Surveillance Technology Policy

Taxi Dashboard Camera
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 video data from the Taxi Dashboard Camera 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 San Francisco Municipal Transportation Agency's ("SFMTA", "Municipal Transportation Agency", or "Department") 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 video data from the Taxi Dashboard Camera will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all department personnel that use, plan to use, or plan to secure video data from the Taxi Dashboard Camera, 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 the video data from the Taxi Dashboard Camera technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

– Review recording of on-board incidents based upon complaints received from the public and at appeals hearing in response to a fine, suspension or response to fine revocation.
– Review video data in response to complaints from the public to ensure compliance by taxi cab companies and other taxi permittees with requirements and conditions under Article 1100 (Regulation of Motor Vehicles for Hire) of Division II of the SF Transportation Code.
– Review video data to confirm taxi cab companies and other taxi permittees complete rides paid for with public funds before paying the companies for those rides. For example, under its wheelchair program taxi incentive, the Department reviews video data from the technology to confirm that taxi cab drivers pick up individuals with certain disabilities before paying drivers for those rides, which are funded under various paratransit programs.
– Review video to investigate criminal acts involving taxi drivers or riders.

– Review video data to investigate accidents involving a taxi cab.

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. Additionally, department may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

BUSINESS JUSTIFICATION

Video data from the Taxi Dashboard Camera supports the Department's mission and provides important operational value in the following ways:

Taxis are one of several modes of transportation the Department regulates within the City. Taxi cab companies and other taxi permittees that operate in the City are subject to a number of requirements and conditions under Article 1100 (Regulation of Motor Vehicles for Hire) of Division II of the SF Transp. Code to ensure safety, equity of service, and sustainability among other goals. The City uses video data or information it acquires from the taxi cab companies and other taxi permittees' use of the technology to enforce their compliance with these requirements and conditions.

In addition, video data from the Taxi Dashboard Camera promises to benefit residents in the following ways:

- Accessibility: Ensures consumer protection and public safety by allowing the Department to review incidents on board taxi cabs, including the behaviors and actions of drivers and riders after receiving incident reports from riders. Allows video audits of accessible trips subsidized by public funds
- Criminal Justice: Ensures consumer protection and public safety by allowing the Department to review incidents on board taxi cabs, including the behaviors and actions of drivers and riders after receiving incident reports from riders or drivers, while also serving as a deterrent by recording incidents in the taxi cab.
- Health: Ensures consumer protection and public health by allowing the Department to review incidents on board taxi cabs, including the behaviors and actions of drivers and riders after receiving incident reports from riders.
- Public Safety: Ensures public safety by allowing the Department to review incidents on board taxi cabs, including the behaviors and actions of drivers and riders after receiving incident reports from riders, as well as serving as a deterrent to drivers who may otherwise operate a vehicle in an unsafe manner.

Video data from the Taxi Dashboard Camera will benefit the department in the following ways:

- Allows investigations to proceed: The Department is responsible for managing surface transportation in the City. The Department uses video data and information from the technology to ensure taxicab companies and other taxi permittees and drivers comply with applicable requirements and conditions under Article 1100 (Regulation of Motor Vehicles to Hire) of Division II of the Transp., which helps ensure consumer protection and, public health and safety.
- Improved Data Quality: the alternative is conducting witness interviews after receiving a report or complaint. Having a recording of an incident helps to inform whether corrective action is warranted.
- Time Savings: The alternative is relying solely on witness interviews, which can be time consuming and may not be reliable in some cases.

To achieve its intended purpose, the video data acquired from the Taxi Dashboard Camera (hereinafter referred to as "surveillance technology") consists of one camera device with two lenses. The camera device is typically mounted behind the rearview mirror or in the upper portion of the windshield of the passenger side of the taxi cab and captures images in the cabin and on the road in front of the taxi cab. Video is saved to secure digital (SD) cards.

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.

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: Department 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:

- Video and audio recordings from taxi cab cabins, including conversations between riders with cab drivers. Front facing video cameras record traffic conditions on the road and routes taken. All information is Level 3 sensitivity per the City's Data Classification Standard.

Notification: Department does not own dashboard cameras in taxi cabs and therefore does not provide public notice. The Transportation Code requires that taxis have a notice notifying passengers of the presence of a security camera in the vehicle.

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):

- Video is viewable on proprietary software (mainly Janus) and is password protected.

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:

9174 Enforcement and Legal Affairs Manager

9177 Investigations Supervisor

8167 Administrative Hearing Examiner

9183 Taxi Director

9144 Taxi Investigators (8 personnel)

B. Members of the public, including criminal defendants

The Municipal Transportation Agency 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. 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, Department shall, at minimum, apply the following safeguards:

Video data are not accessible to unauthorized parties. (All access is password protected.)

Data Sharing: The Municipal Transportation Agency will endeavor to ensure that other agencies or departments that receive data collected from a Taxi Cab Dashboard Camera 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 Municipal Transportation Agency 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 Municipal Transportation Agency Department shall ensure all PII and restricted data is adequately protected to ensure the identities of individual subjects are effectively safeguarded.

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 response.

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.

- 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.

The Municipal Transportation Agency 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.

The Department currently participates in the following sharing practices:

A. Internal Data Sharing

Department shares the following data with the recipients:

Type	**Recipient**
Video (recording on secure digital (SD) card or possible copy from the cloud.)	SFMTA, San Francisco Police Department (SFPD), District Attorney and Public Defender

Data sharing occurs at the following frequency:

The Department shares data from the technology upon request and in accordance with the authorized use cases. The frequency of sharing varies with the timing and number of incidents that trigger requests..

B. External Data Sharing

Department shares the following data with the recipients:

Type	**Recipient**
Department shares video it receives from taxi cab companies and other taxi permittees with outside entities using secure digital SD cards.	California Highway Patrol (CHP) and other law enforcement agencies but only with a warrant

Data sharing occurs at the following frequency:

Varies. Depends on request.

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy the Department will endeavor to ensure that other agencies or departments with which it shares data from the technology receive a copy of and comply with the policy. The Department will

ensure administrative, technical, and physical safeguards are in place before sharing data internally with other City departments. 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.
- Evaluate what data can be permissibly shared with members of the public should a request be made in accordance with San Francisco's Sunshine Ordinance.
- Review all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.

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:

Retention Period	**Retention Justification**
For data used at taxi disciplinary hearings, data is retained indefinitely. For data used for other purposes, including compliance related audits, SD cards are returned to the taxi cab companies and other taxi permittees after audit is performed.	Pursuant to the Department retention policy, video relating to an appeal are stored as part of the hearing file. Video for any other purpose is not retained and is returned to the taxi cab company at the completion of the investigation or audit.

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.

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

Data will be stored in the following location:

- Local Storage

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

Practices:

- For data used at taxi disciplinary hearings, data is retained indefinitely. For data used for other purposes, including compliance related audits,

SD cards are returned to the taxi cab companies and other taxi permittees after audit is performed.

Processes and Applications:

- The Department does not have or require any process or application to scrub images of individual taxi cab drivers or riders (which are the personal identifiable information typically recorded by the technology) because the Department requires these images to perform authorized use cases.

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. This part of the policy does not apply as the Department does not have a training policy.

COMPLIANCE

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

The Department will assign personnel to oversee and enforce compliance with the policy .

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

- 9174 Enforcement and Legal Affairs Manager.

Sanctions for violations of this Policy include the following:

- Violations of the Policy may result in disciplinary action or sanctions commensurate with the severity of the violation. Sanctions may include written warning, suspension, or 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:

Members of the public may register complaints or concerns about the deployment of the technology through 311.org.

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

The Department will respond to complaints submitted through 311 within the time line specified in the Department's 311 response policy.

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.