ShotSpotter Privacy FAQ

What protections are in place to protect community privacy?

There are multiple technology and policy protections in place to protect against audio surveillance:

- Sensors are placed high above the street typically on building or streetlights to avoid street level sounds and the microphones used are not specialized in any way (i.e. everyday cell phone quality)
- The system is tuned to listen for loud impulsive sounds that are gunshots or similar to gunshots (fireworks, car backfires) and takes no action on other sounds that would include street level sounds or human voices
- The sensors store a limited amount of audio locally and that audio is automatically purged every 30 hours
- Sensors are triggered and an incident created only when 3 or more sensors hear the same loud impulsive sound and can verify a location. This creates an incident and sends a short audio snippet to the ShotSpotter Incident Review center. The snippet has the gunfire and 1 second of audio prior to and after the gunfire to establish an ambient noise level. Audio snippets are typically only a few seconds long unless there is a gun battle.
- The company's culture of privacy protection builds in proper measures when new features or processes are contemplated

Has there been independent research to validate the protections?

- The Policing Project of NYU Law School conducted an independent audit of ShotSpotter's gunshot detection system to evaluate the privacy risk. In July 2019 they published a report that stated that there is an extremely low risk of human voice surveillance.
- The Oakland Privacy Advisory Commission reviewed ShotSpotter in November 2019 under one the most stringent local surveillance ordinances in the country. The Commission unanimously approved the continued use of ShotSpotter.
- In 2020, the ShotSpotter system passed review by the San Francisco Privacy Advisory and Surveillance Board.

Can anyone listen to live stream audio or recorded audio from the sensors?

- There is no ability to listen to live streamed audio from the sensor
- If the system misses a gunfire incident, police may contact the company to see if there is any audio or location evidence. In this case, only authorized ShotSpotter personnel with proper credentials can access sensor audio to search. Their search is limited to the 30-hour sensor storage timeframe. The agency must provide evidence of a shooting in order for ShotSpotter personnel to initiate access to a sensor such as a victim, witness or shell casings. Searching is done visually first, not by listening, to identify when impulsive sound events occurred. Once these events are noted, a short portion of the audio is downloaded for auditory review. An audit trails tracks who accessed the sensor and who requested the audio search.

How sensitive are the sensors to picking up voices?

- While an individual sensor could potentially hear a human voice, that sound would be purged within 30 hours with no ShotSpotter employee, police department customer or other 3rd party having the ability to hear it unless an incident was created.
- Human voices are not loud enough to trigger sensors and are rarely heard as part of an incident under review. The person would have to be screaming very loudly above the loud sound that initiated the incident and the audio last only a few seconds.
- 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.

Can you identify anyone through your system?

- No personally identifiable information is associated with an incident.

What data is stored and for how long?

- Audio at the sensor level is purged every 30 hours
- If an incident is created and sent to our Incident Review Center the short audio snippet is stored permanently for evidentiary purposes as well as to train the machine learning model.

Has the system always had these protections?

- The technology and privacy policies have evolved over time. Up until approximately 2012, police departments had direct access to extended audio and some agencies used that to get auditory evidence of sounds prior to and after a gunshot. Significant new protections have been added so that police no longer have access to extended audio and only are able to hear the short audio snippets that are produced when the system and human reviews believe a sound is a gunshot.