# Surveillance Technology Policy

Gunshot Detection Hardware and Services
Emergency Management

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 gunshot detection hardware and services 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 the following:

The San Francisco Department of Emergency Management (DEM) leads the City in planning, preparedness, communication, response, and recovery for daily emergencies, large scale citywide events, and major disasters. DEM is the vital link in emergency communication between the public and first responders, and provides key coordination and leadership to City departments, stakeholders, residents, and visitors.

The Surveillance Technology Policy ("Policy") defines the manner in which the gunshot detection hardware and services 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 gunshot detection hardware and services, 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 gunshot detection hardware and services technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

*Authorized Use(s):*

- *Dispatch is notified of gunshots through the ShotSpotter application, and then creates a call for service for police officers to respond to the location.*

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

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

**BUSINESS JUSTIFICATION**

Gunshot detection hardware and services support the Department's mission and provides important operational value in the following ways:

Gunshot detection hardware and services support the mission of our department to respond to daily emergencies by reporting potential incidents involving gunfire. Gunshot detection hardware and services notifications help make the department aware of gunfire events they would have otherwise not have known about.

In addition, gunshot detection hardware and services promises to benefit residents in the following ways:

| | Benefit | Description |
|---|---|---|
| ☐ | Education | |
| ☐ | Community Development | |
| X | Health | Gun violence and its impacts are a Public Health concern. Preventing gun violence is an essential component to building healthy communities. |
| ☐ | Environment | |
| X | Criminal Justice | Gunshot detection hardware and services alerts enable a fast, precise officer response to unreported gunfire to render Medical aid to victims of a gunshot, secure critical evidence, and apprehend armed individuals which is in the interest of Criminal Justice |
| ☐ | Jobs | |
| ☐ | Housing | |
| X | Public Safety | Gunshot detection hardware and services notifications help make the department aware of gunfire events they would have otherwise not have known about which is in the interest of Public Safety. In 2019, only 15% of SF gunfire incidents were called into 911. |
| ☐ | Other | |

Gunshot detection hardware and services will benefit the department in the following ways:

| | Benefit | Description |
|---|---|---|
| | Financial Savings | |
| X | Time Savings | The technology saves time by notifying dispatch of gunshot activations faster than processing a 911 call. This technology is much faster and |

| | | |
|---|---|---|
| | | more accurate with determining the location than witnesses who call 911. |
| | Staff Safety | |
| X | Data Quality | The technology improves data quality by providing a calculated location for the gunshots, how many gunshots were detected, whether there were multiple guns involved, and the possibility of a high caliber weapon. Most witnesses are unable to provide this level of detail when calling 911. |
| | Other | |

To achieve its intended purpose, ShotSpotter, Inc. (hereinafter referred to as "surveillance technology") is a California-based company that operates ShotSpotter Flex, a proprietary technology that uses sensors strategically placed around a geographic area to detect, locate, and analyze gunshots, and notify law enforcement. ShotSpotter is the most widely used gunshot detection technology in the United States, currently operating in nearly 100 jurisdictions across the country. ShotSpotter uses acoustic sensors that are strategically placed in an array of approximately 20 sensors per square mile. These sensors are connected wirelessly to ShotSpotter's centralized, cloud-based application to reliably detect and accurately triangulate (locate) gunshots. Each acoustic sensor captures the precise time and audio associated with impulsive sounds that may represent gunfire. This data, from multiple sensors, is used to locate the incident, which is then filtered by sophisticated machine algorithms to classify the event as a potential gunshot. Expertly trained acoustic analysts, who are located and staffed in ShotSpotter's 24x7 Incident Review Center, then further qualify those highlighted incidents. These analysts ensure and confirm that the events are in fact gunfire. In addition, the analysts can append the alert with other critical intelligence such as whether a full automatic weapon was fired and whether the shooter is on the move. There are three components to the ShotSpotter system:

1. Gunshot Location Detection (GLD) Sensors: Sensors are installed in different coverage areas in San Francisco.

2. ShotSpotter Headquarters (HQ): Sensors send acoustic information to HQ where computer-based machine-learning algorithms are used to analyze the sound. If the sound and visual audio signature match gunfire, the incident file is then passed along to the Incident Review Center (IRC). Acoustic experts at the IRC review incidents within seconds and provide additional information (e.g. number of gunshots, number of guns, types of guns). Confirmed gunshots are pushed out to Communications (DEM Dispatch) as well as to the San Francisco Police Department ShotSpotter software system within seconds.

3. ShotSpotter Response Software: This software allows certain authorized personnel (SFPD) to use a desktop application that connects to the ShotSpotter system for more in-depth gunshot analysis.

**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 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.

The surveillance technology collects the following data types:

| *Data Type(s)* | *Format(s)* | *Classification* |
|---|---|---|
| Audio - Very short audio snippets of the gunshot(s) are gathered by ShotSpotter. From 1 second before until 1 second after the gunshot(s) | .wav | Level 3 |
| Location – The location of the gunshot is triangulated using data gathered by ShotSpotter. | XYZ Coordinates | Level 3 |

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):

- Only authorized and trained personnel may access the ShotSpotter application via department computers.

Data must always be scrubbed of PII as stated above prior to public use.

*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:

- Public Safety Supervisors and Coordinators (8239-8240) - Supervisors view the data once an activation is triggered, and then enter the data into CAD as an incident.
- Public Safety Dispatchers (8238) - Dispatchers can see the ShotSpotter data once it is entered into CAD and then broadcast the incident to responding officers.

*B. Members of the public, including criminal defendants*

The Department of Emergency Management 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:

Access to the data for DEM personnel is limited to four Supervisor workstations on the dispatch floor, which is also kept secure and access is restricted through logged keycards. The software is also always kept up to date, and requires personnel to login to view the data.

Data Sharing: The Department of Emergency Management will endeavor to ensure that other agencies or departments that may receive data collected by the gunshot detection hardware and services Policy will act in conformity with this Policy.

For internal and externally shared data, shared data shall not be accessed, used, or processed by the recipient in a manner incompatible with the authorized use cases stated in this Policy.

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

The Department of Emergency Management shall ensure all PII and restricted data is de-identified or 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:

- X Confirm the purpose of the data sharing aligns with the department's mission.
- X Consider alternative methods other than sharing data that can accomplish the same purpose.
- X 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.
- X 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.

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

The Department of Emergency Management 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** |
|---|---|
| The location of the gunshots, as well as how many gunshots were detected. If multiple shooters or a high capacity weapons is indicated by ShotSpotter then that is disclosed as well. | San Francisco Police Department |

Data sharing occurs at the following frequency:

Data is shared whenever there is a notification that gunshots were detected. This can occur daily. In addition, the SFPD maintains their own direct access to ShotSpotter..

B. External Data Sharing

Department shares the following data with the recipients:

| **Type** | **Recipient** |
|---|---|
| The location of the gunshots, as well as how many gunshots were detected. If multiple shooters or a high capacity weapons is indicated by ShotSpotter then that is disclosed as well. | Other law enforcement agencies operating within San Francisco. |

Data sharing occurs at the following frequency:

As-needed if an activation is within their jurisdiction. .

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

DEM has strict controls for access to gunshot detection hardware and services, as mentioned in other sections, is only accessed by authorized and trained DEM personnel. The data is only transmitted to the San Francisco Police Department or

relevant law enforcement agency. SFPD has separately submitted their own Surveillance Technology Policy covering gunshot detection hardware and services.

Before data sharing with any recipient, 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.
- Ensure shared data will be done in a cost-efficient manner and exported in a clean, machine-readable format.
- Refer data request to the San Francisco Police Department as they are responsible for ShotSpotter.
- 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** |
|---|---|
| Data from ShotSpotter is the responsibility of the San Francisco Police Department as they have contracted for the service. DEM does NOT maintain the ShotSpotter data, and instead merely accesses it on behalf of the Police Department in order to dispatch police officers to reports of gunshots. Individual incident data is accessible at DEM for up to one week. ShotSpotter (vendor) maintains the data themselves (it is not stored within DEM). ShotSpotter audio sensory data is permanently deleted after 30 hours unless it was accompanied by a loud, impulse sound thought to be a gunshot, in which case it may be saved for investigative purposes by SFPD. Permanent Records: N/A. Refer to SFPD. Current Records: Detected gunshots within the previous week are | DEM does not define the retention period and merely has access to the ShotSpotter data for the time period granted by the San Francisco Police Department and ShotSpotter, Inc. (vendor). DEM can only view gunshots that were detected within the previous week. SFPD and ShotSpotter have set the audio retention period at 30 hours so that they can recover incidents during the prior 24 hours. For instance, to check to see if there was additional gunfire prior to an incident or a missed incident. |

| | |
|---|---|
| visible in the application. Storage Records: N/A. Refer to SFPD. | |

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.

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

Data will be stored in the following location:

☐ Local storage (e.g., local server, storage area network (SAN), network attached storage (NAS), backup tapes, etc.)

☐ Department of Technology Data Center

X Software as a Service Product

☐ Cloud Storage Provider

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

Practices:

- The Department does not store the data on-site, and only accesses the data through a ShotSpotter client application. The data is no longer accessible by the department once the seven-day period passes for each individual incident. Disposal of data is not handled by the department. See SFPD policy for further on data disposal.

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.

All new dispatchers are trained on how the technology works so they can use the data as needed in their interactions with SFPD. Supervisors are also trained on how to access the application installed on the supervisor computers to look at gunshot

detection activation data and then enter that incident into the computer aided dispatch system.

**COMPLIANCE**

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

The use of gunshot detection hardware and services has the same compliance requirement as all other department directives. Data is only accessed under a need to know and right to know basis. Access to the application is limited to Supervisors.

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

- (0923) Operations Manager, Division of Emergency Communications
- (0931) Assistant Deputy Director, Division of Emergency Communications

Sanctions for violations of this Policy include the following:

Violations of the Surveillance Technology Policy follow the same discipline procedures as violations of other directives:

- First Offense: Retraining
- Second Offense: Formal Counseling
- Third Offense: Letter of Reprimand

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 <u>not</u> 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 would be directed to SFPD as they are the owners of the technology.

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

Members of the public would be directed to SFPD as they are the owners of the technology, and it would be up to SFPD to respond to all questions and complaints.

*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.