File No. 250979 **Committee Item No.** 2
Board Item No. 8

COMMITTEE/BOARD OF SUPERVISORS

AGENDA PACKET CONTENTS LIST

Committee: Rules Committee **Date** Feb 9, 2026

Board of Supervisors Meeting **Date** March 10, 2026

Cmte Board

☐	☐	**Motion**
☐	☐	**Resolution**
☒	☐	**Ordinance**
☒	☐	**Legislative Digest**
☐	☐	**Budget and Legislative Analyst Report**
☐	☐	**Youth Commission Report**
☐	☐	**Introduction Form**
☒	☐	**Department/Agency Cover Letter and/or Report**
☐	☐	**Memorandum of Understanding (MOU)**
☐	☐	**Grant Information Form**
☐	☐	**Grant Budget**
☐	☐	**Subcontract Budget**
☐	☐	**Contract/Agreement**
☐	☐	**Form 126 - Ethics Commission**
☐	☐	**Award Letter**
☐	☐	**Application**
☐	☐	**Form 700**
☐	☐	**Information/Vacancies (Boards/Commissions)**
☐	☐	**Public Correspondence**

OTHER **(Use back side if additional space is needed)**

☒	☐	Surveillance Technology Policy
☒	☐	Surveillance Impact Report
☐	☐	
☐	☐	
☐	☐	
☐	☐	
☐	☐	
☐	☐	
☐	☐	

Completed by: Victor Young **Date** Feb 5, 2026
Completed by: _____ **Date** _____

[Administrative Code - Police Surveillance Technology Policy for Electronic Location Tracking Devices]

Ordinance approving the Police Surveillance Technology Policy for electronic location tracking devices and making required findings.

NOTE: **Unchanged Code text and uncodified text** are in plain Arial font.
Additions to Codes are in *single-underline italics Times New Roman font*.
Deletions to Codes are in ~~*strikethrough italics Times New Roman font*~~.
Board amendment additions are in double-underlined Arial font.
Board amendment deletions are in ~~strikethrough Arial font~~.
Asterisks (* * * *) indicate the omission of unchanged Code subsections or parts of tables.

Be it ordained by the People of the City and County of San Francisco:

Section 1. Background.

(a) Terms used in this ordinance have the meaning set forth in Administrative Code Chapter 19B ("Chapter 19B").

(b) Chapter 19B regulates City departments' acquisition and use of Surveillance Technology. Proposition E, approved by the voters in March 2024, amended Chapter 19B to authorize the Police Department to acquire or use surveillance technology for up to one year before Board action. Under Administrative Code Section 19B.2(c), the Police Department must submit a proposed surveillance technology policy to the Board for approval by ordinance within one year of the use or acquisition and may continue to use the surveillance technology after the end of that year unless the Board adopts an ordinance that disapproves the policy.

(c) Under Administrative Code Section 19B.2(b), the Board of Supervisors may approve a Surveillance Technology Policy ordinance following a public hearing at which the Committee on Information Technology ("COIT") considers a proposed Surveillance

Technology Policy and recommends that the Board adopt, adopt with modifications, or decline to adopt the Surveillance Technology Policy for the Surveillance Technology to be acquired or used.

(d) Under Administrative Code Section 19B.3(b), the department seeking approval under Section 19B.2 must submit to the Board and publicly post on the department website a Surveillance Impact Report and a proposed Surveillance Technology Policy ordinance at least 30 days prior to the first public meeting where the Board will consider the Policy.

(e) Under Administrative Code Section 19B.4, the Board will approve a Surveillance Technology Policy ordinance only if it determines that the benefits outweigh the costs, the Policy will safeguard civil liberties and civil rights, and the authorized uses and deployments will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(f) The Police Department initiated a pilot use of projectile Global Positioning System (GPS) electronic location tracking technologies pursuant to Field Operations Bureau Order No. 24-01 (StarChase Pilot Program) issued on October 22, 2024, which established training, deployment, coordination, and post-use reporting requirements.

Section 2. Surveillance Technology Policy for Police Department Use of Electronic Location Tracking Devices.

(a) Purpose. The Police Department seeks Board authorization under Section 19B.2(a) to use Electronic Location Tracking Devices, including GPS tags (e.g., projectile devices), Radio Frequency Identification (RFID) devices, and Radio Frequency Beacon devices, for the following authorized purposes as set forth in the Department's Surveillance Technology Policy ("Policy"): (1) to track a person, vehicle, or property in compliance with a search or arrest warrant, or a recognized warrant exception (e.g., consent or exigent circumstances),

consistent with California Penal Code Sections 1534 and 637.7; (2) to serve as a vehicle pursuit-mitigation option consistent with Department General Order 5.05 (Response and Pursuit Driving) and Administrative Code Section 96I.2(d); and (3) to aid Theft Abatement Operations. The Policy prohibits use for non-law-enforcement purposes; prohibits monitoring, harassment, intimidation, or discrimination based on protected characteristics; prohibits use to enforce prohibitions on gender-affirming or reproductive care or related interstate travel; and requires termination of tracking upon apprehension in projectile-device deployments.

(b) Surveillance Impact Report. The Police Department submitted to COIT a Surveillance Impact Report for Electronic Location Tracking Devices. A copy of the Surveillance Impact Report is in Board File No. 250979, and is incorporated herein by reference.

(c) Public Hearings and COIT Recommendation. On June 27, 2024 and July 19, 2024, the Privacy and Surveillance Advisory Board held public hearings to consider the Surveillance Impact Report and proposed Policy; and on September 19, 2024, COIT held a public hearing to consider the Policy and recommended that the Board adopt it. A copy of the Policy ("San Francisco Police Department Electronic Location Tracking Devices Policy") is in Board File No. 250979, and is incorporated herein by reference.

(d) Pilot Period. The Police Department's pilot use of Electronic Location Tracking Devices pursuant to Proposition E is concluding. The Police Department has proposed the Surveillance Policy to the Board for its approval. Pursuant to Administrative Code Section 19B.2(c)(1), the Police Department may continue to use the technology unless the Board adopts an ordinance that disapproves the Policy.

Section 3. Findings.

The Board of Supervisors hereby finds that the benefits of the Police Department's use

of Electronic Location Tracking Devices outweigh the costs and risks; that the Policy will safeguard civil liberties and civil rights; and that the uses and deployments of Electronic Location Tracking Devices, as set forth in the Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or a Protected Class.

Section 4. Approval of Policy.

Based on the findings stated above, The Board of Supervisors hereby approves the Police Department's Surveillance Technology Policy for the use of Electronic Location Tracking Devices, including projectile GPS devices used as a pursuit-mitigation option, consistent with the Surveillance Impact Report and the Policy considered by COIT and referenced in Sections 2(b) and (c) of this ordinance.

Section 5. Effective Date. This ordinance shall become effective 30 days after enactment. Enactment occurs when the Mayor signs the ordinance, the Mayor returns the ordinance unsigned or does not sign the ordinance within ten days of receiving it, or the Board of Supervisors overrides the Mayor's veto of the ordinance.

APPROVED AS TO FORM:
DAVID CHIU, City Attorney

By: */s/ Jen Huber*
JEN HUBER
Deputy City Attorney

n:\legana\as2025\2600076\01872145.docx

FILE NO. 250979

LEGISLATIVE DIGEST

[Administrative Code - Police Surveillance Technology Policy for Electronic Location Tracking Devices]

Ordinance approving the Police Surveillance Technology Policy for electronic location tracking devices and making required findings.

Background Information

Administrative Code Chapter 19B (Chapter 19B) regulates City Departments' acquisition and use of surveillance technology. Under Chapter 19B, Section 19B.2(c), the Police Department must submit a proposed surveillance technology policy to the Board for approval by ordinance within one year of the use or acquisition and may continue to use the surveillance technology after the end of that year unless the Board adopts an ordinance that disapproves the policy.

On September 19, 2024, the Committee on Information Technology held a public hearing to consider the Police Department's proposed Surveillance Technology Policy ("Policy") for Electronic Location Tracking Devices and recommended that the Board of Supervisors adopt it.

The Police Department initiated a pilot use of projectile Global Positioning System (GPS) electronic location tracking technologies pursuant to Field Operations Bureau Order No. 24-01 (StarChase Pilot Program) issued on October 22, 2024. The Police Department seeks Board authorization under Section 19B.2(a) to continue to use Electronic Location Tracking Devices, including GPS tags (e.g., projectile devices), Radio Frequency Identification (RFID) devices, and Radio Frequency Beacon devices, for the following authorized purposes as set forth in the Policy: (1) to track a person, vehicle, or property in compliance with a search or arrest warrant, or a recognized warrant exception (e.g., consent or exigent circumstances), consistent with California Penal Code Sections 1534 and 637.7; (2) to serve as a vehicle pursuit-mitigation option consistent with Department General Order 5.05 (Response and Pursuit Driving) and Administrative Code Section 96I.2(d); and (3) to aid Theft Abatement Operations. The Policy prohibits use for non-law-enforcement purposes; prohibits monitoring, harassment, intimidation, or discrimination based on protected characteristics; prohibits use to enforce prohibitions on gender-affirming or reproductive care or related interstate travel; and requires termination of tracking upon apprehension in projectile-device deployments.

n:\legana\as2025\2600076\01872151.docx

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/arrest warrant exception [i.e. consent to search, exigent circumstances]. Cal. Pen. Code § 1534. Cal. Pen. Code § 637.7
- To utilize as a vehicle pursuit mitigation option consistent with all applicable SFPD written directives. Vehicle pursuits shall comply with SFPD *Department General Order 5.05 Response and Pursuit Driving* & SF Admin Code 96I.2(d)

Surveillance Oversight Review Dates
PSAB Review: June 27, 2024 & July 19, 2024
COIT Review: September 19, 2024
Board of Supervisors Review: TBD

- To aid Theft Abatement Operations

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 using a projectile electronic location tracking device during 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 Location 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	XLS/XLSX, CSV, PDF, HTML, JSON/XML KML	Level 3
Latitude & Longitude		
Vehicle Speed (in miles per hour)		
Direction (compass)		
Distance traveled (historical and/or real-time)		
Agency Name & Address		
Vehicle Alias Number		
Internal Event Number (code showing activity of the tracking device i.e.: 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 employees designated 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
- 1823, Senior Administrative Analyst
- 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
XLS/XLSX, 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.

XLS/XLSX, 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
XLS/XLSX, 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.	Material (inculpatory and/or exculpatory) evidence must be preserved. Evidence is material if it is

All investigative files shall be maintained according to the California Penal Code, Evidence Code, and according to local, state and federal law.	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.
Theft Abatement Operations	Operations that are a coordinated effort between plainclothes officers and uniformed officers to address retail, vehicle or other organized theft. This can include Bait Car Operations, Fencing Operations or coordinated efforts with retail loss prevention officers.

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.

Surveillance Impact Report

Electronic Location Tracking Devices
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 Police Department's ("SFPD" or "Department") use of Electronic Location Tracking Devices.

PURPOSE OF THE TECHNOLOGY

Pursuant to the San Francisco Charter, 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. SFPD'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.

Electronic Location Tracking Devices may be utilized to increase officer safety, enhance the SFPD ability to gain information about the locations of suspects, where suspect(s) have taken stolen property after a theft, or to have a vehicle pursuit alternative which can mitigate the risk to the public and protect human life.

SFPD shall use Electronic Location Tracking Devices only for the following authorized uses:

Authorized Use(s):

- To track a person, vehicle, or property in compliance with a search/arrest warrant or recognized search/arrest warrant exception [i.e. consent to search, exigent circumstances]. Cal. Pen. Code § 1534. Cal. Pen. Code § 637.7
- To utilize as a vehicle pursuit mitigation option consistent with all applicable SFPD written directives. Vehicle pursuits shall comply with SFPD Department General Order 5.05 *Response and Pursuit Driving* & SF Admin Code 96I.2(d)
- To aid Theft Abatement Operations

Prohibitions and Restrictions:

SFPD may use information collected from Electronic Location Tracking Devices 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 using a projectile electronic location tracking device during a vehicle pursuit, the electronic location tracking device must be removed, and location tracking must cease once officers apprehend the fleeing suspect vehicle.

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.
- Both RFID and RF Beacon tracking devices have a shorter range because they track items within a limited range from the device, typically a few meters.

Third-Party Vendor Access to Data

Data collected or processed by Electronic Location Tracking Devices will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. SFPD will manage and control all data collected by the Electronic Location Tracking Device and SFPD remain the sole Custodian of Records. *See Physical Safeguards for further information.*

IMPACT ASSESSMENT

The impact assessment addresses the conditions for Electronic Location Tracking Devices' approval, as outlined by the Standards of Approval in San Francisco Administrative Code, Section 19B:

1. The benefits of Electronic Location Tracking Device outweigh the costs.
2. SFPD's Policy safeguards civil liberties and civil rights.
3. The uses and deployments of the Electronic Location Tracking Device are not based upon discriminatory or viewpoint-based factors and do not have a disparate impact on any community or protected class.

SFPD's use of Electronic Location Tracking Devices are intended to support and benefit the residents of San Francisco while minimizing and mitigating costs and potential civil rights and liberties impacts on residents.

A. Benefits

SFPD's use of the Electronic Location Tracking Device 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 SFPD 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 Electronic Location Tracking Device that provides location data remotely assists SFPD in safely apprehending suspects and/or evidence of a crime. Provides objective evidence to the prosecuting agencies.

- ☐ Jobs
- ☐ Housing
- ☐ Other

B. Civil Rights Impacts and Safeguards

SFPD strives to mitigate potential civil rights impacts by strictly adhering to the authorized uses and by listing prohibitions and restrictions in the policy as it relates to Electronic Location Tracking Device SFPD has considered the potential impacts to individuals right to privacy, warrantless searches and equal protection of the law and has identified the administrative, technical, and physical protections as mitigating measures as detailed below:

Right to Privacy- SFPD affirms that individuals have the Right to Privacy and freedom of expression in conformance with and consistent with local, state, and federal laws. SFPD strives to mitigate all potential civil rights impacts through responsible technology and associated data use policies and procedures. SFPD intends to use Electronic Location Tracking Device and their associated data exclusively for the authorized uses listed in the surveillance technology policy and impact reports, and in conjunction with SFPD Department General Order 5.16 Search Warrants, which is overseen by the San Francisco Police Commission. Only data that is related to a criminal investigation will be shared with the appropriate parties as listed in the Data Sharing section of the policy. SFPD intends to use Electronic Location Tracking Device 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] and to utilize as a vehicle pursuit option.

Warrantless Searches - In the United States, warrantless searches are restricted under the Fourth Amendment to the United States Constitution as part of the Bill of Rights: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." SFPD will not use Electronic Location Tracking Devices absent a search warrant, or recognized warrant exception (e.g. consent, exigent circumstances, etc.), or outside of the authorized uses listed in the policy.

Equal Protection of the Law- Under the 14th Amendment, people in similar situations shall be treated equally under the law. SFPD will not use electronic location tracking devices to monitor individuals or groups based on a protected category such as - race, gender, religion, or sexual orientation, ensuring enforcement is based only on addressing criminal conduct.

Administrative Safeguards-Each SFPD officer belongs to a chain of command. The Officer in Charge (OIC) of that chain of command is responsible for overseeing compliance with all SFPD rules and regulations. If allegations arise that an officer is not in compliance, the OIC will initiate an investigation

and will take the appropriate action which could include an investigation of misconduct by Internal Affairs and/or the Department of Police Accountability (DPA).

There is an understandable concern with law enforcement utilizing this technology without probable cause of a crime or identifiable law enforcement purposes. Maintaining a list of specific authorized uses for the Electronic Location Tracking Devices will mitigate the usage of data for purposes other than that for which the data was originally collected and ensure the public is aware of its restrictions.

Technical Safeguards-Electronic Location Tracking Devices currently in use, including interfaces, firmware, and operating systems, mitigate unauthorized access to the network and instead only allows necessary device functionality. The data from Electronic Location Tracking Devices used are securely stored by the service provider. Access to the footage is limited to SFPD officers and levels of access are based on role-based permissions. To safeguard evidence integrity, evidence contained within the cloud uses forensic fingerprint of each evidence file using industry standard Secure Hash Algorithms (SHA) hash function. Integrity is validated before and after upload to ensure no changes occur during transmission. Evidence data in transit is FIPS 140-2 validated, and the system is fully compliant with the FBI's Criminal Justice Information Services (CJIS) standards (NSA Suite B 256-bit AES encryption). Additionally, there are full tamper-proof audit records for each evidence file. These records cannot be edited or changed.

Physical Safeguards-Electronic Location Tracking Device access will be limited to SFPD officers who are authorized to use the Electronic Location Tracking Device. Data will be digitally stored into the SFPD's digital evidence storage or uploaded to a storage device and booked into evidence in accordance with evidence booking procedures. All digital evidence captured, recorded, or otherwise produced by the Electronic Location Tracking Device equipment is the sole property of the SFPD. All digital evidence shall be handled in accordance with existing policy on evidence management. SFPD officers shall not edit, alter, erase, duplicate, copy, share, or otherwise distribute digital evidence in any manner without prior authorization from the appropriate designated personnel.

C. Fiscal Analysis of Costs and Benefits

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

Number of Budgeted FTE (new & existing) & Classification	No dedicated FTE (new & existing) for deployment of this tool. SFPD Officers will use the Electronic Location Tracking Device during regular or overtime operations during their regular assigned duties.	
	Annual Cost	***One-Time Cost***

Total Salary & Fringe		
Software	*$44,405.48*	
Hardware/Equipment		$39,117.10
Professional Services	*$15,120*	
Training		
Other		
Total Cost	***$59,525.48***	***$39,117.10***

SFPD funds its use and maintenance of surveillance technology through its Operating Budget, Vehicle Theft Abatement Funds and/or grant funding.

COMPARISON TO OTHER JURISDICTIONS

Law Enforcement Agencies: The following law enforcement agencies currently have Electronic Location Tracking Device and have incorporated it in their department policies and procedures for authorized use specifically during vehicle pursuits:

- Pittsburg Police Department
- Fremont Police Department
- Oakland Police Department
- Redmond Police Department

Electronic Location Tracking Devices are currently utilized by other governmental entities for similar purposes.

For instance, 30+ police departments throughout the United States as well as agencies from every level of government domestically (local, county, state, and federal) and numerous countries worldwide are utilizing a newer GPS technology called StarChase. The technology can be described as an air pressure system attached to the front of a police vehicle that contains a GPS tag/dart. When activated, the tag is released from the police vehicle, affixes to the suspect vehicle, and reports GPS data of the suspect vehicle.

RELATED REMARKS

StarChase LLC: According to Cary Goldberg, who is the National Business Development Manager for StarChase company, law enforcement's use of their GPS tracking technology has currently resulted in

apprehension rates of 86%, which has contributed to significant decreases in injuries, fatalities, and property damage to police officers, suspects, and the public.

ACLU: Jay Stanley, a Senior Policy Analyst for the ACLU Speech, Privacy and Technology Project, made comments in response to numerous inquiries about the new GPS technology. Stanley stated the following: "I don't see any problem with this technology, assuming that it is used in the kind of way that everybody probably imagines it being used. In other words, that:

- It is used only in police chases that commence when a police officer has the equivalent of probable cause of wrongdoing (even if just fleeing a temporary detention like a traffic stop) and do not have time to get a warrant.
- The device is removed, and the location tracking ends the first time the police catch up to the person they are chasing.
- The police catch up to the suspect as soon as they can (in other words, no letting them wander around for extended periods of time without pursuing them, in order to learn things about them).

Any other uses of GPS tracking technology outside the heat of a chase should require a search warrant. And on the other side of the equation, this has the potential to obviate the need for high-speed pursuits by police cars through cities and towns, which are very dangerous and kill hundreds each year, with a third or more of those fatalities being innocent bystanders."

OFFICE OF THE MAYOR
SAN FRANCISCO

DANIEL LURIE
MAYOR

TO: Angela Calvillo, Clerk of the Board of Supervisors
FROM: Adam Thongsavat, Liaison to the Board of Supervisors
RE: Administrative Code - Police Surveillance Technology Policy for Electronic Location Tracking Devices
DATE: September 30, 2025

Ordinance approving the Police Surveillance Technology Policy for electronic location tracking devices and making required findings.

Should you have any questions, please contact Adam Thongsavat at adam.thongsavat@sfgov.org

1 DR. CARLTON B. GOODLETT PLACE, ROOM 200
SAN FRANCISCO, CALIFORNIA 94102-4681
TELEPHONE: (415) 554-6141

BOARD of SUPERVISORS

City Hall
1 Dr. Carlton B. Goodlett Place, Room 244
San Francisco 94102-4689
Tel. No. (415) 554-5184
Fax No. (415) 554-5163
TDD/TTY No. (415) 554-5227

M E M O R A N D U M

TO: Paul Yep, Interim Police Chief, Police Department

FROM: Victor Young, Assistant Clerk

DATE: October 7, 2025

SUBJECT: LEGISLATION INTRODUCED

The Board of Supervisors' Rules Committee received the following proposed Ordinance:

File No. 250979

Ordinance approving the Police Surveillance Technology Policy for electronic location tracking devices and making required findings.

If you have comments or reports to be included with the file, please forward them to Victor Young at the Board of Supervisors, City Hall, Room 244, 1 Dr. Carlton B. Goodlett Place, San Francisco, CA 94102 or by email at: victor.young@sfgov.org.

(attachment)

c. Steven Lopez, Police Dept.
Carl Nicita, Police Dept.
Giannina Miranda, Police Dept.