Surveillance Technology Policy

San Francisco Police Department
Automated License Plate Readers (ALPR)

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 ALPR 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

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 the ALPR 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 secure ALPR data, 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 ALPR technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

1. Locate stolen, wanted, and or other vehicles that are the subject of investigation
2. To apprehend wanted persons subject to arrest warrants or who are otherwise lawfully sought by law enforcement.
3. To locate victims, witnesses, suspects, missing children, adults, and/or elderly individuals, including in response to Amber Alerts and Silver Alerts and others associated with a law enforcement investigation.
4. To assist with criminal investigations initiated by local, state and regional public safety departments by identifying vehicles associated with targets of criminal investigations.
5. Counter-terrorism: Identify potential threats to critical infrastructure sites.
6. For other law enforcement purposes as authorized by law: Investigations of major crimes.

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

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

Surveillance Oversight Review Dates
COIT Review: January 21, 2021
Board of Supervisors Review: August 4, 2021

opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data. Additionally, departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

- An ALPR alert alone does not substantiate law enforcement response or contact. Contacting an individual solely based on an ALPR alert in the absence of confirming disposition of the vehicle (stolen or recovered), verifying that the observed license plate number matches the ALPR data, and verifying the reason a vehicle or owner is wanted or of interest shall be prohibited.
- No SFPD member shall access ALPR data for any use other than the authorized use cases herein
- ALPR scanning is limited to vehicles exposed to public view.
- No content captured by ALPR cameras other than license plate and vehicle information, geo-location, and time date of capture, shall constitute cause for police enforcement.

BUSINESS JUSTIFICATION

ALPR supports the Department's mission and provides important operational value in the following ways:

ALPR readers allow for automatic and efficient identification of license plates that may be associated with criminal activity or missing persons. The identification of a license plate allows SFPD to recover a victim's vehicle, investigate a crime and lawfully apprehend suspects. SFPD is able to protect life and property using this technology.

In addition, ALPR promises to benefit residents in the following ways:

☐	Education	
☐	Community Development	
☐	Health	
☐	Environment	
X	Criminal Justice	On-street enforcement of: Stolen Vehicles; Amber Alerts; Unregistered Vehicles; Wanted Criminals; Parking Violations; Be on the Lookout (BOLO), assists criminal investigations
☐	Jobs	
☐	Housing	

In addition, the following benefits are obtained:

Benefit		Description
☐	Financial Savings	
X	Time Savings	
X	Staff Safety	
☐	Data Quality	

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 kept up to date and maintained.
Safety:	Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.
Data Collection:	Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology. Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard. Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

The surveillance technology collects the following data types:

Data Type(s)	*Format(s)*	*Classification*
Digital images of vehicle license plates and their associated vehicles	Encoded and stored in SQL	Level 3
Date and time the license plate passes a digital-image site where an ALPR is located	SQL server datetime	Level 3

Notification: Decals identifying that ALPR is in use will be placed on marked patrol vehicles outfitted with ALPR. Decals will not be placed on unmarked vehicles outfitted with ALPR, as it poses operational and officer safety issues. Posted signs are not logistically feasible as marked patrol vehicles are constantly reassigned based on operational needs, which fluctuate.

The public notice shall include the following items in its public notice:

- X Type of technology in use
- ☐ Information on the surveillance technology
- ☐ Description of the authorized use
- ☐ Type of data collected
- ☐ Will persons be individually identified
- ☐ Data retention
- ☐ Department identification
- ☐ Contact information

Access: All parties requesting access must adhere to the following rules and processes: US DOJ's

*California Law Enforcement Telecommunications System (CLETS) rules and regulations, NCRIC ALPR policy, Dept. Bulletin 15-221 and DGO 10.08, SFPD members must be approved to access the ALPR data and the data must be tied to an investigation and per.

*CLETS is the computer network that connects public safety agencies across the state to criminal histories, driver records, and other databases. DOJ grants each public safety agency's access.

Officers shall not stop a vehicle solely based on an ALPR alert. Before stopping a vehicle based on an ALPR alert for a stolen or felony want, the officer conducting the stop shall:

1. Visually verify the alphanumeric characters on the plate of the suspect vehicle to be detained, AND
2. Verify through CLETS or through the Department of Emergency Management (dispatch has CLETS access) that the license plate on the vehicle to be detained is currently listed on the DOJ database as stolen or wanted.

Other ALPR alerts (e.g. 852 "auto boost", 459 "burglary", 10-43 "of interest to special investigation", etc.) do not provide officers with justification to conduct a traffic stop or detain a vehicle and the occupants. Sufficient probable cause has not been established to stop a "vehicle of interest" that is the focus of a criminal investigation.

These alerts may provide officers with additional instructions or information when a vehicle is located.

Officers should follow the instructions on the alert, use discretion, and have independent probable cause to justify a traffic stop.

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.

- Sworn members, Civilian Crime analysts, Radio Shop Technicians (access to hardware)

The following providers are required to support and maintains the surveillance technology and its associated data to ensure it remains functional:

- NCRIC hosts the ALPR data repositories. Vehicle Theft Abatement Funds pay for maintenance.

B. Members of the public

ALPR data is classified as Level 3 Sensitive. ALPR data has previously been deemed as exempt from the California Public Records Act, however each request submitted by a member of the public will be reviewed to determine whether the data can be released. SFPD shall comply with the requirements of the Federal and State Constitutions, and federal and State civil procedure laws and rules.

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). To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards: Northern California Regional Intelligence Center (NCRIC) hosts the ALPR data collected by SFPD equipment. Only Authorized SFPD members with an account can access the repository of data via the Back Office Server Software (BOSS) application. SFPD Information Technology Division and Special Investigations Division will not grant user access to ALPR data unless they are approved to do so. All SFPD members are required to comply with CLETS and department written directives. Non-compliance may result in progressive discipline measures.
Data Sharing:	If the ALPR data is not exempt from California Public Records Act, SFPD 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. SFPD will endeavor to ensure that other agencies or departments that may receive data collected by [the Surveillance Technology Policy that it operates] will act in conformity with this Surveillance Technology 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. SFPD 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) SFPD shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded. Each department that believes another agency or department receives or may receive data collected from its use of STs should consult with its assigned deputy city attorney regarding their response.

The Department currently participates in the following sharing practices:

A. Internal and External Data Sharing

Department shares the following data with the recipients:

- District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence;
- Public Defender's Office or criminal defense attorney via the District Attorney's Office in accordance with California discovery laws
- Data sharing occurs at the following frequency: as-needed

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

X 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, scrub faces, and ensure all PII is removed in accordance with the department's data policies.

X 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 shared data will be done in a cost-efficient manner and exported in a clean, machine-readable format.

B. External Data Sharing:

Department shares the following data with the recipients:

- NCRIC 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.
- Data sharing occurs at the following frequency: as-needed.

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall:

- Comply with all applicable laws, rules, and regulations, including but not limited to, to the extent applicable, the California Values Act (Government Code Section 7284 et seq.).

If Department's general counsel determines ALPR data can be disclosed in response to a public information request, the department will redact PII as it will be considered investigative/evidentiary material. The Department may use its discretion when releasing investigative/evidentiary material per SFPD DGO 3.16.

Data Retention:

Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.

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

SFPD defers to the NCRIC retention standard: ALPR records are maintained for 12 months from capture. If a record is connected to a criminal investigation or criminal intelligence file it may be retained for 5 years.

ALPR Technology data associated with a criminal investigation may be downloaded onto an electronic storage device or printed. Downloaded, copied, and printed data shall be maintained in accordance with applicable local, state and federal evidentiary laws, to include retaining the data through the adjudication of a case in a recognized court of law, as well as allotment of time for an appeals process and statute of limitations.

ALPR does not collect PII data and as such PII data shall not be kept in a form which permits identification of data subjects

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will be stored in the following location:

- ☐ Local storage
- ☐ Vendor managed storage
- ☐ Department of Technology Data Center
- ☐ Software as a Service Product
- ☐ Cloud Storage Provider

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

Practices: ALPR data are cleared after 1 year from capture unless associated with a criminal investigation.

	Processes and Applications: If ALPR data is associated with a criminal investigation and must be disposed of due to retention schedule, confidential information shall be disposed of according to SFPD Department Notice 20-166: https://www.sanfranciscopolice.org/sites/default/files/2020-08/SFPDNotice20.116.20200804.pdf CLETS Information (print-outs, CDs, Flash Drives, Diskettes or any other storage media) no longer has a necessary law enforcement purpose, members shall dispose of it in the following manner: • Hard copies and print-outs - with the exception of staples and paper clips - shall be placed in the gray colored Shred Works shredding bins. Facility Coordinators, or other designated SFPD employees, shall ensure that these bins are always located in a secure area of the SFPD facility. • If a member has stored CLETS Information on any electronic storage media, the member shall be responsible for its proper destruction.
Training:	To reduce the possibility that surveillance 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. NCRIC provides training information to the Department.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

These policies will have the same compliance requirements as all Department Written Directives and Police Commission Resolutions.

The Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties: Deputy Chief of Investigations, Lieutenant of Special Investigations Division.

In addition, each member of the department belongs to a chain of command. The Officer in Charge (OIC) of that chain of command is responsible for overseeing compliance with all SFPD written directives and the surveillance technology polices. If allegations arise that a member 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.

Sanctions for violations of this Policy include the following:

San Francisco Police Department will conduct an internal investigation though the Chief of Staff/Internal Affairs (IA) Unit. 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 DPA. Depending on the severity of the allegation of misconduct, the Chief or the DPA 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.
Sensitive Data:	Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions.
Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.

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

Public:

Members of the public can register complaints with the Department of Police Accountability (DPA). 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.

Department shall acknowledge and respond to concerns in a timely and organized response. To do so, Department shall:

SFPD will update the SFPD public website to include surveillance technology policies and will include a general email address for public inquiries. The general email box will be assigned to a staff member in the Chief's Office.

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.