Cal OES) sections.

The Department’s data retention period and justification are as follows:

Retention Period	Retention Justification
1.) Intelligence Files, Evidence and Related Reports and Data will be retained for a minimum of two (2) years. Reports and data provided per warrant request to investigators is retained per the	Material (inculpatory and/or exculpatory) evidence must be preserved. Evidence is material if it is relevant to an important issue in the case, and evidence is exculpatory if it supports a defense or tends to show that a defendant is not guilty

<p>departments retention policy and times will vary per offense type.</p> <p>2.) Laboratory work product (casefiles, working copy of the device and reports) are stored by the SFPD CSI-Multimedia Evidence Unit indefinitely unless requested in writing or legal request to delete.</p> <p>Electronic communications are also retained pursuant to the provisions outlined in CA Penal Code §1546 – 1546.4</p> <p>For questions relating to retention timelines, please contact: SFPDChief@sfgov.org.</p>	<p>of the crime. Retention allows for any appeals process to occur or if further analysis is needed it will be available.</p> <p>Evidence, if deemed relevant to a criminal, civil, or administrative matter may be retained for a minimum period of 2 years and in accordance with federal/state law(s). Examples include:</p> <ul style="list-style-type: none"> -Incident/Citizen Contact -Misdemeanor Case (including report, statements, cite or arrest) -Runaway- Returned <p>Evidence, if deemed relevant to a criminal, civil, or administrative matter may be retained indefinitely, and in accordance with federal/state law(s). Examples include:</p> <ul style="list-style-type: none"> -Homicide -Violent Felony/DOA -Collision- Major Injury/Fatal -Sex Crimes -Internal Affairs Investigations -Officer Involved Shootings <p>Note: Evidence in multiple cases will use the longest retention policy for all of the cases.</p>
--	--

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed.

Per CA Penal Code §1546.1 (g) "If a government entity receives electronic communication information voluntarily provided pursuant to subdivision (f), it shall destroy that information within **90 days** unless one or more of the following circumstances apply:

- (1) The government entity has or obtains the specific consent of the sender or recipient of the electronic communications about which information was disclosed.
- (2) The government entity obtains a court order authorizing the retention of the information. A court shall issue a retention order upon a finding that the conditions justifying the initial voluntary disclosure persist, in which case the court shall

authorize the retention of the information only for so long as those conditions persist, or there is probable cause to believe that the information constitutes evidence that a crime has been committed.

(3) The government entity reasonably believes that the information relates to child pornography and the information is retained as part of a multiagency database used in the investigation of child pornography and related crimes.

(4) The service provider or subscriber is, or discloses the information to, a federal, state, or local prison, jail, or juvenile detention facility, and all participants to the electronic communication were informed, prior to the communication, that the service provider may disclose the information to the government entity.”

Exceptions to Retention Period - PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

- None

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

- If ordered by the court, evidentiary data will be securely wiped using forensic tools or destroyed.

COMPLIANCE

Department Compliance: Department shall oversee and enforce compliance with this Policy according to the respective memorandum of understanding of employees and their respective labor union agreement.

Allegations of 19B Violations: Members of the public may submit written notice of an alleged violation of Chapter 19B to SFPDChief@sfgov.org. If the Department takes corrective measures in response to such an allegation, the Department will post a notice within 30 days that generally describes the corrective measures taken to address such allegation. The Department will comply with allegation and misconduct processes as set forth by the city Charter.

If a Department is alleged to have violated the Ordinance under San Francisco Administrative Code Chapter 19B, Department shall post a notice on the Department’s website that generally describes any corrective measure taken to address such allegation.

Department is subject to enforcement procedures, as outlined in San Francisco Administrative Code Section 19B.8.

Oversight Personnel

Department shall be assigned the following personnel to oversee Policy compliance by the Department and third-parties.

Unit's command staff, depending on rank of sworn member using the technology.

- Q50-Q-52, Sergeant
- Q60-Q62, Lieutenant
- 0933 Crime Lab Manager
- 8262 Criminalist III
- 0955 Forensic Services Director

Unless assigned to Forensics Services, Q2 through Q62 data access is limited to the reports provided by the SFPD forensic practitioners or Forensic Services staff.

Sanctions for Violations - Sanctions for violations of this Policy include the following:

San Francisco Police Department will conduct an internal investigation through the Chief of Staff/Internal Affairs (IA) Unit or may refer the case to the Department of Police Accountability. The results of the investigation will be reported to the Chief of Police, who will determine the penalty for instances of misconduct. Under San Francisco Charter section A8.343, the Chief may impose discipline of up to a 10-day suspension on allegations brought by the Internal Affairs Division or the Department of Police Accountability. Depending on the severity of the allegation of misconduct, the Chief or the Department of Police Accountability may elect to file charges with the Police Commission for any penalty greater than the 10-day suspension. Any discipline sought must be consistent with principles of just cause and progressive discipline and in accordance with the SFPD Disciplinary Guidelines.

If a Department is alleged to have violated the Ordinance under San Francisco Administrative Code Chapter 19B, Department shall post a notice on the Department's website that generally describes any corrective measure taken to address such allegation.

Department is subject to enforcement procedures, as outlined in San Francisco Administrative Code Section 19B.8.

DEFINITIONS

Personally Identifiable Information: Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

Raw Data: Information collected by a surveillance technology that has not been processed and cleaned of all personal identifiable information. The distribution and use of raw data is tightly restricted.

AUTHORIZATION

Section 19B.4 of the City's Administrative Code states, "It is the policy of the Board of Supervisors that it will approve a Surveillance Technology Policy ordinance only if it determines that the benefits the Surveillance Technology ordinance authorizes outweigh its costs, that the Surveillance Technology Policy ordinance will safeguard civil liberties and civil rights, and that the uses and deployments of the Surveillance Technology under the ordinance will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class."

QUESTIONS & CONCERNS

Complaints of Officer Misconduct: Members of the public can register complaints about SFPD activities with the Department of Police Accountability (DPA), 1 South Van Ness Ave 8th Floor, San Francisco, CA 94103, (415) 241-7711, <https://sf.gov/departments/department-police-accountability>. DPA, by Charter authority, receives and manages all citizen complaints relating to SFPD use of force, misconduct, or allegations that a member has not properly performed a duty. DPA manages, acknowledges, and responds to complaints from members of the public.

Concerns and Inquiries: Department shall acknowledge and respond to complaints and concerns in a timely and organized response, and in the following manner: The Department has included a 19B Surveillance Technology Policy page on its public website : <https://www.sanfranciscopolice.org/your-sfpd/policies/19b-surveillance-technology-policies>. This page includes an email address for public inquiries: SFPDChief@sfgov.org. This email is assigned to several staff members in the Chief's Office who will respond to inquiries within 48 hours.

Inquiries from City and County of San Francisco Employees: All questions regarding this policy should be directed to the Chief of Police at SFPDChief@sfgov.org. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the Chief of Police at SFPDChief@sfgov.org



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:

Digital forensic tools are used for the following tasks:

- 1) To analyze computer volumes and mobile devices by filtering and sifting through data such as internet history, downloads, recent searches, locations media, messages, etc.

Surveillance Oversight Review Dates

PSAB Review: 2/24/2023; 6/29/2023

COIT Review: 9/21/2023

Board of Supervisors Approval: TBD

- 2) To extract data from digital devices.
- 3) To bypass locks and pass codes on mobile devices and computers.
- 4) To 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.
- 5) To organize results of digital forensic examinations.

As of the date of this STP, the tools in use are from the vendor Cellebrite (Inspector, Digital Collector and UFED 4PC).

Nothing herein prohibits procurement of additional data extraction/digital forensic tools provided the Department adheres to the authorized use(s) and prohibitions outlined in this STP.

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
----------------	--------------------

<input type="checkbox"/>	Education	
<input type="checkbox"/>	Community Development	
<input type="checkbox"/>	Health	
<input type="checkbox"/>	Environment	
<input checked="" type="checkbox"/>	Criminal Justice	Forensic computer analysis can be used to discover and document evidence in criminal investigations.
<input type="checkbox"/>	Jobs	
<input type="checkbox"/>	Housing	
<input type="checkbox"/>	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.

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
----------------	--------------------

<input checked="" type="checkbox"/>	Financial Savings	Forensic computer analysis can document and discover relevant files on devices quickly, reducing investigator hours examining devices.
<input checked="" type="checkbox"/>	Time Savings	Forensic computer analysis can document and discover relevant files on devices quickly, reducing investigator hours examining devices.
<input type="checkbox"/>	Staff Safety	
<input checked="" type="checkbox"/>	Data Quality	Forensic computer analysis provides investigators with specific and relevant documents from devices in criminal investigations.
<input type="checkbox"/>	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, Lieutenant 8252-8254 Forensic Examiner 8259-8262 Criminalists 0955 Forensic Services Director	
	Annual Cost	One-Time Cost
Total Salary & Fringe		
Software	\$35,520	
Hardware/Equipment		
Professional Services		
Training		
Other		
Total Cost	35,520	None

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

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.