Surveillance Technology Policy

Electronic Toll Readers - FasTrak
San Francisco International Airport

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 FasTrak Electronic Toll Readers (hereinafter referred to as "surveillance 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 provide an exceptional airport in service to our communities.

The Surveillance Technology Policy ("Policy") defines the manner in which the surveillance 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 the surveillance technology employees, contractors, and volunteers. Employees, consultants, volunteers, and vendors while working on behalf of the City with the Department are required to comply with this Policy.

POLICY STATEMENT

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

Authorized Use(s):

– Process parking transactions.
– Investigation of parking transaction disputes.

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

Department may use information collected from technology only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data.

BUSINESS JUSTIFICATION

Reason for Technology Use

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

SFO is committed to efficiently delivering world-class customer service while maximizing revenue opportunities. Use of FasTrak Toll Readers provides:

- The ability to accept an alternate payment method that efficiently processes parking fees.
- Parking efficiency minimizes traffic on SFO's roadways. More efficient payment systems for customers reduce traffic congestion and bottlenecks, decreasing the likelihood of collisions and improving customer safety.
- A uniform methodology for SFO parking fee collection and more effectively quantifies parking demand, which supports future SFO planning.

NOTE: It is the parking customer's decision to sign-up for and use the FasTrak technology as a payment option. Use of FasTrak to pay for parking at the Airport is not required.

Description of Technology

- FasTrak transponders are activated by toll readers in designated FasTrak lanes. Individual account information is stored in the transponders. The toll readers identify the individual transponders and validate active accounts.
- During operational hours, the toll reader collects the transponder tag number, as well as the time, date, and location of tag. Customers can avoid having their transponder tag number collected by placing the transponder tag in the mylar bag in which the tag was first obtained by the customer.
- Upon exiting the parking facility, the parking fee amount is calculated and billed to the Bay Area Toll Authority (BATA) who in turn charges the FasTrak customer. Transponders are only read in designated FasTrak Entry and Exit lanes.
- The transponder information is transferred from the toll reader to the toll reader provider's central database.
- If the account is in good standing, the parking fee amount is billed to the Bay Area Toll Authority who in turn deducts from the customer's prepaid account.
- If the Entry and Exit lanes have gates, the gates open.
- The electronic system records each parking transaction, including the time, data, location, and parking charge of each vehicle.

Resident Benefits

The surveillance technology promises to benefit residents in the following ways:

	Benefit	Description
☐	Education	
☐	Community Development	

☐	Health
☐	Environment
☐	Criminal Justice
☐	Jobs
☐	Housing
X	Other

- Public Safety – More efficient payment systems for customers reduce traffic congestion and bottlenecks, decreasing the likelihood of collisions and improving customer safety.

- Other – Convenience; limits parking congestion through more efficient payment processes.

Department Benefits

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

	Benefit	Description
X	Financial Savings	Low maintenance and operating costs, in addition to minimal training of personnel on the use of the technology.
X	Time Savings	Parking fee collections are much more efficient.
X	Staff Safety	Staff no longer need to sit in parking booths that are near fast-moving vehicles.
X	Data Quality	Provides a uniform methodology for SFO parking fee collection and more effectively quantifies parking demand, which supports future SFO planning.
☐	Other	

POLICY REQUIREMENTS

This Policy defines the responsible data management processes and legally enforceable safeguards required by the Department to ensure transparency, oversight, and accountability measures. Department use of surveillance technology and information collected, retained, processed or shared

by surveillance technology must be consistent with this Policy; must comply with all City, State, and Federal laws and regulations; and must protect all state and federal Constitutional guarantees.

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

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

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

Data Type(s)	*Format(s)*	*Classification*
Video Images	MOV	Level 3
Still Images	Downloaded as PDFs	Level 3
Transaction Details (time and date stamp, location, toll charge)	Plain Text	Level 2
Toll Tag Number	Plain Text	Level 3

Notification: Airport shall notify the public of surveillance technology operation by posting the technology policy on the external agency website, FLYSFO.com. 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:

X Information on the surveillance technology
X Description of the authorized use
X Type of data collected
X Data retention
X Department identification
X Contact information

There is also signage in the Airport's parking facilities designated exit lanes where FasTrak is accepted as a payment option.

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

Authorized personnel must submit a request to the data steward to access the limited dataset identified. Requesting personnel must specify the reason for their request. The data steward will review the reason to ensure it aligns with the authorized use and the requesting personnel's work function. The requesting personnel must have completed the required privacy and security training prior to access.

Access to personal information collected by the FasTrak toll readers is limited only to certain operations and technical employees for limited, approved purposes based on their specific work responsibilities.

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:

- 1657 Accountant IV
- 0922 Manager I
- 0923 Manager II
- 0932 Manager IV

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

- FasTrak
- New South Parking
- Scheidt & Bachmann

B. Members of the public

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

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

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

Training: To reduce the possibility that 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.

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 dictated by this policy. 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.

More specifically, Department training will include:

Privacy and security training are required for employees with access to PII, upon hire or assignment to projects involving electronic toll readers. In addition, regular periodic refresher training is required for those employees.

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

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

Data can only be accessed through the Parking Access and Revenue Control System (PARCS) application. Users must provide unique computer login credentials such as username and password to access the data. Passwords must comply with the City and County of San Francisco cyber security requirements.

Administrative:
• Access to Personally Identifiable Information ("PII") and Payment Card Industry ("PCI") Information is limited only to certain operations and technical employees for limited, approved purposes based on their specific work responsibilities.
• Privacy and security training is required for employees with access to PII, upon hire or assignment to projects involving toll readers. In addition, regular periodic refresher training is required for those employees.

Technical:
• Servers and network perimeters are protected with firewalls and are continuously monitored.

• Databases are implemented to ensure PII is segregated from aggregate information. Data is aggregated into a non-identifiable format before sharing.
• Internal and external audits of perimeter and software code security are conducted.

Physical:
• All network equipment and servers containing sensitive data are maintained in a secured location accessible only to Airport badged, authorized personnel.

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

☐ Software as a Service Product

X Cloud Storage Provider

Data Sharing: 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.

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

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

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

A. Internal Data Sharing:

The department shares surveillance technology data with other departments or entities inside the City and County of San Francisco, as follows:

- City Attorney's Office
- Law Enforcement: SFPD – AB

B. External Data Sharing:

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

Data Type	Data Recipient
- Transaction details (time and date stamp, location, toll charge) - Toll Tag Number	- FasTrak CSC contractor (Third-party service provider) - San Mateo County Sheriff

Frequency - Data sharing occurs at the following frequency:

The third-party service provider is provided with relevant data in order to verify FasTrak transactions in processing customer disputes. The department requires the third-party to maintain the confidentiality of the information and to use it only as necessary to perform their duties in connection to the toll readers.

PII will not be disclosed to any other third party, except as required to comply with laws or legal processes served on the department.

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

The Airport has strict contractor agreements with all third-party providers that clearly state the conditions for data disclosure to the third-party, including acceptable and prohibited uses by the third-party, required protections and safeguards, and reporting procedures requiring third-party providers to disclose their compliance with established contractor agreements.

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
FasTrak data retention = 4.5 years	Required by the Bay Area Toll Authority

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.

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

PII required to comply with laws or legal processes served on the Airport will be retained longer than the stated period.

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

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

- Practices: Through its contractor, the department shall discard all PII no more than four years and 6 months after the date the PII is collected.
- Processes and Applications: PII is converted to a non-identifiable format and aggregated. Aggregated data does not contain information that could be used to contact or identify individual customers.

COMPLIANCE

Department Compliance

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

Staff from parking operator New South Parking and parking equipment provider Scheidt & Bachmann will be assigned to maintain updates and perform required maintenance. Compliance with the Surveillance Technology Policy will be self-assessed and reported on regularly by SFO Parking Management via the department's Annual Surveillance Report. The department will also positively respond and amend appropriate recommendations detailed in the annual Audit prepared by the Controller's Office of the City Service Auditor.

Interdepartmental, Intergovernmental & Non-Governmental Entity Compliance

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

In addition, the Airport's Information Technology and Telecommunications (ITT) and Government Affairs & Policy teams will both govern and oversee compliance with the policy. Any resulting policy is to be shared with the Airport community with follow-up items documented, if any.

Oversight Personnel

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

- 1823 Senior Administrative Analyst
- 0922 Parking Operations Manager
- 0932 Airport Parking Manager

Sanctions for Violations

Sanctions for violations of this Policy include the following:

- First offence: Violator shall be verbally notified by Airport management of nature of violation.
- Second offence: Violator shall be notified in writing of second offence and privileges to access toll readers and associated data shall be suspended for 60 days.
- Third offence (following reinstatement of operator privileges): Violator shall be permanently banned from Toll Reader operations and disciplinary action may be taken depending upon the severity of second/third offences.

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 Inquiries

Members of the public may submit complaints or concerns via phone, mail or online submission through the Contact SFO portal (https://www.flysfo.com/contact-sfo). Submissions are reviewed by Airport Guest Services team regularly and forwarded to the Airport stakeholder responsible for handling, as necessary. Additionally, Airport Commission holds bi-monthly public meetings where the public may register complaints or concerns during the Public Comment section of the calendared agenda.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response, and in the following manner:

The Airport will review and respond to constituent calls and complaints within 3 business days. Airport management shall review complaints received on a quarterly basis to discuss best practices, evaluate for lessons learned and opportunities to improve and refine the toll reader program based on caller complaints, concerns, and other community feedback.

Inquiries from 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.