ShotSpotter®

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

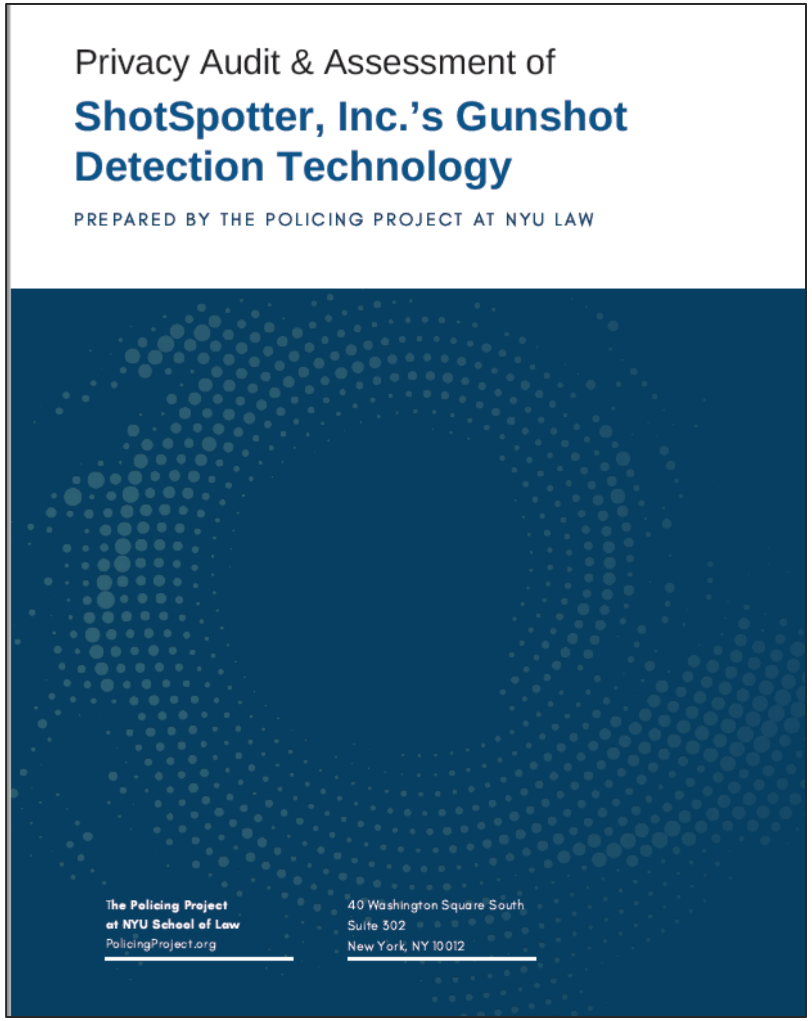
- In 2019 the company commissioned an independent audit of its technology, processes and policies to get an unbiased view of its approach to privacy. The report confirmed the risk of voice surveillance is extremely low and the auditing organization praised the company for taking steps to further enhance its privacy protections based on the audit (details on next slide)

- 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

- We 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 spool 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



Privacy Audit & Assessment of

ShotSpotter, Inc.’s Gunshot Detection Technology

PREPARED BY THE POLICING PROJECT AT NYU LAW

The Policing Project
at NYU School of Law
PolicingProject.org

40 Washington Square South
Suite 302
New York, NY 10012

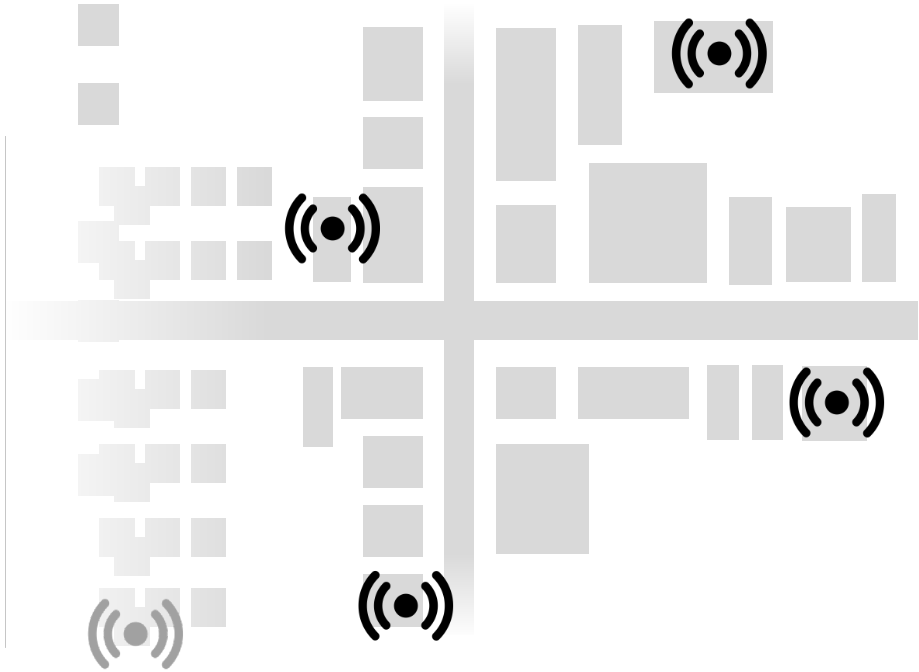
Community Privacy Protections: Prior to System Activation

- When ShotSpotter comes to a new city, we strongly encourage our police agency customers to engage with their communities about the decision to acquire and use our technology.

- Using a data-driven approach, ShotSpotter works with our clients to determine the geographic area they want covered by ShotSpotter (i.e. the most gun violent areas)

- When the coverage area is set, ShotSpotter engineers determine where to place sensors so as to allow even gunshot detection throughout the area. Police do not determine where to place sensors and do not have access to a database of sensor locations.

- ShotSpotter acoustic sensors are not positioned, tuned or specialized to pick up human voices. The sensors use ordinary microphones and are placed high above the street.

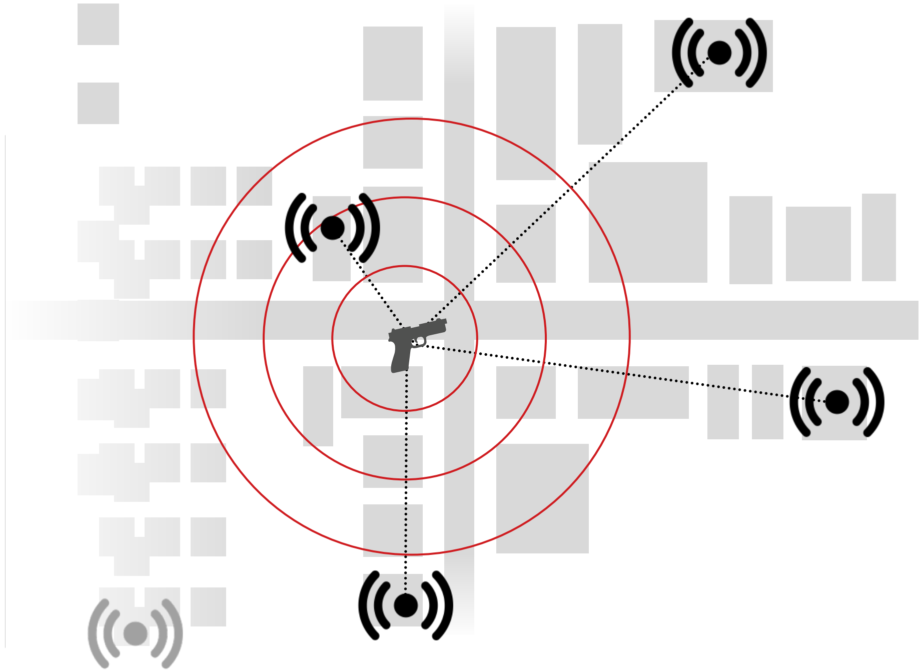


Community Privacy Protections: Before and During an Incident

- 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.

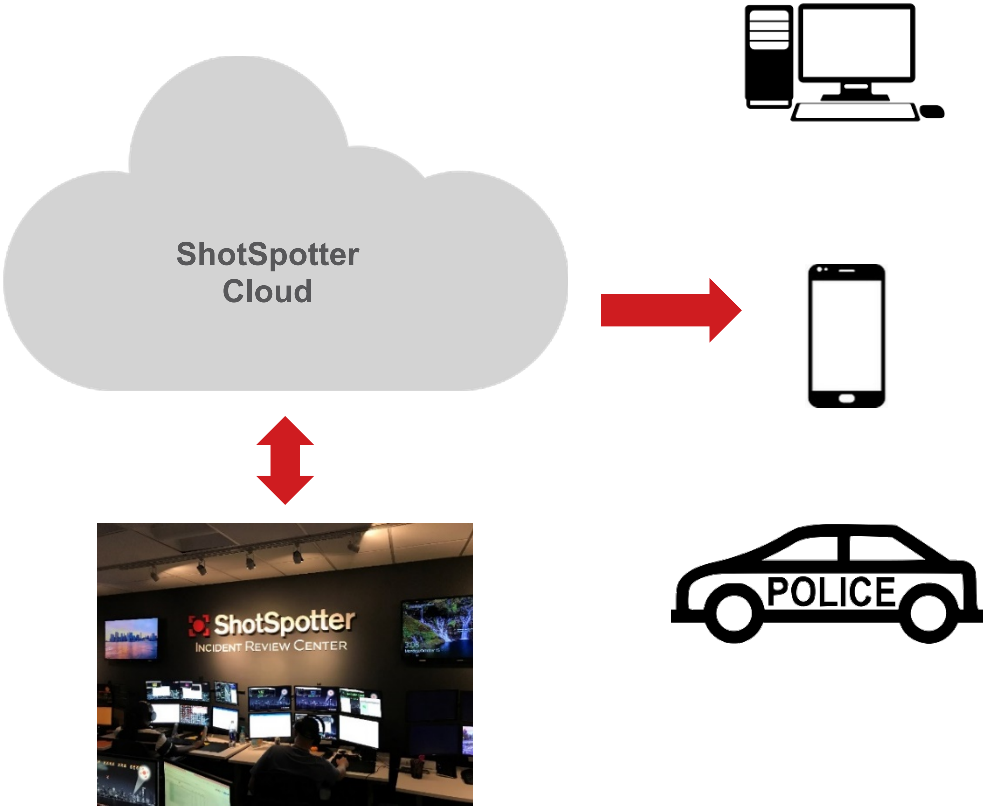


Community Privacy Protections: Before and During an Incident

- 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 and loud enough to be heard over 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.

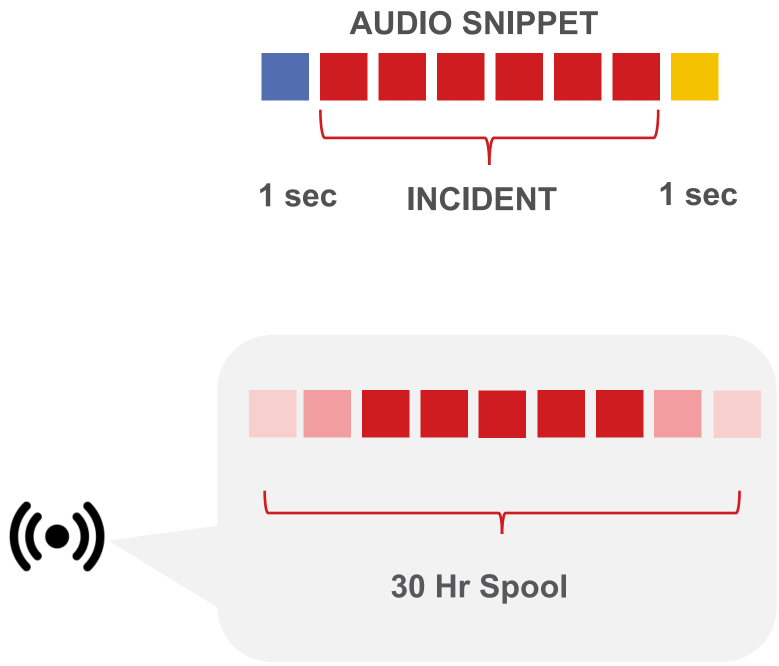


Community Privacy Protections: After an Incident

- 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 may not have triggered an alert. 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.


AUDIO SNIPPET
1 sec
INCIDENT
1 sec
30 Hr Spool