Surveillance Technology Policy

Electronic Location Tracking Devices
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 Electronic Location Tracking Devices 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 or 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 Policy ("Policy") for Electronic Location Tracking Devices sets forth the parameters the devices will be used by describing the (1) intended purpose, (2) authorized use cases, (3) restricted uses, and (4) requirements.

This Policy applies to all Department personnel that use, plan to use, or plan to secure Electronic Location Tracking Devices, (hereinafter referred to as "surveillance technology"), 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.

The Department shall oversee and enforce compliance with this policy according to the respective memorandum of understanding between employees and their respective labor union agreement.

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 track a person, vehicle, or property in compliance with a search/arrest warrant or recognized search warrant exception [i.e. consent to search, exigent circumstances].
- To utilize as a vehicle pursuit mitigation option.

Surveillance Oversight Review Dates
PSAB Review: June 27, 2024
COIT Review: TBD
Board of Supervisors Review: TBD

Prohibitions and Restrictions

The Department may use information collected from surveillance technology only for legally authorized purposes. Electronic Location Tracking Devices shall not be used:

- To monitor, harass, intimidate, or discriminate against any individual or group based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data.
- For the 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, the Department shall not share any data collected 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.
- For a non-law enforcement related matter.
- If related to a vehicle pursuit, the electronic location tracking device must be removed, and location tracking must cease once officers apprehend the fleeing suspect vehicle.

BUSINESS JUSTIFICATION

Description of Technology

Electronic Location Tracking Device is defined as any device attached to a vehicle or other movable item that reveals its location or movement by the transmission of electronic signals as described in California Penal Code Section 637.7(d).

The Department utilizes the following Electronic Location Tracking Devices:

- Global Positioning System (GPS) tracking devices, which can be affixed to a vehicle or embedded within an item and provide location information via the Internet using Global Positioning System data. GPS tracking devices have a long range and do not have a distance limitation because of the utilization of GPS satellites which send the data to the device itself.
- Radio Frequency Identification (RFID) tracking devices can be embedded within an item and provide location information by using radio waves to identify the location of people or objects RFID tag and reader distance ranges up to 1,500 ft.
- Radio Frequency Beacon (RF Beacon) tracking devices are small, wireless Bluetooth-enabled devices that transmit signals to nearby smartphones or other devices and are often used for location-based services based on their proximity to the beacon. RF Beacon range is 1-500 ft

Reason for Technology Use

Electronic Location Tracking Devices support the Department's mission and provide important operational value in the following ways:

- Reduces the need to engage in vehicle pursuits by instead utilizing an electronic location tracking device to mitigate the risk to the public and protect human life, which is the highest priority of the SFPD.

- Allows officers to safely and expeditiously apprehend individuals who commit serious crimes.
- Allows officers to monitor suspect movements and patterns of the suspect and the vehicle remotely, if necessary. This can allow officers to gather the appropriate resources to facilitate a safe apprehension of the suspect and the vehicle, which ultimately reduces the risk to the officers, public, and the suspect(s).
- Provides officers with information on the location of evidence of a crime.
- Provides officers with information about the locations where suspect(s) take stolen property after the theft and where it is stored after being illegally sold.

Resident 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
X	Education	Presentations to the Police Commission or community meetings by the Department can demonstrate that Electronic Tracking Devices are de-escalation tools and can be used to assist in safely apprehending suspects
▪	Community Development	
X	Health	According to the CDC, community violence affects millions of people, and their families, schools, and communities every year. Community violence can cause significant physical injuries and mental health conditions such as depression, anxiety, and post-traumatic stress disorder. Successfully prosecuting major crime is an essential part of protecting life and building a healthy community.
▪	Environment	
X	Criminal Justice	Utilizing technology that provides location data remotely assists officers in safely apprehending suspects and/or evidence of a crime. Provides objective evidence to the prosecuting agencies.
▪	Jobs	
▪	Housing	
▪	Other	

Department Benefits

The Electronic Tracking Devices will benefit the Department in the following ways:

	Benefit	Description
X	Financial Savings	Using Electronic Location Tracking Devices can produce financial savings because officers are not required to conduct physical surveillance during the entire time the electronic tracking location device is active.
X	Time Savings	Using Electronic Location Tracking Devices alleviates Department officers from having to conduct constant physical surveillance, which enables them to handle other duties and tasks while the electronic tracking location device is active.
X	Officer and Community Safety	Electronic Location Tracking Devices allow Department officers to track vehicles out of sight and from a distance. Having the knowledge of the specific location of a vehicle or property enables officers to strategically deploy law enforcement resources to a precise location for intervention or apprehension of a suspect.
▪	Data Quality	
▪	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 Electronic Location Tracking Devices and information collected, retained, processed, or shared by this 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: The department shall only collect data required to meet the needs of the authorized use cases. All data collected by Electronic Tracking Devices, including PII, shall be classified according to the City's Data Classification Standard.

The Electronic Location Tracking Devices collects some or all the following data type(s):

Data Type(s)	*Format(s)*	*Classification*
IMEI # of the GPS tracking device. Speed MPH	CSV, PDF, HTML, JSON/XML	Level 3 or 4

KML
Latitude & Longitude
Speed (in miles per hour)
Direction (compass)
Agency Name & Address
Vehicle Number
Vehicle Speed
Internal Event Number (code showing activity of the tracking device ie: orientation, position etc.
Agency Point of Contact (name, contact email, telephone number)

.

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

Only Department officers may access and operate electronic location tracking devices and any access must be related to a criminal investigation.

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 surveillance technology:

- Authorized non-sworn officers designated and trained by the Chief of Police to utilize the Electronic Location Tracking Devices. Q2-Q4, Police Officer
- Q35-Q37, Assistant Inspector
- Q0380- Q0382, Inspector
- Q50-Q-52, Sergeant
- Q60-Q62, Lieutenant
- Q80-Q82, Captain
- 0488-0490, Commander
- 0400-0402, Deputy Chief

- 0395, Assistant Chief
- 0390, Chief of Police
- 1822, Administrative Analyst

B. Members of the public

The 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 Electronic Location Tracking Devices or their associated data will be misused or used contrary to its authorized use, all individuals requiring access to the associated data must receive training on data security policies and procedures.

The 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. The 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.

Data Security: The 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.

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

The Department Technology Division will ensure that data security aligns with the FBI's Criminal Justice Information Services Division (CJIS) standards which is an

important compliance standard for law enforcement at the local, state, and federal levels, and is designed to ensure data security in law enforcement. The Department maintains compliance with requirements established and enforced by the Department of Justice California Law Enforcement Telecommunications (CLETS). The Department ensures all contractors and vendors who have access or exposure to Confidential Offender Record Information (CORI) have fulfilled training and background requirements. Click here for CLETS Policies, Practices and Procedures.

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.)

- Department of Technology Data Center

X Software as a Service Product

X Cloud Storage Provider

Data Sharing: The Department will endeavor to ensure that other agencies or departments that may receive data collected by the surveillance technology will act in conformity with this Policy.

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.

The 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)*

The 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.
- Redact names and ensure all PII is removed in accordance with the Department's data policies.
- 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
CSV, PDF, HTML, JSON/KML	District Attorney's Office, California Attorney General's Office, United States Attorney's office for use as evidence to aid in prosecution, in accordance with laws governing evidence.
CSV, PDF, HTML, JSON/KML	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:

- As needed
- Upon request
- As required by law or court order

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
CSV, PDF, HTML, JSON/KML	Law enforcement partners, as part of a criminal or administrative investigation; Parties to civil litigation, or other third parties, in response to a valid court order.

Frequency - Data sharing occurs at the following frequency:

- As needed
- Upon request
- As required by law or court order

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
Minimum of 2 years. All investigative files shall be maintained according to the California Penal Code, Evidence Code, and according to local, state and federal law.	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 of the crime. Retention allows for any appeals process to occur or if further analysis is needed it will be available. 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: -Incident/Citizen Contact -Misdemeanor Case (including report,

	statements, cite or arrest) -Runaway- Returned Evidence, if deemed relevant to a criminal, civil, or administrative matter is retained indefinitely, and in accordance with federal/state law(s). Examples include: -Homicide -Violent Felony/DOA -Collision - Major Injury/Fatal -Sex Crimes Note: Evidence in multiple cases will use the longest retention policy for all the cases.

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 is processed.

Data Disposal: Upon completion of the data retention period, the Department shall dispose of data in the following manner: Data destruction via deleting/wiping/erasing/degaussing or otherwise making the data irretrievable.

COMPLIANCE

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: The Department shall be assigned the following personnel to oversee Policy compliance by the Department and third parties:

Unit Oversight is as follows:

- Q50-Q-52, Sergeant
- Q60-Q62, Lieutenant
- Q80-Q82, Captain

Sanctions for Violations: San Francisco Police Department will conduct an internal investigation though 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

Exigent Circumstances	An emergency requiring swift action to prevent imminent danger to life or severe damage to property.
Personally Identifiable Information (PII):	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 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. 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.