SHOTSPOTTER:
IMPACT AND USE POLICY

APRIL 11, 2021

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that ShotSpotter does not use artificial intelligence and machine learning.	Public comment highlighted a lack of industry-standard definitions for artificial intelligence and machine learning.
Expanded upon ShotSpotter capabilities.	Added language clarifying ShotSpotter capabilities.
Expanded upon ShotSpotter safeguards and security measures.	Added language regarding information security. Added language to reflect the removal of ShotSpotter data access when job duties no longer require access.
Expanded upon ShotSpotter data retention.	Added language to reflect NYPD obligations under federal, state and local record retention laws. Added language clarifying ShotSpotter sensor retention.
Expanded upon ShotSpotter external entities section.	Added language to reflect NYPD obligations under the local privacy laws.
Expanded upon disparate impact language for ShotSpotter.	Added information from an independent privacy audit and assessment of ShotSpotter's "extremely low" risk of being used for voice surveillance. Added language detailing ShotSpotter sensor location selection.
Minor grammar changes.	Minor syntax edits were made.

ABSTRACT

ShotSpotter is a gunshot detection system. ShotSpotter uses acoustic sensors to quickly detect and alert New York City Police Department (NYPD) personnel of confirmed gunfire incidents. The system reduces gunfire incident response times, provides valuable evidence for investigations and criminal prosecutions, and enhances both public and officer safety.

The NYPD produced this impact and use policy because the gunshot detection system processes acoustic data, and shares acoustic and location data with NYPD personnel.

CAPABILITIES OF THE TECHNOLOGY

When a gun is fired, the sudden expansion of highly pressurized gases creates a loud and sudden sound. Known as a muzzle blast, this sound is a byproduct of a successful gunshot. ShotSpotter sensors "listen" for gunshot-like sounds, i.e., sounds that are instantaneous, impulsive and sharp.

When at least three (3) different ShotSpotter sensors detect a gunshot-like sound, the precise time, location, and short audio snippet of the gunfire is immediately transmitted from the sensors to the ShotSpotter Incident Review Center where trained human analysts review all incident data. The analysts can determine whether the sound was gunfire or a similar noise, like fireworks or a car backfiring. The audio snippet consists of audio recorded one (1) second before the gunshot-like sound, the audio of the gunshot-like sound, and one (1) second after the gunshot-like sound.

In seconds, the NYPD is notified of confirmed gunfire report. A potential gunfire incident is automatically created in the Computer Aided Dispatch (CAD) system and routed to the proper NYPD precinct. The job is then assigned to a patrol unit. ShotSpotter can provide additional relevant information including the number of shots fired, whether the shooter was moving at the time of the incident and, if so, the direction of the shooter's movement.

Authorized NYPD personnel can access confirmed gunfire event data using Domain Awareness System (DAS).[1]

Human voices cannot initiate a possible gunfire events because they do not produce an instantaneous sharp sound loud enough to be picked up by three (3) or more sensors. Live streaming of ShotSpotter sensor audio is not possible by the NYPD or ShotSpotter employees.

ShotSpotter sensors are not positioned, tuned or designed to pick up human voices. The sensors are placed high above street level and use ordinary microphones; similar to ones found in cellphones. ShotSpotter devices are not and cannot be used to covertly listen to conversations, street-noise, or any non-gunfire acoustic data. ShotSpotter does not make use of any still or video cameras or biometric technologies.

[1] For additional information on DAS, please refer to the DAS impact and use policy.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD ShotSpotter policy seeks to balance the public safety benefits of this technology with individual privacy. ShotSpotter must be used in a manner consistent with the requirements and protection of the Constitution of the United States, the New York State Constitution, and applicable statutory authorities.

NYPD personnel may only use ShotSpotter for legitimate law enforcement purposes.

Court authorization is not necessary in order for the NYPD to use ShotSpotter. Gunfire detection sensors process acoustic data that is audible in open, public locations that do not enjoy a reasonable expectation of privacy.

In accordance with the Public Oversight of Surveillance Technology Act, an addendum to this impact and use policy will be prepared as necessary to describe any additional uses of ShotSpotter.

No person will be the subject of police action solely because of actual or perceived race, color, religion or creed, age, national origin, alienage, citizenship status, gender (including gender identity), sexual orientation, disability, marital status, partnership status, military status, or political affiliation or beliefs.

The misuse of ShotSpotter will subject employees to administrative and potentially criminal penalties.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

ShotSpotter sensor data is transmitted to the ShotSpotter Incident Review Center and to the NYPD over a secured stand-alone network. Data is encrypted both in transit and at rest via Secure Socket Layer (SSL)/Transport Layer Security (TLS) certifications.

Confirmed gunfire event data is accessible to NYPD personnel through DAS and may be stored in case management systems. DAS is confidential-password-protected and access is restricted to only authorized users. NYPD personnel authorized to access ShotSpotter data consist only of NYPD personnel in various commands, whose access has been requested by their Commanding Officer, and approved by the NYPD Information Technology Bureau (ITB). Confirmed gunfire event data is limited to NYPD personnel with an articulable need to use the information in furtherance of a lawful duty. Access to confirmed gunfire event data is removed when the technology is no longer necessary for NYPD personnel to fulfill their duties (e.g., when personnel are transferred to a command that does not use the technology).

NYPD personnel utilizing case management and computer systems are authenticated by username and password. Access to case management and computer systems is limited to personnel who have an articulable need to access the system in furtherance of lawful duty. Access rights within NYPD case management and computer systems are further limited based on lawful duty. Access levels are only granted for functions and abilities relevant to individual commands. Authorized users can only access data and perform tasks allocated to them by the system administrator according to their role.

The NYPD has a multifaceted approach to secure data and user accessibility within NYPD systems. The NYPD maintains an enterprise architecture (EA) program, which includes an architecture review process to determine system and security requirements on a case by case basis. System security is one of many pillars incorporated into the EA process. Additionally, all NYPD computer systems are managed by a user permission hierarchy based on rank and role via Active Directory (AD) authentication. Passwords are never stored locally; user authentication is stored within the AD. The AD is managed by a Lightweight Directory Access Protocol (LDAP) to restrict/allow port access. Accessing NYPD computer systems remotely requires dual factor authentication. All data within NYPD computer systems are encrypted both in transit and at rest via Secure Socket Layer (SSL)/Transport Layer Security (TLS) certifications which follow industry best practices.

NYPD personnel must abide by security terms and conditions associated with computer and case management systems of the NYPD, including those governing user passwords and logon procedures. NYPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the NYPD, only as required in the execution of lawful duty.

NYPD personnel are responsible for preventing third parties' unauthorized access to information. Failure to adhere to confidentiality policies may subject NYPD personnel to disciplinary and/or criminal action. NYPD personnel must confirm the identity and affiliation of individuals requesting information from the NYPD and determine that the release of information is lawful prior to disclosure.

Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

POLICIES & PROCEDURES RELATING TO RETENTION, ACCESS & USE OF THE DATA

ShotSpotter sensors store thirty (30) hours of audio. Audio older than thirty (30) hours is automatically deleted on what is known as a first-in-first-out basis; when new audio is processed, the oldest audio is deleted to make room. The audio is not transmitted to the Incident Review Center unless a possible gunfire incident is detected. NYPD personnel cannot access the audio retained in ShotSpotter sensors.

Under strict conditions, ShotSpotter personnel can access the 30 hours of stored audio if presented with evidence that a gunshot was missed. In this case, ShotSpotter personnel can review specific portions of the audio to determine if the system picked up the gunshot. If a missed gunshot is found, an audio snippet is provided to the NYPD. Only audio that is a confirmed gunfire incident is retained longer than thirty (30) hours.

ShotSpotter data may only be used for legitimate law enforcement purposes or other official business of the NYPD, including in furtherance of criminal investigations, civil litigations, and disciplinary proceedings. ShotSpotter data relevant to an investigation is stored in an appropriate NYPD computer or case management system. NYPD personnel utilizing case management and

computer systems are authenticated by username and password. Access to case management and computer systems is limited to personnel who have an articulable need to access the system in furtherance of lawful duty. Access rights within NYPD case management and computer systems are further limited based on lawful duty.

The Retention and Disposition Schedule for New York Local Government Records (the Schedule) establishes the minimum length of time local government agencies must retain their records before the records may be legally disposed.[2] Published annually by the New York State Archives, the Schedule ensures compliance with State and Federal record retention requirements. The NYC Department of Records and Information Services (DORIS) publishes a supplemental records retention and disposition schedule (the Supplemental Schedule) in conjunction with the Law Department specifically for NYC agencies in order to satisfy business, legal, audit and legal requirements.[3]

The retention period of a "case investigation record" depends on the classification of a case investigation record. The classification of case investigation records is based on the final disposition of the case, i.e., what the arrestee is convicted of or pleads to. Further, case investigations are not considered closed unless it results in prosecution and appeals are exhausted, it results in a settlement, it results in no arrest, or when restitution is no longer sought.

Case investigation records classified as a homicide, suicide, arson (first, second or third degree), missing person (until located), aggravated sexual assault (first degree), course of sexual conduct against a child (first degree), active warrant, or stolen or missing firearms (until recovered or destroyed), must be retained permanently. Case investigation records classified as a fourth degree arson or non-fatal (including vehicular accidents) must be retained for a minimum of ten (10) years after the case is closed. Case investigation records classified as any other felony must be retained for a minimum of twenty-five (25) years after the case is closed. Case investigation records classified as a misdemeanor must be retained for a minimum of five (5) years after the case is closed. Case investigation records classified as a violation or traffic infraction must be retained for a minimum of one (1) year after the case is closed. Case investigation records classified as an offense against a child as defined by the Child Victims Act, excluding aggravated sexual assault (first degree), course of sexual conduct against a child (first degree), must be retained until the child attains at least age fifty-five (55). Case investigation records connected to an investigation that reveals no offense has been committed by an adult must be kept for a minimum of five (5) years after the case is closed. Case investigation records connected to an investigation that reveals the individual involved was a juvenile and no arrest was made or no offense was committed must be kept for at least one (1) year after the juvenile attains age eighteen (18).

Personal information data files on criminals and suspects must be retained for at least five (5) years after the death of the criminal or suspect, or ninety (90) years after the criminal or suspect's date of birth as long as there has been no arrest in the last five (5) years, whichever is shorter. Personal information data files on associated persons, such as victims, relatives and witnesses must be retained as long as, or information as part of relevant case investigation record.

[2] *See* N.Y. Arts & Cult. Aff. Law § 57.19 - 25, *and* 8 NYCRR Part 185.
[3] *See* NYC Charter 3003.

The misuse of any ShotSpotter data will subject employees to administrative and potentially criminal penalties.

POLICIES & PROCEDURES RELATING TO PUBLIC ACCESS OR USE OF THE DATA

Members of the public may request ShotSpotter data pursuant to the New York State Freedom of Information Law. The NYPD will review and evaluate such requests in accordance with applicable provisions of law and NYPD policy.

EXTERNAL ENTITIES

If ShotSpotter data is relevant to a criminal case, the NYPD will turn the data over to the prosecutor with jurisdiction over the matter. Prosecutors will provide ShotSpotter data to the defendant(s) in accordance with criminal discovery laws.

Other law enforcement agencies may request ShotSpotter data from the NYPD in accordance with applicable laws and regulations, and NYPD policies. Additionally, the NYPD may provide ShotSpotter data or information related to it to partnering law enforcement and city agencies pursuant to on-going criminal investigations, civil litigation, and disciplinary proceedings. Information is not shared in furtherance of immigration enforcement.

Following the laws of the State and City of New York, as well as NYPD policy, information related to ShotSpotter may be provided to community leaders, civic organizations and the news media in order to further an investigation, create awareness of an unusual incident, or address a community-concern.
Pursuant to NYPD policy and local law, NYPD personnel may disclose identifying information externally only if:

1. Such disclosure has been authorized in writing by the individual to whom such information pertains to, or if such individual is a minor or is otherwise not legally competent, by such individual's parent or legal guardian and has been approved in writing by the Agency Privacy Officer assigned to the Legal Bureau;
2. Such disclosure is required by law and has been approved in writing by the Agency Privacy Officer assigned to the Legal Bureau;
3. Such disclosure furthers the purpose or mission of the NYPD and has been approved in writing by the Agency Privacy Officer assigned to the Legal Bureau;
4. Such disclosure has been pre-approved as in the best interests of the City by the City Chief Privacy Officer;
5. Such disclosure has been designated as routine by the Agency Privacy Officer assigned to the Legal Bureau;
6. Such disclosure is in connection with an investigation of a crime that has been committed or credible information about an attempted or impending crime;
7. Such disclosure is in connection with an open investigation by a City agency concerning the welfare of a minor or an individual who is otherwise not legally competent.

Government agencies at the local, state, and federal level, including law enforcement agencies other than the NYPD, have limited access to NYPD computer and case management systems. Such access is granted by the NYPD on a case by case basis subject to the terms of written agreements between the NYPD and the agency receiving access to a specified system. The terms of the written agreements also charge these external entities with maintaining the security and confidentiality of information obtained from the NYPD, limiting disclosure of that information without NYPD approval, and notifying the NYPD when the external entity receives a request for that information pursuant to a subpoena, judicial order, or other legal process. Access will not be given to other agencies for purposes of furthering immigration enforcement.

The NYPD purchases ShotSpotter and associated equipment or Software as a Service (SaaS)/software from approved vendors. The NYPD emphasizes the importance of and engages with vendors and contractors to maintain the confidentiality, availability, and integrity of NYPD technology systems.

Vendors and contractors may have access to NYPD ShotSpotter associated software or data in the performance of contractual duties to the NYPD. Such duties are typically technical or proprietary in nature (e.g., maintenance or failure mitigation). In providing vendors and contractors access to equipment and computer systems, the NYPD follows the principle of least privilege. Vendors and contractors are only allowed access on a "need to know basis" to fulfill contractual obligations and/or agreements.

Vendors and contractors providing equipment and services to the NYPD undergo vendor responsibility determination and integrity reviews. Vendors and contractors providing sensitive equipment and services to the NYPD also undergo background checks.

Vendors and contractors are legally obligated by contracts and/or agreements to maintain the confidentiality of NYPD data and information. Vendors and contractors are subject to criminal and civil penalties for unauthorized use or disclosure of NYPD data or information.

If ShotSpotter data is disclosed in a manner violating the local Identifying Information Law, the NYPD Agency Privacy Officer, upon becoming aware, must report the disclosure to the NYC Chief Privacy Officer as soon as practicable. The NYPD must make reasonable efforts to notify individuals effected by the disclosure in writing when there is potential risk of harm to the individual, when the NYPD determines in consultation with the NYC Chief Privacy Officer and the Law Department that notification should occur, or when legally required to do so by law or regulation. In accordance with the Identifying Information Law, the NYC Chief Privacy Officer submits a quarterly report containing an anonymized compilation or summary of such disclosures by City agencies, including those reported by the NYPD, to the Speaker of the Council and makes the report publically available online.

TRAINING

All recruits attending the NYPD Police Academy receive training on the proper operation of DAS and its associated equipment. NYPD personnel receive command level training on the proper use of ShotSpotter. All NYPD personnel use DAS and ShotSpotter in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

Supervisors of personnel are responsible for security and proper utilization of NYPD technology and associated equipment. Supervisors are directed to inspect all areas containing NYPD computer systems at least once each tour and ensure that all systems are being used within NYPD guidelines.

Any search conducted in DAS relating to ShotSpotter data is auditable by ITB.

All NYPD personnel are advised that NYPD computer systems and equipment are intended for the purposes of conducting official business. The misuse of any system or equipment will subject employees to administrative and potentially criminal penalties. Allegations of misuse are internally investigated at the command level or by the Internal Affairs Bureau (IAB).

Integrity Control Officers (ICOs) within each Command are responsible for maintaining the security and integrity of all recorded media in the possession of the NYPD. ICOs must ensure all authorized users of NYPD computer systems in their command understand and comply with computer security guidelines, frequently observe all areas with computer equipment, and ensure security guidelines are complied with, as well as investigating any circumstances or conditions which may indicate abuse of the computer systems.

Requests for focused audits of computer activity from IAB, Commanding Officers, ICOs, Investigations Units, and others, may be made to ITB.

HEALTH & SAFETY REPORTING

There are no known health and safety issues with ShotSpotter or the associated equipment.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The safeguards and audit protocols built into this impact and use policy for ShotSpotter mitigate the risk of impartial and biased law enforcement. ShotSpotter only notifies NYPD personnel of a potential gunfire incident. ShotSpotter cannot be used to covertly listen to conversations, street-noise, or any noise that is not gunfire. ShotSpotter does not use biometric measurement technologies.

An independent privacy audit conducted in 2019 by the Policing Project at New York University School of Law concluded that the risk of voice surveillance using ShotSpotter is "extremely low.[4]"

The NYPD uses a data-driven approach to request ShotSpotter coverage in areas experiencing recurrent or an increased number of shooting incidents. ShotSpotter engineers determine where to place sensors to optimize even gunshot detection throughout an area. The NYPD does not determine sensor locations and does not have access to a database of sensor locations kept by ShotSpotter.

[4] *Privacy Audit & Assessment of ShotSpotter, Inc.'s Gunshot Detection Technology*, POLICING PROJECT AT N.Y.U., https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5d40c3693d74b7000160dfbc/1564525424759/Privacy+Audit+and+Assessment+of+Shotspotter+Flex.pdf (last visited Mar. 31, 2021).

The NYPD is committed to the impartial enforcement of the law and to the protection of constitutional rights. The NYPD prohibits the use of racial and bias-based profiling in law enforcement actions, which must be based on standards required by the Fourth and Fourteenth Amendments of the U.S. Constitution, Sections 11 and 12 of Article I of the New York State Constitution, Section 14-151 of the New York City Administrative Code, and other applicable laws.

Race, color, ethnicity, or national origin may not be used as a motivating factor for initiating police enforcement action. When an officer's decision to initiate enforcement action against a person is motivated even in part by a person's actual or perceived race, color, ethnicity, or national origin, that enforcement action violates NYPD policy unless the officer's decision is based on a specific and reliable suspect description that includes not just race, age, and gender, but other identifying characteristics or information.