



 **ShotSpotter[®]**

Gunshot Detection



ShotSpotter Report – 8th Precinct

8th Precinct			
	Last Week	Quarter to Date	Year to Date
Incidents	7	47	47
Shots Fired	26	967	967
Guns Recovered	1	4	4



ShotSpotter Report – 9th Precinct

9th Precinct			
	Last Week	Quarter to Date	Year to Date
Incidents	30	186	186
Shots Fired	114	1,863	1,863
Guns Recovered	1	4	4



ShotSpotter 2021

	2021 Total		
	All	2021 8 th PCT	2021 9 th PCT
Incidents	3,878	936	2,942
Shots Fired	15,710	3,942	11,768
Guns Recovered	218	36	182



ShotSpotter Arrests

2021 ShotSpotter Incidents With Arrest(s) Made

All	2021 8 th PCT	2021 9 th PCT
76	14	62

2022 YTD ShotSpotter Incidents With Arrest(s) Made

All	2022 8 th PCT	2022 9 th PCT
3	3	0



Reported Shots Fired Incidents

Weekly Avg Shots Fired CFS and ShotSpotter Runs

	All	8 th PCT	9 th PCT
Pre - CFS	15.5	6.5	8.5
Post - Runs	91.4	21.8	69.5
Post - CFS	5.0	2.0	3.0



Notification of Deficiencies

307.8 - 5 Responsibilities

307.8 - 5.1 Crime Intelligence Unit

5. Notify ShotSpotter Technology of any deficiencies, including but not limited to:
 - a. That the location of an incident was inaccurate or
 - b. A confirmed firearm discharge within the coverage area was never reported by the gunshot detection system;

Service level agreement of 90% accuracy of missed notifications, mislocates and misclassifications



Training Requirement

307.8 - 5.5 Professional Education and Training

Professional Education and Training (PET) shall be responsible for coordinating training on ShotSpotter application use and on the ShotSpotter response process. PET shall ensure that the following members are trained in ShotSpotter:

- a. Any sworn member assigned to a precinct where any part of a Coverage Area falls within their precinct;
- b. Detective Bureau personnel assigned to cases that could involve a firearm discharge incident;
- c. Any sworn member who indicate interest in receiving the ShotSpotter training;
- d. Precinct Intelligence Unit members; and
- e. Communications Operations members.

- Training conducted **on two (2) occasions** before access to ShotSpotter system is given
- Virtual or In-Person format on **system usage, DPD Gunshot Detection Policy**
- Continuing access to **ShotSpotter Litmos Training** site and resources



ShotSpotter Technology uses audio sensors to pinpoint location of gunfire

ShotSpotter Can

- Detect outdoor audible gunfire with a defined perimeter
- Send a short audio snippet to the ShotSpotter Incident Review Center (IRC).

ShotSpotter Cannot

- Be triggered by human voices
- Produce live streaming of sensor audio by company employees, police, or other third parties



DPD policy has strict civil liberty protections

- **DPD cannot monitor live audio** from audio sensors
- DPD can only hear **audio from confirmed gunshot incidents**
- Recorded audio shall only be reviewable when pertinent **to an active investigation** involving the discharge of a firearm
 - *Audio only includes one second before and after the firearm discharge*
- Violations of these protections will be subject to **discipline or termination**



DPD policy has strict civil liberty protections

- ShotSpotter alert, by itself, **does not give responding members the legal authority to enter private residences, private buildings,** and the constitutional curtilage surrounding those properties
- **ShotSpotter as Investigative Lead ONLY.** Members shall not arrest solely on a ShotSpotter notification
 - Any possible connection/involvement of any subject must be determined through further investigation and investigative resources



Contract Details: ShotSpotter Inc.

Conditions

- All data is owned exclusively by the City.
- ShotSpotter must receive written permission prior to releasing, selling, disseminating any data unless there is a court order, or subpoena.
- Within 60 days after the termination of the contract, ShotSpotter agrees to deactivate sensors and delete all user account information.

- **No cameras are included in this contract.**
- **No facial recognition software is being used for this project.**
- **Audio is permanently deleted after 30 hours if no gunshot is detected.**
- **DPD cannot listen to live audio from the sensors. DPD can only listen to recorded audio from a sensor of a confirmed or likely gunshot incident.**



Overview of Community Privacy Protections

Making Communities Safer





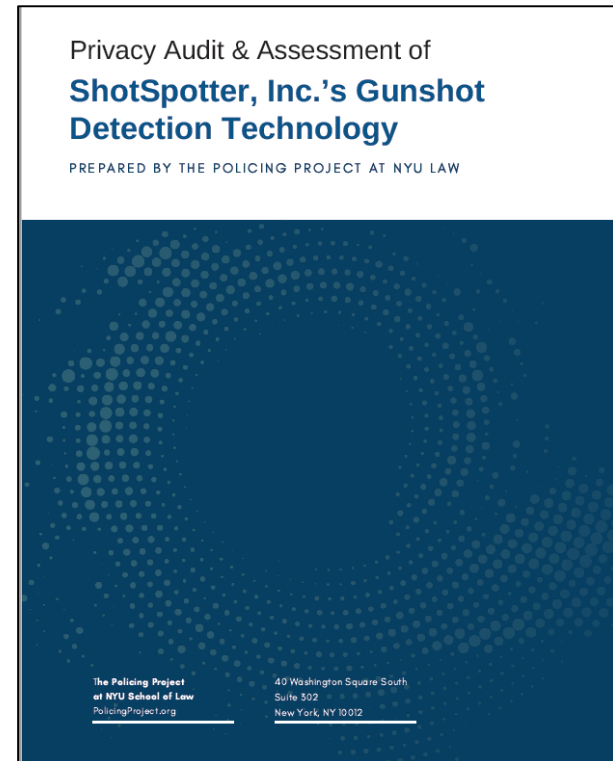
Summary

- ShotSpotter has been incorporating privacy protections into its gunshot detection technology and policies for several years
- In 2019 the company commissioned an independent audit of its technology, processes and policies to get an unbiased view of its approach to privacy. The report confirmed the risk of voice surveillance is extremely low and the auditing organization praised the company for taking steps to further enhance its privacy protections based on the audit
- The ShotSpotter gunshot detection solution unanimously passed review by the city of Oakland in November 2019 which has one of the most stringent city surveillance ordinances in country. In November 2020, the system also passed review by the San Francisco Privacy and Surveillance Board. [Related article](#)
- They train all existing and new employees on privacy protections and constantly consider privacy a key factor when assessing the development of new features and products



Independent Privacy Audit Conclusions and Recommendations

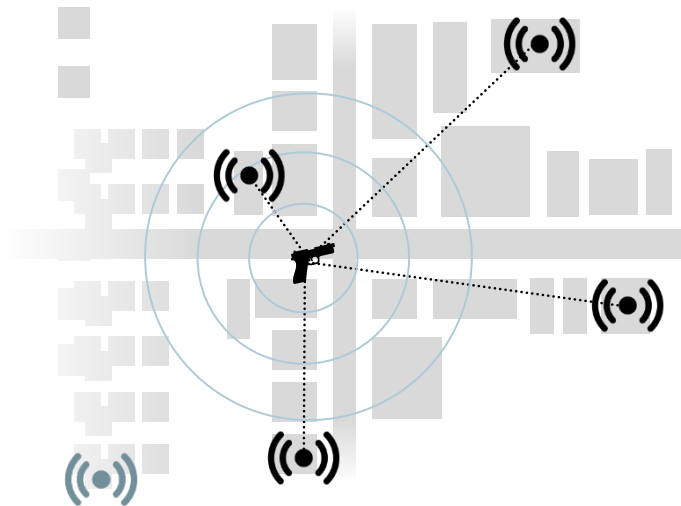
- **Policing Project at NYU Law School** conducted independent review of ShotSpotter privacy policies and procedures in 2019.
- Given **total access** to all systems and documentation and **total editorial control** over report content
- Overall assessment
 - “We ultimately conclude that **the risk of voice surveillance is extremely low.**”
 - “While sensors constantly are “listening,” audio is only temporarily stored, and audio is only retained if the computer algorithm or human reviewer detects a gunshot. All other audio is routinely purged from SST’s systems.”
- ShotSpotter adopted Policing Project’s 11 **detailed recommendations** to further minimize any risk:
 - Reduce audio pool from 72 hours to 30 hours
 - Minimize length of audio snippets to 1 second before and after the incident itself
 - Strengthen internal access procedures
- Policing Project’s **full report** available at: policingproject.org/ShotSpotter





Community Privacy Protections: Before and During an Incident

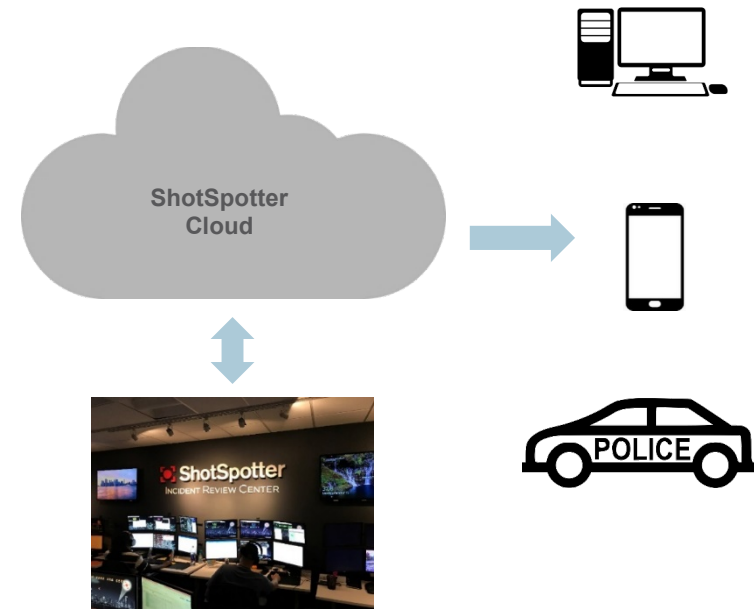
- Sensors “listen” for gunshot-like sounds and trigger only when detecting an impulsive sound (instantaneous and sharp). When at least three different sensors detect a gunshot-like sound at the same time and determine a location, they send a short audio snippet to the ShotSpotter Incident Review Center (IRC).
- Human voices will never trigger a sensor because they do not produce an instantaneous sharp sound and they are not loud enough to be picked up by three or more sensors.
- Live streaming of sensor audio is not possible by company employees, police or third parties.





Community Privacy Protections: Before and During an Incident

- Upon detecting a likely gunshot, trained ShotSpotter personnel listen to a short computer-generated audio snippet of the gunfire to double check that it is actually gunfire. This snippet only includes the gunfire sound and 1 second before and after to establish ambient noise.
- It is highly unusual for a human voice to be included in a snippet. For this to occur, the voice must be concurrent with the gunfire. There is no personally identifiable information in any ShotSpotter audio snippet.
- In the past extended audio was available to police agencies and prosecutors for court cases. This is no longer possible under new policy and technology controls.





Community Privacy Protections: After an Incident

- The company made changes to the system since 2012 to prevent police and employee access to extended audio.
- If ShotSpotter receives a request, including a subpoena, for additional audio beyond the gunshot snippet, the company has and will continue to fight the request.
- Occasionally, police contact ShotSpotter because a gunshot incident was not picked up by our sensors. Sensors store 30 hours of audio and automatically delete audio older than 30 hours. Neither police nor third parties ever have direct access to this audio.

