Surveillance Technology Policy

Parking Enforcement ALPR Technology
Municipal Transportation Agency

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 Parking Enforcement ALPR Technology 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: connect San Francisco through a safe, equitable, and sustainable transportation system.

The Surveillance Technology Policy ("Policy") defines the manner in which the Parking Enforcement ALPR Technology 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 Parking Enforcement ALPR 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.

POLICY STATEMENT

The authorized use of Parking Enforcement 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):

Identify vehicles parked on city streets in violation of time-limited parking restrictions.
Identify vehicles parked on city streets that have five or more unpaid parking citations.
Identify vehicles parked on city streets that are listed on SFPD's hotlist of stolen vehicles. Hotlists contain license plate numbers and state of vehicles reported stolen. Hotlist is transmitted via Secure FTP. Hotlist is updated/overwritten daily. The SFMTA does not generate hotlists.
Future use – Pilot program to identify vehicles parked at metered spaces after paid parking session expires.
Future use – Determine occupancy and turnover rates at public parking spaces throughout the city.

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

Further, 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.

BUSINESS JUSTIFICATION

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

The SFMTA uses ALPR technology to efficiently identify vehicles parked on city streets in violation of time-limited parking restrictions, and promote timely turnover of parking spaces. This use supports the SFMTA's mission because it helps ensure the sustainability of and more equitable access to the City's limited parking resources, which are part of its larger transportation system.

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

☐	Education	
☑	Community Development	Informs planning, policy development, and pricing for public parking spaces (e.g., for specific commercial districts).
☐	Health	
☑	Environment	Improves street conditions by ensuring timely turnover of parking spaces for use by city residents and visitors.
☑	Criminal Justice	Identifies vehicles reported to SFPD as stolen so they may be returned to their owners.
☐	Jobs	
☐	Housing	
☑	Other	Helps ensure timely turnover of parking spaces, giving city residents and visitors more equitable access to limited parking resources.

Parking Enforcement ALPR Technology will benefit the department in the following ways:

Benefit		Description	Quantity
☑	Financial Savings	Minimizes physical chalking by PCOs; chalking can cause repetitive motion injuries, which result in workers compensation claims filed against the city.	
☑	Time Savings	Helps parking control officers cover larger geographic areas and improves effectiveness and efficiency in performing their duties.	
☑	Staff Safety	Minimizes repetitive motion injuries from physical chalking by automating the process for PCOs to mark vehicles.	
☑	Data Quality	Improves and simplifies information provided to PCOs, which makes parking enforcement more accurate and efficient. Provides higher volumes of data about parking utilization and turnover rates than	

currently available, which informs planning, policy development, and pricing for public parking spaces.

☐ Other

Other benefits include N/A

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. Data types can take the form video, audio, still images. Data formats can take the form of XML, PDF, HTML, Plain Text, JPEG, etc. The surveillance technology collects the following data types and formats: • Video in MOV format • Still images from cameras in PDF format The surveillance technology collects the following data types: *Data Type(s)* | *Format(s)* | *Classification* Digital images of vehicle license plates | JPEG on device; | Level 3

	<table><tr><td>and their license plate numbers</td><td>proprietary format in server (g64m).</td></tr><tr><td>Date and time stamps</td><td>Date & time stamps SQL on device; proprietary format in server (g64m). Level 3</td></tr><tr><td>Geo-location</td><td>SQL on device; proprietary format in server (g64m). Level 3</td></tr></table>
Notification:	Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas. Department notifications shall identify the type of technology being used and the purpose for such collection. Department includes the following items in its public notice: ☐ 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 (please refer to the data sharing section to ensure all information covered in that section is also included below): Employee logs into the tablet computer to access data captured during shift. Only authorized users may use ALPR or access ALPR data. Authorized user must complete mandatory training and obtain login credentials. *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. • 8214 – Parking Control Officer(s); 1824 – Principal Administrative Analyst; 1823 – Sr. Administrative Analyst; 5277 – Planner I; 5288 – Transportation Planner II; 5289 – Transportation Planner III; 5290 – Transportation Planner IV, Sustainable Streets Division

	The following providers are required to support and maintains the surveillance technology and its associated data to ensure it remains functional: • Conduent Technology – Citation-processing contractor • Genetec – ALPR vendor (subcontractor to Conduent Technology) *B. Members of the public* Municipal Transportation Agency 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. Anyone, including criminal defendants, may access such data. 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, including by criminal defendants. Members of the public, including criminal defendants, 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.
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: • Users require unique login credentials to access the ALPR system; system is accessible on portable tablets (used in vehicles) and on desktop workstations; • Users approved to access ALPR devices and ALPR data under these guidelines are permitted access only for uses authorized under the Surveillance Technology Policy; and • All activity in the ALPR system is logged and can be audited.
Data Sharing:	Municipal Transportation Agency 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. Municipal Transportation Agency 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. Municipal Transportation Agency 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) Municipal Transportation Agency 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 Data Sharing Department shares the following data with the recipients: The department does not share surveillance technology data with other departments or entities inside the City and County of San Francisco. Data sharing occurs at the following frequency: 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, scrub faces, 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.

<table>
<tr><td></td><td>☑ 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:

SFMTA Administrative Hearings - Uses ALPR data to validate contested parking citations in public-parking spaces throughout the City.

Data sharing occurs at the following frequency:
If requested. SFMTA Administrative Hearings infrequently requests data.</td></tr>
<tr><td>Data Retention:</td><td>Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.

Please list data retention schedules (i.e., x type of data will be retained for 1 year) based on the following categories:
• Permanent records (i.e., records that are essential): shall be retained and preserved indefinitely
• Current records (i.e., records for operational necessity, ready reference, convenience): record retention schedules may vary but generally less than 10 years
• Storage records (i.e., records retained offsite): record retentions may vary but generally less than 10 years

The Department's data retention period and justification are as follows:
<table><tr><td>Data stored on ALPR devices are purged on every 24 hours.

ALPR data downloaded to the ALPR vendor's server are retained as follows:
• Digital images not associated with parking citations are retained for seven days;
• Digital images associated with parking citations are retained for 365 days;
• Metadata (i.e., license plate numbers, time and date stamps, and geo-location) are retained for 365 days.
• Anonymized ALPR data will be retained indefinitely for planning purposes.</td><td>Data on ALPR devices are stored for 24 hours to ensure uploading to ALPR vendor's server.
For ALPR downloaded to the ALPR vendor's server:
• Digital images not associated with a parking citation are retained for seven days to allow enforcement of 72-hour parking restrictions – the PCOs requires imaged taken at least 72 hours apart to enforce restrictions;
• Digital images associated with parking citations are retained for 365 days to support validation of contested parking citations at SFMTA Administrative Hearings; and
• Metadata (i.e., license plate numbers, time and date stamps, and geo-location) are retained for 365</td></tr></table></td></tr>
</table>

	<table><tr><td></td><td>days for use by SFMTA Parking and Curb Management to analyze and determine occupancy and turnover rates in public-parking spaces .</td></tr></table> PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s): Only if required by law. Departments must establish appropriate safeguards for PII data stored for longer periods. Data will be stored in the following location: ☑ Local 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: Vender purges ALPR data at the end of applicable retention period. Processes and Applications: The SFMTA will use ALPR data to determine parking utilization and turnover rates at public parking spaces Citywide. The ALPR vendor will de-identify these data by replacing license plate numbers with unique identifiers before data are provided to the SFMTA.
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. The training for users to access the information collected in the field consists of classroom training provided by a Genetec authorized trainer.

	Training covers functionality of the system, use of the software; searching plates in the system, identifying hits and validation procedures and login and logoff procedures. For backend users, training is also conducted by a Genetec authorized trainer and includes access and use of the software to generate reports, validate each systems status in real time, system settings including access rights. Access is restricted by the system administrator by user rights control settings.

COMPLIANCE

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

The Director of Parking Enforcement and Traffic will enforce and assign staff members under their direction to oversee compliance with the Surveillance Technology Policy. Principal Administrative Analyst from Finance and Information Technology Division will oversee pilots of ALPR technology.

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

Commander of Parking Enforcement and Traffic; IT Operations Support Admin; Principal Administrative Analyst from Finance and Information Technology Division.

Sanctions for violations of this Policy include the following:

Violations of the Surveillance Technology Policy will result in disciplinary action commensurate with the violation. Sanctions include written warning, suspension, and termination of employment.

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.

EXCEPTIONS

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained or processed by the surveillance technology be shared with law enforcement.

DEFINITIONS

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

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

Complaints or concerns can be submitted to the Department by

Members of the public can register complaints/concerns or submit questions via 311.org or by directly contacting the SFMTA Parking Enforcement and Traffic Division.

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

Questions and complaints received through 311.org are tracked through that system's tracking database; questions and complaints submitted directly to the SFMTA are tracked using Salesforce's case management software.

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the employee's supervisor or to the director. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.

APPENDIX A: Surveillance Technology Policy Requirements

The following section shows all Surveillance Technology Policy requirements in order as defined by the San Francisco Administrative Code, Section 19B.

1. A description of the product and services addressed by the Surveillance Technology, including the identity of any provider(s) whose services are essential to the functioning or effectiveness of the Surveillance Technology equipment or services for the intended purpose.

An ALPR is a camera that captures color images of license plates within its field of view. Mobile cameras are mounted on moving objects, such as parking enforcement vehicles.
Software extracts the license plate numbers from the images and stores the images, plate numbers, and dates, times, and locations of the image captures in a searchable database.
An ALPR system consists of the cameras, the software that reads and converts images of license plates into data, and the searchable database that stores the data.

The system consists of the Genetec Auto Vu Sharp IP-based automatic license plate recognition cameras with onboard processing and the AutoVu Standard Software package. The cameras include Sharp V, AutoVu cameras mounted on the roof of the enforcement vehicle and wheel focused camera on the side of the vehicle. The roof top mounted cameras read the license plates and the side mounted cameras photograph the wheel/tire to compare on the second pass for time-limited enforcement. The system utilizes the Genetec Patroller software 6.5 to create the user interface and in-vehicle mapping. The system utilizes cellular communication to transmit reads to the backend software. The backend software consists of the Genetec Security Center software to manage access to all uploaded plate reads, hotlists, and user-level access credentials.

Genetec

2. A description of the purpose(s) for which the Surveillance Technology equipment or services are proposed for acquisition, including the type of data that may be collected by the Surveillance Technology equipment or services.

Technology Use:

The SFMTA uses ALPR technology to efficiently identify vehicles parked on city streets in violation of time-limited parking restrictions, and promote timely turnover of parking spaces. This use supports the SFMTA's mission because it helps ensure the sustainability of and more equitable access to the City's limited parking resources, which are part of its larger transportation system.

PII:

true

3. The uses that are authorized, the rules and processes required prior to such use, and uses of the Surveillance Technology that will be expressly prohibited.

Authorized Uses:

Identify vehicles parked on city streets in violation of time-limited parking restrictions.

Identify vehicles parked on city streets that have five or more unpaid parking citations.

Identify vehicles parked on city streets that are listed on SFPD's hotlist of stolen vehicles. (Hotlists contain license plate numbers and state of vehicles reported stolen. Hotlist is transmitted via Secure FTP;hotlist is updated/overwritten on a daily basis. The SFMTA does not generate hotlists.)

Future use – Pilot program to identify vehicles parked at metered spaces after paid parking session expires.

Future use – Determine occupancy and turnover rates at public parking spaces throughout the city.

Rules:

Prohibited Uses:

Only authorized users may use ALPR or access ALPR data. Authorized user must complete mandatory training and obtain login credentials.

4. A description of the formats in which information collected by the Surveillance Technology is stored, copied, and/or accessed.

Data Type	Formats STP
Digital images of vehicle license plates and their license plate numbers	JPEG on device; proprietary format in server (g64m).
Date and time stamps	Date & time stamps SQL on device; proprietary format in server (g64m).
Geo-location	SQL on device; proprietary format in server (g64m).

5. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information, including restrictions on how and under what circumstances data collected with Surveillance Technology can be analyzed and reviewed, and the rules and processes required prior to access or use of the information.

Employee Job Classification & Title:

Only authorized users may use ALPR or access ALPR data. Authorized user must complete mandatory training and obtain login credentials.

Department:

Sustainable Streets Division

If applicable, contractor or vendor name:

Conduent Transportation

Rules and processes required prior to data access or use:

- Users require unique login credentials to access the ALPR system; system is accessible on portable tablets (used in vehicles) and on desktop workstations;
- Users approved to access ALPR devices and ALPR data under these guidelines are permitted access only for uses authorized under the Surveillance Technology Policy; and

- All activity in the ALPR system is logged and can be audited.

6. The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms.

Only authorized users may use ALPR or access ALPR data. Authorized user must complete mandatory training and obtain login credentials.

7. The limited time period, if any, that information collected by the Surveillance Technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s) enumerated in the Surveillance Technology Policy, the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period

Retention:

Data on ALPR devices are stored for 24 hours to ensure uploading to ALPR vendor's server.
For ALPR downloaded to the ALPR vendor's server:

- Digital images not associated with a parking citation are retained for seven days to allow enforcement of 72-hour parking restrictions – the PCOs requires imaged taken at least 72 hours apart to enforce restrictions;
- Digital images associated with parking citations are retained for 365 days to support validation of contested parking citations at SFMTA Administrative Hearings; and
- Metadata (i.e., license plate numbers, time and date stamps, and geo-location) are retained for 365 days for use by SFMTA Parking and Curb Management to analyze and determine occupancy and turnover rates in public-parking spaces .

Reason for retention:

Only if required by law.

Deletion process:

Data on ALPR devices are stored for 24 hours to ensure uploading to ALPR vendor's server.
For ALPR downloaded to the ALPR vendor's server:

- Digital images not associated with a parking citation are retained for seven days to allow enforcement of 72-hour parking restrictions – the PCOs requires imaged taken at least 72 hours apart to enforce restrictions;
- Digital images associated with parking citations are retained for 365 days to support validation of contested parking citations at SFMTA Administrative Hearings; and
- Metadata (i.e., license plate numbers, time and date stamps, and geo-location) are retained for 365 days for use by SFMTA Parking and Curb Management to analyze and determine occupancy and turnover rates in public-parking spaces .

Retention exemption conditions:

The SFMTA will use ALPR data to determine parking utilization and turnover rates at public parking spaces Citywide. The ALPR vendor will de-identify these data by replacing license plate numbers with unique identifiers before data are provided to the SFMTA.

8. How collected information can be accessed or used by members of the public, including criminal defendants

Will the data be accessible to the public:

Data stored on ALPR devices are purged on every 24 hours.

ALPR data downloaded to the ALPR vendor's server are retained as follows:

- Digital images not associated with parking citations are retained for seven days;
- Digital images associated with parking citations are retained for 365 days;
- Metadata (i.e., license plate numbers, time and date stamps, and geo-location) are retained for 365 days.
- Anonymized ALPR data will be retained indefinitely for planning purposes.

How it can be accessed:

9. Which governmental agencies, departments, bureaus, divisions, or units that may receive data collected by the Surveillance Technology operated by the Department, including any required justification or legal standard necessary to share that data and how it will ensure that any entity receiving such data complies with the Surveillance Technology Policy.

Name of agency: SFMTA Administrative Hearings - Uses ALPR data to validate contested parking citations in public-parking spaces throughout the City.

Justification:

10. The training required for any individual authorized to use the Surveillance Technology or to access information collected by the Surveillance Technology

Training required:

true

Description of training:

The training for users to access the information collected in the field consists of classroom training provided by a Genetec authorized trainer. Training covers functionality of the system, use of the software; searching plates in the system, identifying hits and validation procedures and login and logoff procedures.
For backend users, training is also conducted by a Genetec authorized trainer and includes access and use of the software to generate reports, validate each systems status in real time, system settings including access rights. Access is restricted by the system administrator by user rights control settings.

11. The mechanisms to ensure that the Surveillance Technology Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy

Training required:

true

Process for responding to complaints:

Commander of Parking Enforcement and Traffic; IT Operations Support Admin; Principal Administrative Analyst from Finance and Information Technology Division.

Oversight process:

Violations of the Surveillance Technology Policy will result in disciplinary action commensurate with the violation. Sanctions include written warning, suspension, and termination of employment.

Compliance personnel titles:

8214 – Parking Control Officer(s); 1824 – Principal Administrative Analyst; 1823 – Sr. Administrative Analyst; 5277 – Planner I; 5288 – Transportation Planner II; 5289 – Transportation Planner III; 5290 – Transportation Planner IV, Sustainable Streets Division

Restrictions:
Only authorized users may use ALPR or access ALPR data. Authorized user must complete mandatory training and obtain login credentials.

12. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

Complaint procedures:

Questions and complaints received through 311.org are tracked through that system's tracking database; questions and complaints submitted directly to the SFMTA are tracked using Salesforce's case management software.

Departmental follow-up process:

The Director of Parking Enforcement and Traffic will enforce and assign staff members under their direction to oversee compliance with the Surveillance Technology Policy. Principal Administrative Analyst from Finance and Information Technology Division will oversee pilots of ALPR technology.

Members of the public can register complaints/concerns or submit questions via calls or emails at 311.org.