Surveillance Technology Policy

ShotSpotter, Inc. ("ShotSpotter")
Police

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 ShotSpotter, Inc. ("ShotSpotter") 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: In order protect life and property, prevent crime and reduce the fear of crime, we will provide service with understanding, response with compassion, performance with integrity and law enforcement with vision.

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

Authorized Use(s):

Gunshot detection: Record gunshot sounds and use sensors to locate the origin of the gunshots.
1. Patrol Officers receive gunshot alerts to respond to crime scene.
2. Investigators use ShotSpotter Investigative Portal reports to find shell casing evidence on scene and to further analyze the incident.

- On an annual basis, the Department will evaluate the impact of the technology on the following measures:

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

A ShotSpotter alert will not, on its own, identify an individual, reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, information concerning an individual person's sex life or sexual orientation. Recordings of ambient noise, or any other sound outside of verified gunshots shall be prohibited for use in any investigation and shall not cause police enforcement.

BUSINESS JUSTIFICATION

ShotSpotter, Inc. ("ShotSpotter") supports the Department's mission and provides important operational value in the following ways:

The ShotSpotter system enables SFPD to be aware of gunshots in the absence of witnesses and/or reports to 911 of gunshots. The ShotSpotter system notifies SFPD of verified gunshot events, which expedites police and ambulance response rates to incidents involving illegal gunfire. ShotSpotter Alerts help SFPD locate victims, witnesses, evidence and suspects.
It shall be the policy of the SFPD to properly utilize ShotSpotter to enhance the Department's ability to respond to and investigate violent crimes involving illegal gunfire.

In addition, ShotSpotter, Inc. ("ShotSpotter") promises to benefit residents in the following ways:

☐	Education	
☐	Community Development	
☑	Health	Gun violence and its impacts are a public health concern. Preventing gun violence is an essential component to building health communities.
☐	Environment	
☑	Criminal Justice	ShotSpotter notifications help make the department aware of gunfire events they would have otherwise not have known about. In 2019, only 15% of SF gunfire incidents were called into 911. ShotSpotter alerts enable a fast, precise officer response to unreported gunfire to render aid to victims of a gunshot, secure critical evidence, and apprehend armed individuals.
☐	Jobs	
☐	Housing	
☐	Other	

ShotSpotter, Inc. ("ShotSpotter") will benefit the department in the following ways:

Benefit		Description	Quantity
☐	Financial Savings		
☑	Time Savings	If a 911 caller reports a gunshot incident, it usually takes several minutes to capture and relay the information to officers often with imprecise data on the exact location. With ShotSpotter, officers receive alerts within 60 seconds of trigger pull with closest address data enabling a faster response to a crime scene to potentially save victims.	
☒	Staff Safety	Officers can approach a crime scene more safely with ShotSpotter alerts knowing the precise location and time of the event and whether there are multiple shooters or high capacity weapons being used.	
☒	Data Quality	Only 15% of gunshot incidents in SF have an accompanying 911 call (2019). Without ShotSpotter there would be no police response to 85% of gun crime representing over 850 incidents. However, with ShotSpotter, virtually all incidents are captured with an exact location enabling the department to better protect and serve the community.	
☐	Other		

Other benefits include

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: *Data Type(s)* / *Format(s)* / *Classification* acoustic / .wav format / Level 3
Notification:	Publicly posted signage near the location of the technology is not feasible as the technology is not physically guarded and because of the intent of the technology to detect illegal gunfire the unguarded and unprotected technology is susceptible to vandalism and attempts to disable the intent of the technology.

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): Authorized personnel may access the browser-based ShotSpotter system via vehicle computers to only access the cloud-based system. SFPD members also have the option to activate ShotSpotter app on their Department issued mobile phones. Authorized personnel must always gain access through a login/password-protected system which records all login access. SFPD has no direct access to actual ShotSpotter sensors. Only ShotSpotter-specified support engineers can use a technology to access the data in the sensors prior to the 30-hour deletion period, if investigators need to search for previous gunshots. SFPD may request data within the first 24 hours, prior to the 30-hour deletion period. 1. Authorized personnel may access the ShotSpotter system via vehicle computers and receive notifications of verified ShotSpotter activations. SFPD may also notify authorized personnel of ShotSpotter activations. Authorized personnel may respond to such notifications based upon priorities as mandated by their supervisors. 2. The ShotSpotter system shall only be used for official law enforcement purposes. 3. Only specifically authorized personnel authorized by the Chief or Chief designee (e.g. personnel with SFPD's Investigations Division) will have access to historical ShotSpotter system data via desktop ShotSpotter system applications. The ShotSpotter system may be used for authorized patrol and investigation purposes. Contacting individuals at locations where ShotSpotter activations occur shall be conducted in accordance with applicable law and policy. 4. Accessing data collected by the ShotSpotter system requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation or assignment to a unit which responds to gunshot calls (e.g. Patrol Division). 5. Members approved to access ShotSpotter system data may only use data for legitimate law enforcement purposes only, such as when the data relate to gunshots, a specific criminal investigation or department-related civil or administrative action. 6. All verified ShotSpotter system activations are entered into SFPD's computer-aided dispatch (CAD) record management system (RMS) with ShotSpotter system specific ID numbers. Authorized personnel can then query the CAD/RMS system for any and all ShotSpotter system activations. *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. • The Department and ShotSpotter The following providers are required to support and maintains the surveillance technology and its associated data to ensure it remains functional: • ShotSpotter

	B. Members of the public ShotSpotter data is classified as Level 3, Sensitive and public release is restricted, however each request submitted by a member of the public will be reviewed to determine whether the data can be released. SFPD shall comply with the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules.
Data Security:	To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards: The Department must have a subscription to ShotSpotter system and only has access to Reviewed Alerts delivered via the Investigator Portal password-protected internet portal and user interface supplied by ShotSpotter. ShotSpotter has limited or eliminated audio access for several positions (including SST executives) whose access to audio was not essential. To address, deter and detect possible misuse, ShotSpotter requires supervisor approval before a ShotSpotter employee is permitted to download extended audio. For every instance in which a ShotSpotter employee accesses stored sensor audio, ShotSpotter requires its employees to document what audio was accessed, who accessed the audio, and who approved the download, the law enforcement officer making the request, and the evidentiary basis for the request. Supervisory personnel regularly review this audit trail to ensure that audio is being accessed only when necessary and according to proper procedures. These regular reviews assess which law enforcement agencies may be using the process at a much higher rate, ShotSpotter personnel who listen to a significantly longer duration of audio, or other patterns that may require corrective action. ShotSpotter's privacy policy can be accessed here: https://www.shotspotter.com/privacy-policy
Data Sharing:	SFPD will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules. SFPD will endeavor to ensure that other agencies or departments that may receive data collected by [the Surveillance Technology Policy that it operates] will act in conformity with this Surveillance Technology Policy. For internal and externally shared data, shared data shall not be accessed, used, or processed by the recipient in a manner incompatible with the authorized use cases stated in this Policy.

	SFPD shall ensure proper administrative, technical, and physical safeguards are in place before sharing data with other CCSF departments, outside government entities, and third-party providers or vendors. (See Data Security) SFPD shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded. Each department that believes another agency or department receives or may receive data collected from its use of STs should consult with its assigned deputy city attorney regarding their response. The Department currently participates in the following sharing practices: A. Internal Data Sharing Department shares the following data with the recipients: San Francisco District Attorney's Office, San Francisco Public Defender's Office, US Attorney. ShotSpotter data will only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law. Data sharing occurs at the following frequency: Frequency depends on cases/incidents 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 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: CGIC Partners; US Attorney. ShotSpotter data will only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law.

	Data sharing occurs at the following frequency: as-needed To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall: Direct the request to ShotSpotter. ShotSpotter may offer redacted data that complies with the Right to Know Law Request and/or Open Public Records Act/Freedom of Information Act, ShotSpotter and its confidential, proprietary Data and records are protected under the exemptions expressly defined in the Public Records Act, Evidence Code and California Civil Code as follows: ShotSpotter gunfire alert Data and records are a trade secret, and are exempt from disclosure pursuant to Evidence Code section 1060 which refers to subdivision (d) of Section 3426.1 of the California Civil Code for the definition of trade secret, as follows: "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. ShotSpotter keeps the gunfire alert Data and records confidential and secret by not releasing them to the public and by including Data restriction rights and confidentiality clauses in all customer agreements. Further, locations of specific sensors, gunshots at or near specific locations, and actual locations of areas covered is a matter of public safety and will not be released under any conditions. Additionally, the data is protected as some or all can be involved in on-going criminal investigations.
Data Retention:	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

	• Criminal Investigative file retention schedule is subject to evidence laws, CA penal code and statute of limitations. The Department's data retention period and justification are as follows: ShotSpotter: The sensors delete all acoustic data after 30 hours unless the gunshot-like impulsive acoustic event sends the data to ShotSpotter for analysis. Only verified gunshot data is maintained in perpetuity, both by ShotSpotter HQ as well as on SFPD desktop applications. SFPD: Records shall be purged according to the current San Francisco Police Department Records Retention and Destruction Schedule which calls for destruction of intelligence files every two years from the last date of entry with the following exceptions: a. Information may be maintained if it is part of an ongoing investigation or prosecution. b. All written memoranda requesting authorization to commence an investigation and subsequent authorizations shall be maintained for not less than five years after termination of the investigation. c. Records showing violation of these guidelines shall not be destroyed or recollected for the purpose of avoiding disclosure. It shall be the policy of the SFPD that once the requisite retention period for a record has passed, the record shall be destroyed unless there are particular circumstances that dictate that the record be retained. It shall be the policy of the SFPD to work with contractors providing off-site storage of records to ensure that records are destroyed once the requisite time period for retention has passed ShotSpotter does not collect PII data and as such PII data shall not be kept in a form which permits identification of data subjects. ShotSpotter maintains verified gunshot data indefinitely. 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: Audio is only temporarily stored (30 hours), and then a very select amount of audio is retained only if the computer algorithm or human reviewer detects a gunshot. All other audio is routinely purged from ShotSpotter's systems. Processes and Applications: The ShotSpotter real-time Incident Review Center (IRC) will review at least 90% of all gunfire incidents within 60 seconds. This human review is intended to confirm or change the machine classification of the incident type, and, depending on the reviewer's confidence level that the incident is or may be gunfire, will result in an alert ("Reviewed Alert") sent to the Customer's dispatch center, patrol car mobile data terminals (MDT), and officer smartphones (via the ShotSpotter App), based on the following criteria: High confidence incident is gunfire; Uncertain if incident is gunfire or not; Low confidence incident is gunfire
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. The ShotSpotter Gun Shot Detection Program Manager shall oversee the training program for any members with access to the ShotSpotter system and data.

COMPLIANCE

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

Surveillance Technology Policies shall have the same compliance requirements as all Department Written Directives and Police Commission Resolutions.

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

Deputy Chief of Investigations and the Commander of Investigations in addition, each member of the Department belongs to a chain of command. The Officer in Charge (OIC) of that chain of command is responsible for overseeing compliance with all SFPD written directives and the surveillance technology polices. If allegations arise that a member is not in compliance, the OIC will initiate an investigation and will take the appropriate action which could include an investigation of misconduct by Internal Affairs.

Sanctions for violations of this Policy include the following:

San Francisco Police Department will conduct an internal investigation though the Chief of Staff/Internal Affairs (IA) Unit. The results of the investigation will be reported to the Chief of Police, who will determine the penalty for instances of misconduct. Under San Francisco Charter section A8.343, the Chief may impose discipline of up to a 10-day suspension on allegations brought by the Internal Affairs Division or the DPA. Depending on the severity of the allegation of misconduct, the Chief or the DPA may elect to file charges with the Police Commission for any penalty

greater than the 10-day suspension. Any discipline sought must be consistent with principles of just cause and progressive discipline and in accordance with the SFPD Disciplinary Guidelines.

If a Department is alleged to have violated the Ordinance under San Francisco Administrative Code Chapter 19B, Department shall post a notice on the Department's website that generally describes any corrective measure taken to address such allegation.

Department is subject to enforcement procedures, as outlined in San Francisco Administrative Code Section 19B.8.

DEFINITIONS

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

Members of the public can register complaints about SFPD activities with the Department of Police Accountability (DPA). DPA, by Charter authority, receives and manages all citizen complaints relating to SFPD. DPA manages, acknowledges and responds to complaints from members of the public.

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

Update the SFPD public website to include surveillance technology policies and will include a general email for public inquiries. The general email box will be assigned to a staff member in the Chief's Office who will respond to inquiries within 48 hours.

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the Chief of Police at SFPDChief@sfgov.org. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the Chief of Police at SFPDChief@sfgov.org.

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.

ShotSpotter manages the cloud-based service with a subscription service which provides the SFPD with access to the following:

- Gunshot Alerts
- Apps for Dispatch, Patrol Officers, Investigators, and District Station Personnel
- Incident Review Center
- Investigative Lead Summary
- Investigator Portal

ShotSpotter Inc. 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 (dispatch) as well as to the SFPD ShotSpotter software system within seconds.

3. The SFPD ShotSpotter Software System: This system is cloud-based and desktop-based; SFPD authorized personnel can use internet browsers to connect to the ShotSpotter system via SFPD computers. Certain authorized personnel use desktop applications that connect to the ShotSpotter system for more in-depth gunshot analysis.

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 ShotSpotter system enables SFPD to be aware of gunshots in the absence of witnesses and/or reports to 911 of gunshots. The ShotSpotter system notifies SFPD of verified gunshot events, which expedites police and ambulance response rates to incidents involving illegal gunfire which will help locate victims, witnesses, evidence (casings, bullets, blood etc.,) and suspects.

PII:

false

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:

Gunshot detection: Record gunshot sounds and use sensors to locate the origin of the gunshots.

1.) Patrol Officers receive gunshot alerts to respond to crime scene.
2.) Investigators use ShotSpotter reports to find shell casing evidence on scene and to further analyze the incident.

Rules:

Prohibited Uses:

1. Unauthorized members using an authorized members log in to access historical ShotSpotter system data via desktop ShotSpotter system applications.

2. Using the ShotSpotter system for anything other than official law enforcement purposes.

3. Using ambient noise or any other sound outside of verified gunshots for use in any investigation.

4. Authorized members accessing data collected by the ShotSpotter system absent a right to know and a need to know.

A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation or assignment to a unit which responds to gunshot calls (e.g. Patrol Division).

5. Authorized members approved to access ShotSpotter system data using data for illegitimate purposes

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

Data Type	Formats STP
acoustic	.wav format Mp3

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: Individuals designated by the Chief or Chief-designee can include the following: Police Service Aide (PSA), Police Officer, Sergeant, Lieutenant, Captain, crime analyst, Deputy Chief, Commanders, Assistant Chief, Chief of Police, Media Relations Unit members or specifically designated civilian staff.

1. Authorized personnel may access the ShotSpotter system via vehicle computers and receive notifications of verified ShotSpotter activations. SFPD may also notify authorized personnel of ShotSpotter activations. Authorized personnel may respond to such notifications based upon priorities as mandated by their supervisors.

2. The ShotSpotter system shall only be used for official law enforcement purposes.

3. Only specifically authorized personnel authorized by the Chief or Chief designee (e.g. personnel with SFPD's Investigations Division) will have access to historical ShotSpotter system data via desktop ShotSpotter system applications. The ShotSpotter system may be used for authorized patrol and investigation purposes. Contacting individuals at locations where ShotSpotter activations occur shall be conducted in accordance with applicable law and policy.

4. Accessing data collected by the ShotSpotter system requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation or assignment to a unit which responds to gunshot calls (e.g. Patrol Division).

5. Members approved to access ShotSpotter system data may only use data for legitimate law enforcement purposes only, such as when the data relate to gunshots, a specific criminal investigation or department-related civil or administrative action.

6. All verified ShotSpotter system activations are entered into computer-aided dispatch (CAD) record management

system (RMS) with ShotSpotter system specific ID numbers. Authorized personnel can then query the CAD/RMS system for any and all ShotSpotter system activations.

Department:

SFPD and ShotSpotter

If applicable, contractor or vendor name:

ShotSpotter

Rules and processes required prior to data access or use:

The department must have a subscription to ShotSpotter system and only has access to Reviewed Alerts delivered via the Investigator Portal password-protected internet portal and user interface supplied by ShotSpotter.

ShotSpotter has limited or eliminated audio access for several positions (including SST executives) whose access to audio was not essential. To address, deter and detect possible misuse, ShotSpotter requires supervisor approval before a ShotSpotter employee is permitted to download extended audio. For every instance in which a ShotSpotter employee accesses stored sensor audio, ShotSpotter requires its employees to document what audio was accessed, who accessed the audio, and who approved the download, the law enforcement officer making the request, and the evidentiary basis for the request. Supervisory personnel regularly review this audit trail to ensure that audio is being accessed only when necessary and according to proper procedures. These regular reviews assess which law enforcement agencies may be using the process at a much higher rate, ShotSpotter personnel who listen to a significantly longer duration of audio, or other patterns that may require corrective action.
ShotSpotter's privacy policy can be accessed here: https://www.shotspotter.com/privacy-policy

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

Only authorized and trained personnel are permitted access to the system. The system always requires user and password ID for login. Furthermore, only personnel specifically designated by the Chief or Chief-designee have access to the system desktop applications which provide access to any historical downloadable data Authorized personnel may access the ShotSpotter system via vehicle computers and receive notifications of verified ShotSpotter activations. All verified ShotSpotter system activations are entered into SFPD's computer-aided dispatch (CAD) record management system (RMS) with ShotSpotter system specific ID numbers. Authorized personnel can then query the CAD/RMS system for any and all ShotSpotter system activations. The ShotSpotter verified activations entered into CAD/RMS require personnel to have level two CAD access which must adhere to the California Law Enforcement Telecommunications System (CLETS) guidelines.

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:

ShotSpotter: The sensors delete all acoustic data after 30 hours unless the gunshot-like impulsive acoustic event sends the data to ShotSpotter for analysis. Only verified gunshot data is maintained in perpetuity, both by ShotSpotter HQ as well as on SFPD desktop applications.
SFPD: Records shall be purged according to the current San Francisco Police Department Records Retention and Destruction Schedule which calls for destruction of intelligence files every two years from the last date of entry with the following exceptions:
a. Information may be maintained if it is part of an ongoing investigation or prosecution.
b. All written memoranda requesting authorization to commence an investigation and subsequent authorizations shall be maintained for not less than five years after termination of the investigation.
c. Records showing violation of these guidelines shall not be destroyed or recollected for the purpose of avoiding disclosure.

Reason for retention:

ShotSpotter policy and SFPD retention schedule.

Deletion process:

It shall be the policy of the SFPD that once the requisite retention period for a record has passed, the record shall be destroyed unless there are particular circumstances that dictate that the record be retained. It shall be the policy of the SFPD work with contractors providing off-site storage of hardcopy records to ensure that records are destroyed once the requisite time period for retention has passed.

Retention exemption conditions:

ShotSpotter maintains verified gunshot data indefinitely.

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:

Members of the public and media may submit a public information request to the Department, however, ShotSpotter keeps the gunfire alert data and records confidential and secret by not releasing them to the public and by including Data restriction rights and confidentiality clauses in all customer agreements. Further, locations of specific sensors, gunshots at or near specific locations, and actual locations of areas covered is a matter of public safety and will not be released under any conditions. Additionally, the data is protected as some or all can be involved in on-going criminal investigations.

Criminal defendants may request to access the ShotSpotter data per the rules of criminal procedure around discovery and inspection. Accessibility will be determined by the courts.

How it can be requested by members of the public: https://www.sanfranciscopolice.org/get-service/public-records-request

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: San Francisco District Attorney's Office, San Francisco Public Defender's Office, US Attorney, CGIC Partners, City Attorney. ShotSpotter data will only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law.

Justification: Law Enforcement purposes/on-going criminal investigations or prosecutorial process.

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 ShotSpotter Gun Shot Detection Program Manager shall oversee the training program for any members with access to the ShotSpotter system and data. Additionally, the Manager shall ensure all members with access have reviewed the Surveillance Technology Policy for ShotSpotter.

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

Process for responding to complaints from members of the public:

The Department of Police Accountability (DPA), by Charter authority, receives and manages all citizen complaints relating to the police department.
Complaints that come to the Department from members of the public will be forwarded to the DPA.

Oversight process:

Should a violation of ShotSpotter occur, San Francisco Police Department will conduct an internal investigation though the Chief of Staff/Internal Affairs (IA) Unit. The results of the investigation will be reported to the Chief of Police, who will consider in determining the charges for instances of misconduct. Under San Francisco Charter section A8.343, the Chief may impose discipline of up to a 10-day suspension on allegations brought by the Internal Affairs Division or the DPA. Depending on the severity of the allegation of misconduct, the Chief or the DPA may elect to file charges with the Police Commission. Any discipline sought must be consistent with principles of just cause and progressive discipline.

Compliance personnel titles:

SFPD Investigations Commander and Deputy Chief, SFPD and ShotSpotter. In addition, each member of the Department belongs to a chain of command. The Officer in Charge (OIC) of that chain of command is responsible for overseeing compliance with all SFPD policies.

Restrictions:
1. Authorized personnel may access the ShotSpotter system SFPD may also notify authorized personnel of ShotSpotter activations. Authorized personnel may respond to such notifications based upon priorities as mandated by their supervisors.
2. The ShotSpotter system shall only be used for official law enforcement purposes.
3. Only specifically authorized personnel authorized by the Chief or Chief designee (e.g. personnel with SFPD's Investigations Division) will have access to historical ShotSpotter system data via desktop ShotSpotter system applications. The ShotSpotter system may be used for authorized patrol and investigation purposes. Contacting individuals at locations where ShotSpotter activations occur shall be conducted in accordance with applicable law and policy.
4. Accessing data collected by the ShotSpotter system requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation or assignment to a unit which responds to gunshot calls (e.g. Patrol Division).
5. Members approved to access ShotSpotter system data may only use data for legitimate law enforcement purposes only, such as when the data relate to gunshots, a specific criminal investigation or department-related civil or administrative action.
6. All verified ShotSpotter system activations are entered into SFPD's computer-aided dispatch (CAD) record management system (RMS) with ShotSpotter system specific ID numbers. Authorized personnel can then query the CAD/RMS system for any and all ShotSpotter system activations.

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:

Complaints from members of the public will be forwarded to the Department of Police Accountability(DPA) for investigation. DPA manages complaint responses.

Departmental follow-up process:

DPA manages the complaint follow- up process. Surveillance Technology Policies will have the same procedural authority as any Departmental Written Directive. Non-compliance can result in progressive discipline or sustained complaints.

Members of the public can register complaints with the Department of Police Accountability https://sfgov.org/dpa/complaints**.** *Members of the public can register questions and concerns or submit questions via calls or emails at 311.org.*