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


Policing
Project
NYU School of Law

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

ShotSpotter Inc. ("SST") is a California-based company that operates ShotSpotter Flex (hereafter referred to as "ShotSpotter"), 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. SST's primary customers are local law enforcement agencies.

Earlier this year, SST asked the Policing Project at New York University School of Law to conduct a thorough privacy assessment of ShotSpotter. Our engagement with SST focused on identifying the risks ShotSpotter poses to personal privacy and to suggest technological, policy, and procedural changes to address those risks. We agreed to conduct this assessment on the condition that we have complete access to all SST policies, procedures, and personnel related to ShotSpotter,[1] and that we have complete editorial control over our recommendations and report. In our view, SST has been notably open and transparent throughout this process.

Having conducted a thorough review of SST's current policies and procedures, and as explained in more detail below, we believe that on the whole ShotSpotter presents relatively limited privacy risks. In our analysis, the primary personal privacy concern with ShotSpotter is the possibility that the technology could capture voices of individuals near the sensors, and conceivably could be used for deliberate voice surveillance. Although we believe the risk of this occurring is already relatively low, this report offers a variety of recommendations for how SST can make ShotSpotter even more privacy protective.

As discussed in more detail in this report, our recommendations cover a wide range of issues, chief among them that SST:

1. Substantially reduce the duration of audio stored on ShotSpotter sensors;
2. Commit to denying requests and challenging subpoenas for sensor audio;
3. Commit to not sharing specific sensor location; and
4. Improve internal controls and supervision regarding audio access.

SST has adopted nearly all of our recommendations verbatim, with only

1. Contractual arrangements prevented SST from providing us with one piece of information. See *infra* Part VI.

slight modifications or qualifications based on how ShotSpotter functions.

Although we were asked to comment on ShotSpotter's personal privacy implications, we conclude our analysis by offering some additional guidance regarding data sharing with third parties. Although we do not see this as a personal privacy issue, we believe this is one area where SST can and should refine its approach. SST has taken these comments seriously and is in the process of thinking through its response.

Throughout this process, SST has consistently demonstrated commendable commitment to modifying its technology to balance its public safety function with protections for individual privacy. The changes we asked SST to make—both to how their technology operates and their internal procedures—were certainly not without cost. SST made a conscious choice to bear these costs. We hope others follow SST's leadership in this regard; indeed, we believe this type of open audit and assessment—whether performed by us or by others—should become the norm for companies selling technologies to governments and policing agencies.

Indeed, we believe this type of open audit and assessment—whether performed by us or by others—should become the norm for companies selling technologies to governments and policing agencies.

II. OUR ENGAGEMENT WITH SHOTSPOTTER

ABOUT THE POLICING PROJECT

The Policing Project is a non-profit entity at New York University School of Law. Our mission is to partner with communities and police to promote public safety through transparency, equity, and democratic engagement. (More information about our mission is available in Part VIII or at www.policingproject.org.)

One of the Policing Project's core areas of focus is policing technologies. Certain new technologies hold great promise to make policing safer, more effective, and more accountable. But at the same time, we have serious concerns about possible invasions of privacy, inaccuracy, and perpetuation of racial bias. Rather than being "for" or "against" a new technology, we believe the proper approach is to figure out if society can benefit from a particular technology while eliminating or minimizing any harm. In this regard, cost-benefit analysis of policing technologies is both appropriate and essential. The decision to deploy any technology should have democratic approval based on public information about the potential benefits and harms. Democratic legitimacy requires the inclusion in that process of those communities most impacted by the use of the technology.

To that end, we have adopted a range of strategies. In consultation with police and affected communities, we are drafting use policies for a variety of new technologies, including drones, predictive analytics, social media monitoring, and more. We are conducting rigorous social science research into the effectiveness of certain technologies.[2] We are also developing tools that encourage public authorization before policing technologies are acquired or used.

Rather than being "for" or "against" a new technology, we believe the proper approach is to figure out if society can benefit from a particular technology while eliminating or minimizing any harm.

One of our strategies is to work directly with certain private companies in the policing technology space to assess their products; offer recommendations as to whether those products pose civil rights or civil liberties concerns; and recommend how those concerns might be mitigated, either through design, use policies, or internal procedures.[3] To this end, we have determined that, when invited to do so by municipalities, law

2. With the generous support of the Laura & John Arnold Foundation, the Policing Project and Professor Jillian Carr of Purdue University Krannert School of Management are conducting a cost-benefits analysis of the St. Louis County Police Department's use of ShotSpotter. This privacy assessment and our research study have from the outset remained entirely independent.
3. Relatedly, Policing Project Faculty Director Barry Friedman sits on the Axon AI and Policing Technology Ethics Board, and the Policing Project staffs the Board. See http://www.policingproject.org/axon-ethics-board

enforcement agencies, or private vendors, we will conduct an audit and assessment of policing technologies. SST has exercised commendable leadership in opening itself up to this assessment. We hope this becomes the norm for companies selling technologies that pose civil liberties or civil rights concerns, including those involving racial inequities. Such evaluation is essential so that communities can make wise acquisition and regulatory decisions.

Throughout our work, we disclose any conceivable conflicts, particularly when private companies are involved. Since 2018, SST has provided the Policing Project with unrestricted funding (as do other entities) for our policing technology work in general. SST compensated us for our time and travel in conducting this audit and assessment. SST CEO Ralph Clark also sits on our Advisory Board.[4] Note that our Board is *advisory* only with no legal authority or governing powers over the organization. This pre-existing relationship played a large part in initiating this work.

THE PRESENT ENGAGEMENT

In February 2019, during the course of discussions of adopting ShotSpotter in Toronto, segments of that community raised a number of reservations, including privacy-related concerns.[5] After the Toronto Police Department ultimately decided not to pursue ShotSpotter, SST contacted the Policing Project to discuss how it could address concerns like those raised in Toronto. At that time, as discussed above, we already were developing a model for the audit and assessment of policing technologies. Thus, we suggested SST engage us to conduct an audit and assessment of ShotSpotter from a privacy perspective.

Before going further, we think it essential to explain that this report is in no way a comment on the concerns raised in Toronto (or any other city). Each community has its unique laws, concerns, and history, and the Policing Project believes that every community should decide for itself what policing technologies are appropriate for their specific needs. This is the essence of front-end accountability, which motivates all our work. Our aim is to provide information to the public that can aid in sound and informed decision-making about policing technologies.

We hope that for companies selling technologies that pose civil liberties or civil rights concerns, including those involving racial justice, it becomes the norm to have products evaluated in this way.

In April 2019, SST officially engaged the Policing Project to conduct a thorough privacy assessment of its policies and procedures for ShotSpotter, and to make concrete suggestions as to how SST could address privacy concerns. Because we were

4. To view our full advisory board, visit: http://www.policingproject.org/our-advisory-board.
5. See, e.g., Jeff Gray, *Toronto police end ShotSpotter project over legal concerns*, THE GLOBE AND MAIL (Feb. 13, 2019), https://www.theglobeandmail.com/canada/toronto/article-toronto-police-end-shotspotter-project-over-legal-concerns/.

asked to conduct a *privacy*-focused assessment, we focused on what sort of data is captured, aggregated, mined, retained, and shared. We did not analyze other potential benefits or costs of ShotSpotter or any other SST technology. For example, we have not evaluated how well SST's gun detection technology actually works (its rate of false positives or negatives) or the process by which ShotSpotter reports are admitted into evidence at criminal trials. We have not explored or evaluated any other potential civil rights or civil liberties concerns.

We believe it is essential that private companies in the policing technology space take seriously their obligation to minimize their impact on civil rights and civil liberties.

Our assessment process began with a thorough document review—both of publicly available information and internal SST materials, such as contracts, training materials, and documents provided to law enforcement customers. We conducted a site visit to SST's Newark, California headquarters, interviewed numerous SST personnel, and observed SST's Incident Review Center in action. We followed up with additional questions and received additional information. We provided SST with a set of recommendations in May, giving SST time to evaluate and respond to our recommendations before the publication of this report.

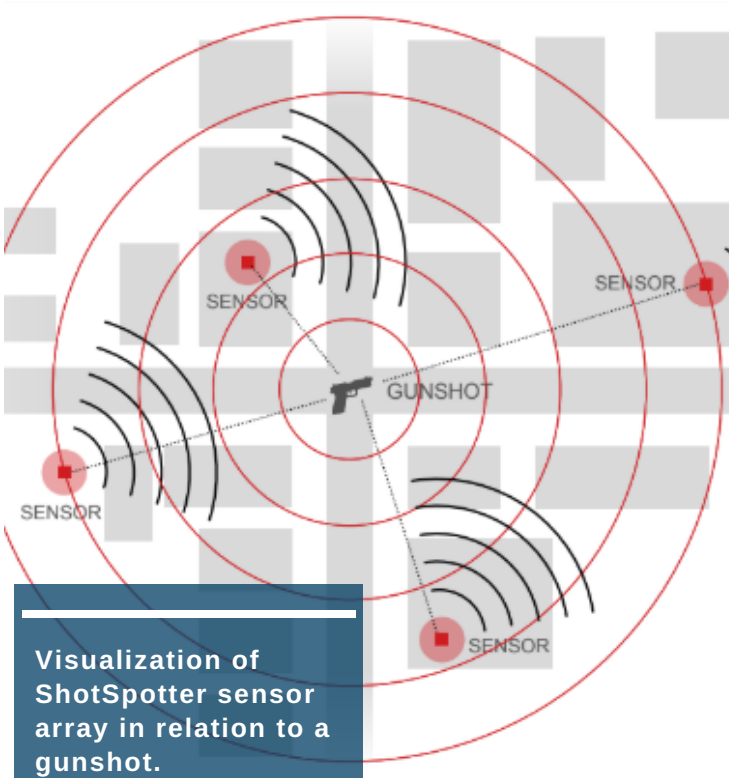
We have had complete control over the substance of our recommendations and the contents of this report. SST has reviewed it for factual errors only.

This is our first such engagement. Although we do not think this type of private engagement can or should take the place of community voice or official regulation, we believe it is essential that private companies in the policing technology space take seriously their obligation to minimize their impact on civil rights and civil liberties. We see this type of engagement—whether performed by us or others having the relevant expertise—as an important model for improving the transparency and accountability of policing technologies across the country.

III. HOW SHOTSPOTTER FLEX WORKS

According to SST, ShotSpotter is a "gunshot detection, location, and forensic analysis" technology. Specifically, ShotSpotter analyzes sound to detect that gunfire has occurred, locate the source of that gunfire, and determine certain characteristics of the gunfire (such as how many shots were fired and the precise timing of those shots).

The technology has two basic components: (1) an array of microphone-equipped sensors spread across the coverage area, and (2) the ShotSpotter Incident Review Center ("IRC") at SST headquarters in Newark, California.



Visualization of ShotSpotter sensor array in relation to a gunshot.

The process begins with SST working with the customer to determine the desired physical boundaries for ShotSpotter's gunshot detection technology. Ultimately, the choice of boundaries is one for the customer, considering the needs and resources of the particular community. The larger the coverage area, the greater the cost.

Once the coverage area is set, SST engineers work to determine how many sensors are needed and where they should be placed in order to achieve reliable detection throughout the area. Sensors are equipped with microphones that are similar to a typical smartphone microphone at picking up sound. SST personnel install the sensors on buildings and lampposts typically 20-30 feet above the ground. Sensors are placed this high so as to maximize their range, require lower sensor density, and to minimize street-level audio. The sensor network is then tested to ensure proper operation.

Once operational, these sensors are continuously "listening" and a proprietary AI-enhanced algorithm is constantly analyzing incoming audio. The algorithm reviews the audio for loud "impulsive" sounds—that is, loud sounds that start and end suddenly (similar to a gunshot). In addition to actual gunfire, impulsive sounds

that trigger the algorithm can include certain construction noises, helicopters, motorcycles, fireworks, and other similar sounds. Whenever ShotSpotter's algorithm detects an impulsive sound, the algorithm attempts to identify these sounds (e.g., "gunfire," "helicopter," "construction"). Although all audio, including street noise, traffic, or human voice, are inputs to the algorithm, only gunshot-like sounds ("impulsive" sounds) actually trigger the sensor and the next stage of the process.

notifications from customer locations around the world to determine whether the impulsive sounds detected by the ShotSpotter algorithm are actual gunshots.[6] The IRC is notified of the majority, but not all, of the impulsive sounds that trigger three sensors. As the ShotSpotter algorithm has improved over time, SST has determined that its system is sufficiently accurate in identifying particular types of impulsive sounds, such as helicopters or fireworks, so that these

Technicians in the ShotSpotter Incident Review Center

When three or more sensors are triggered at the same time—that is, they detect an impulsive sound (such as a gunshot)—the IRC is notified as to the time and location of the event. Requiring three sensors to detect a sound is necessary to determine a precise location. It also means that softer sounds (e.g., a car door) will not trigger a notification of the IRC. There is no human involvement until after the IRC is notified via an encrypted cellular network.

In the IRC, SST personnel constantly review

type of incidents often are not sent to the IRC and are discarded as non-gunfire.

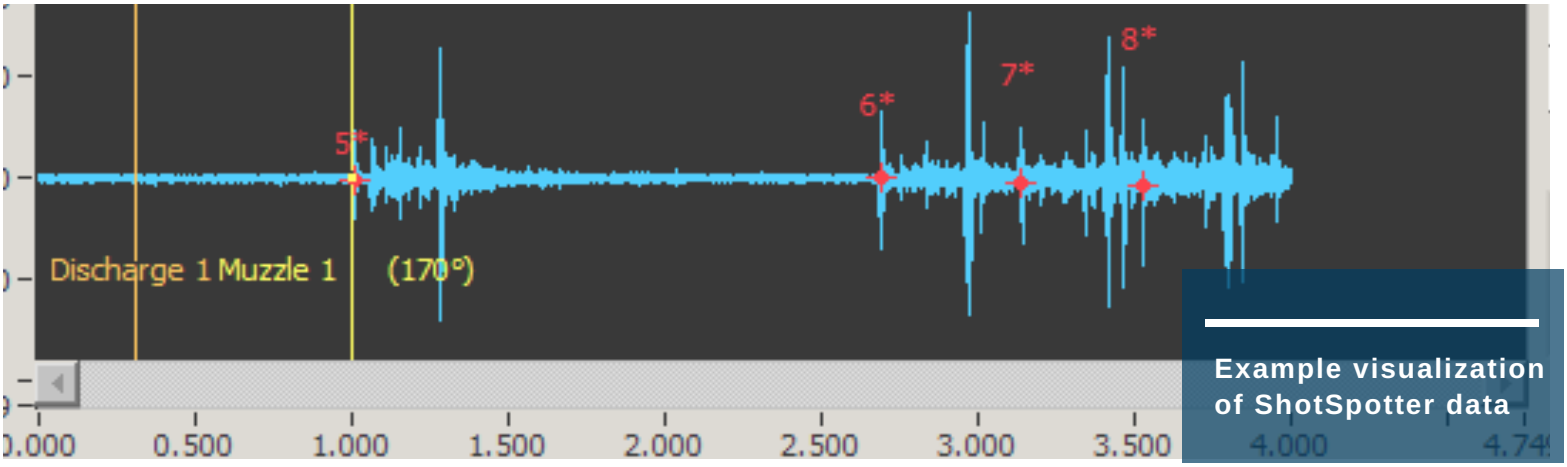
The IRC personnel's individualized review of each notification includes three components related to the captured audio:

1). Personnel are provided with the ShotSpotter algorithm's best assessment of the nature of the sound (e.g., "gunshot," "helicopter," "construction," "fireworks"), including a confidence threshold.

6. IRC personnel work in eight-hour shifts, with two to six specialists and one supervisor per shift. These personnel receive substantial training and testing in this role, though a review of this training or of accuracy rates was outside of the scope of our privacy assessment.

2). Personnel listen to brief audio snippets of the incident from each of the nearby sensors. Snippets include up to one second of audio prior to the incident, the gunshot incident itself, and one second of audio after the incident. The pre- and post-incident audio is provided to help reviewers better assess the nature of the incident itself by giving them a sense of the ambient noise immediately prior to and after the incident. This is the only audio IRC personnel are provided. These audio snippets are retained indefinitely by SST.

3). Personnel also are presented with a visualization of the audio from each of the nearby sensors. The following is a sample visualization, which SST personnel are trained to read:



Example visualization of ShotSpotter data

Based on this acoustic information, as well as other related data (e.g., time of day, location), the IRC reviewer makes a determination as to whether the acoustic event was a gunshot.

If the reviewer finds it was a gunshot, the reviewer sends an alert, including location information and a single audio snippet, to the relevant law enforcement agency via a password-protected application on a mobile phone, in-car laptop, or computer. In addition to the audio snippets, SST provides ShotSpotter customers with detailed information about the location, sequence, and timing of each shot during an incident. According to SST, the typical time from gunshot to alert is less than one minute.

This is the ordinary process in the vast majority of cases. On occasion, however, law enforcement customers contact ShotSpotter about a possible missed gunshot. In such cases, ShotSpotter asks customers to provide their best information about date/time/location of the incident, as well as some proof that the incident occurred (e.g., casings, eyewitness statements).[7]

With this information in hand, a limited number of authorized employees, either IRC personnel or forensic engineers, begin a review of stored audio from nearby sensors, to determine if any of the sensors detected the gunshot. SST personnel cannot listen to sensor audio in real time. Instead, IRC personnel must begin by reviewing graphic

7. An "ear"-witness—someone who claims they heard a gunshot—is not sufficient to trigger this review process.

visualizations of the audio (similar to those pictured above), not by listening to the audio itself. They focus on impulsive events at the relevant location, at the relevant time, and if they locate one, select that portion of the audio to download and listen to. Downloaded audio recordings in these cases have up to two seconds of audio prior to the incident, the incident itself, and up to four seconds after the incident. The pre- and post-incident audio is again provided for a baseline ambient noise level so as to better assess the incident. By listening to the audio from multiple sensors, reviewers can determine whether a gunshot was detected. If so, that snippet is sent to the law enforcement agency.

A sensor is only accessed in the event that SST is presented with evidence of a missed gunshot and only saved in the event that a missed or mislocated gunshot is detected.

In order to make this review process possible, each sensor locally stores 72 hours of audio. Sensors constantly overwrite stored audio and replaced it with more recent audio. Therefore, in order to review for a missed gunshot, law enforcement must provide SST with notice of the possible missed gunshot within 72 hours.

Other than the snippets, discussed above, which are stored indefinitely, audio stored on a sensor is only accessed in the event that SST is presented with evidence of a missed gunshot and only saved in the event that a missed or mislocated gunshot is detected.[8]

Although ShotSpotter acoustic sensors can be integrated into other technologies (such as smart lamp posts), no matter what the physical configuration, only SST personnel have access to ShotSpotter sensors and their stored audio.

8. The only other audio that SST retains are limited samples (such as samples of wind or other noise) for research and development purposes—specifically, to train its algorithm to perform more accurately.

IV. OVERALL PRIVACY ASSESSMENT

SST describes ShotSpotter as a gunshot detection, location, and forensic analysis technology. But some have raised the concern that ShotSpotter might be used as a voice surveillance tool—that is, that it could be used to listen to and record conversations occurring near ShotSpotter sensors. In particular, communities that have been disproportionately impacted by policing, which are most often communities of color, have expressed concern that ShotSpotter might enter a city under the auspices of gunshot detection, but be utilized for targeted voice surveillance in neighborhoods already stricken by gun violence.[9] This concern has been bolstered by a handful of occasions in the past that human voice has been captured by sensors and used in a criminal prosecution.[10]

We wholly agree that from a privacy perspective, it would be of serious concern if ShotSpotter were used for voice surveillance. Voice surveillance could take two forms—persistent surveillance and targeted surveillance. The former might occur if sensors constantly were recording (and SST was listening to and/or retaining) voice audio and sharing such audio with law enforcement for any purpose. Surveillance also could be "targeted," *i.e.*, listening in to specific locations or after-the-fact review of sensor audio in search of relevant voice recordings.

Having conducted a thorough review of SST's policies and procedures, we conclude that the risk of voice surveillance is extremely low in practice. This conclusion is not meant to minimize or dismiss the concerns that others have raised to date. Indeed, it is surely possible that ShotSpotter sensors will, on occasions, capture some intelligible voice audio related to a gunfire incident. Still, based on our understanding of how ShotSpotter operates today, we have little concern that the system will be used for anything approaching voice surveillance.

We reach this conclusion based on our assessment of the variety of safeguards already built in to how ShotSpotter operates, as well as the recommendations SST has agreed to implement at our behest (discussed below). Of particular

9. See, *e.g.*, Lyndsay Winkley, *San Diego police to continue using gunshot detection, despite some criticism*, THE SAN DIEGO UNION TRIBUNE (Oct. 7, 2017), https://www.sandiegouniontribune.com/news/public-safety/sd-me-sdpd-shotspotter-20171005-story.html; Josh Sanburn, *Shots Fired*, TIME (Sept. 21, 2017), https://time.com/4951192/shots-fired-shotspotter; Means Coleman, R. & Brunton, D., *You Might Not Know Her, But You Know Her Brother: Surveillance Technology, Respectability Policing, and the Murder of Janese Talton Jackson*. 18 SOULS: A CRITICAL J. OF BLACK POLITICS, CULTURE, & SOC. 408-20 (Dec. 2016), https://www.academia.edu/31517733/Souls_A_Critical_Journal_of_Black_Politics_Culture_and_Society_You_might_not_know_her_but_you_know_her_brother_Surveillance_Technology_Respectability_Policing_and_the_Murder_of_Janese_Talton_Jackson

10. See, *e.g.*, Alexandra S. Gecas, *Gunfire Game Changer or Big Brother's Hidden Ears?: Fourth Amendment and Admissibility Quandaries Relating to Shotspotter Technology*, 2016 UNIV. ILL. L. REV. 1073, 1088 ("ShotSpotter acknowledged three extremely rare 'edge cases' out of three million detected incidents in the last decade where the sensors recorded people shouting in a public street at the location where the sensors detected gunfire." (internal quotation marks omitted)), https://illinoislawreview.org/wp-content/uploads/2016/07/Gecas.pdf.

importance to our conclusion is the fact that although sensors constantly are "listening," audio is only temporarily stored (formerly 72 hours; soon to be 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 SST's systems.

Moreover, we view as essential the fact that the audio review and retention process is centralized within SST—that is, that neither law enforcement customers nor third parties have access to the raw audio or can determine what audio to download and retain. (Our recommendations address requests and subpoenas for audio.) It should be noted that prior to 2012, police agencies were in control of the audio review and download process locally, but a technology and business model change resulted in SST having centralized control over its sensors and audio through its IRC. Currently, no police department has control over any audio except the snippets provided by SST as part of its alerts.

We do note, however, that although no third parties have access to ShotSpotter stored audio, and ShotSpotter's review and analysis is centralized, ShotSpotter alerts can trigger a range of responses by law enforcement—from dispatching police officers to the location, to programming CCTV cameras to turn toward the direction of an alert, to factoring into predictive policing software, to reinforcing stereotypes regarding particular neighborhoods. We fully appreciate that the mere fact of additional police response—be it in person or CCTV cameras—is itself a concern to some communities. But this is not unique to ShotSpotter; indeed, this can be the case for citizen-initiated reports of gunshots. The range of possible police responses to ShotSpotter alerts highlights how every technology, no matter how privacy protective, must also be used in ways that are racially just, transparent, and subject to democratic approval.

V. PERSONAL PRIVACY ENHANCING RECOMMENDATIONS

Although we perceive that ShotSpotter, under current operating procedures, presents a low privacy risk, we nonetheless have a variety of recommendations designed to further minimize the risk that ShotSpotter might inadvertently or deliberately be used for voice surveillance. We provided these recommendations to SST in advance of this report and have incorporated SST's responses below. As evident from these responses, SST has adopted all of our recommendations, with only slight modifications or qualifications based on how ShotSpotter functions.

01 Substantially reduce the length of audio stored on each sensor.

At present, in order to allow IRC personnel to search for possible missed gunshots, ShotSpotter sensors locally store 72 hours of recent audio, after which the audio is permanently deleted. As explained above, law enforcement customers can report possible missed shots to SST so long as they have evidence that shots were fired. With a rough location and time, IRC personnel or forensic engineers follow the process described previously to first review graphic visualizations of the audio to determine whether any sensors captured a possible gunshot. If so, audio is downloaded, and if it is determined to be a gunshot, an audio snippet is transmitted to law enforcement.

This review process somewhat increases the possibility that human voice will be captured and reviewed because: (1) the process is initiated by law enforcement, and some might be concerned those agencies are interested in obtaining sensor audio for the purpose of voice surveillance; and (2) IRC reviewers or forensic engineers must manually select and listen to additional audio to determine if there was an undetected gunshot. Arguably then, if SST were to completely eliminate all stored audio, the chance of voice surveillance would be substantially limited. But taking this dramatic step also would deprive SST and its customers of the ability to look back for missed gunshots.

We are informed that the IRC processes approximately three to four "missed or mislocated gunshot" requests per day. Balancing this valuable service against the limited possibility of voice surveillance generally, we do not recommend SST take the dramatic step of eliminating stored audio entirely. Instead, we recommend SST drastically cut back the duration of stored audio. Put another way: SST should delete stored audio in a much shorter time frame than 72 hours.

Our understanding from SST is that most missed gunshots are reported by law enforcement customers within 30 hours. As such, SST can accomplish its goal of searching for missed gunshots while reducing the period of stored audio from 72 hours to 30 hours.

By reducing the length of time that SST stores audio, SST will lower the possibility that its technology can be seen as a surveillance device, or that law enforcement even will attempt to use the sensor buffer for investigative purposes other than missed gunshots.

SST has adopted this recommendation and has implemented a software update that is currently being pushed out to all of its sensors across the country. This rollout will be complete by early August 2019. Customers have already been informed of this change in policy.

02 Do not share precise sensor locations with law enforcement.

SST works with law enforcement to set ShotSpotter's coverage area. Once the area is set, SST engineers alone determine precise sensor locations necessary in order to ensure even coverage. SST does not provide law enforcement with access to a database or list of precise sensor locations, nor does SST respond to requests for sensor locations from police or the public. SST says it fights subpoenas for requests to have the precise sensor locations. As a general matter, law enforcement has no need to know the precise sensor locations.[11]

We recommend formalizing the practice that law enforcement customers not be given precise sensor locations in SST company policy. By withholding this information, SST minimizes the possibility (or the allure) that law enforcement officers investigating a particular incident would view ShotSpotter sensors as an investigative tool like CCTV and request audio from a sensor.

SST has adopted this recommendation and now clearly states, in both public and client-facing documents, that law enforcement will not have access to precise sensor locations, requests for sensor locations will not be honored, and subpoenas will be resisted in court.

03 Deny requests and challenge subpoenas for additional audio.

No matter what internal controls SST places on its technology, and no matter the internal emphasis on privacy and avoiding voice surveillance, there always will remain the possibility that third parties—police, prosecutors, civil litigants, etc.—may request or subpoena extended sensor audio beyond the short snippets provided upon a detected gunshot in an effort to capture voice. No matter how uncommon an occurrence, we believe it prudent to be alert to and prepared for this possibility.

Although a corporate policy to deny requests and challenge legal subpoenas will not necessarily be decisive in court, it should weigh heavily against parties making any such request.

SST has adopted this recommendation in both public and client-facing documents, that requests for extended audio will not be honored and subpoenas will be resisted in court.

11. We understand that on occasion a police officer (generally a patrol officer) will accompany SST personnel when SST asks for consent to place a sensor. The officer does not accompany personnel during installation. Although this provides a lone officer with knowledge of the general area of a few sensors, this is not the type of systematic knowledge that concerns us.

04 Minimize the duration of audio snippets.

Prior to this privacy assessment, in cases of a law enforcement agency requesting research on a possible missed or mislocated gunshot, SST policy was to provide law enforcement personnel with an audio snippet of up to two seconds of audio from immediately before the gunshot, the audio of the gunshot itself, and up to four seconds of audio from immediately after incident. For live-captured incidents, however, SST provided only one second before and one second after.

In the few past instances in which human voice was captured incidentally by ShotSpotter sensors, that voice audio was captured as part of the gunshot audio snippet. In order to minimize the chance of incidentally capturing and transmitting voice audio to law enforcement, we recommend standardizing and minimizing the duration of audio from before and after the gunshot. Specifically, we suggest SST provide at most one second of audio from before and after any incident.

SST has adopted this recommendation and has now implemented an automated process where all snippets include only one second of pre- and post-incident audio.

05 Strictly limit which SST personnel have access to sensor audio.

Despite efforts to mitigate privacy concerns by avoiding certain locations for sensors and placing them high off the ground, the possibility will always remain that ShotSpotter sensors will capture voice audio. As such, access to the sensors must be sharply controlled. In addition to ensuring that sensors and the SST cloud are adequately encrypted and protected against external attack, SST must take steps to fortify its internal operations.[12] Our first recommendation on this front is that SST conduct an internal review of which personnel have access to sensor audio and ensure that access is limited only to those personnel who actually need access to perform their work.

SST has adopted this recommendation and has already completed its review of personnel with access to sensor audio. As a result of this review, SST has limited or eliminated audio access for several positions (including SST executives) whose access to audio was not essential.

06 Require supervisor approval for any audio download longer than one minute.

In our view, the greatest risk for invasion of personal privacy comes when SST personnel access actual stored sensor audio (as opposed to the audio visualizations typically used to locate gunshot-like events). Although we have no reason to believe that SST personnel abuse this privilege, in order to deter and detect possible misuse, we recommend SST implement a safeguard that requires supervisor approval before an SST employee is permitted to download extended audio. In order to strike a balance between allowing SST personnel to search

12. It is also key, as noted above, that third parties (customers or not) never are given access to these sensors.

quickly for missed gunshots, while still installing a layer of protection, we recommend requiring supervisor approval for audio downloads of longer than one minute per incident.

SST has adopted this recommendation.

07 Create a clear audit trail for every audio download.

Further, we recommend that for every instance in which an SST employee accesses stored sensor audio, SST ensure there exists a clear audit trail describing what audio was accessed, the SST employee who accessed the audio, the supervisor who approved the download (under Recommendation No. 6, above), the law enforcement agency and officer who made the request, and the evidentiary basis for the request.

SST has adopted this recommendation.

08 Conduct periodic review of the audio download audit trail.

In addition to creating an audit trail (Recommendation No. 7, above) for when stored sensor audio is accessed, we recommend SST create a regular process by which supervisory personnel review this audit trail. This review should ensure that audio is being accessed only when necessary and according to proper procedures. Such a review also should be on the lookout for any law enforcement agencies that are using the process at a much higher rate, SST personnel who listen to a significantly longer duration of audio than necessary, or other patterns that may require corrective action.

SST has adopted this recommendation.

09 Revise SST's longstanding privacy policy.

In addition to making internal changes to its operations, we recommended SST make changes to a number of its public-facing and client-facing documents, to emphasize that ShotSpotter should only be used for gunshot detection, and not voice surveillance, and to document the steps SST has taken to emphasize privacy protections.

SST has long had a privacy policy.[13] Although that policy addressed many relevant privacy issues, with our privacy assessment, we suggested SST make revisions and updates. In particular, we suggested SST revise the policy for clarity and to focus on privacy protections.

SST has adopted this recommendation. The updated policy is available at: https://www.shotspotter.com/privacy-policy[14]

10 Revise client-facing documents to emphasize privacy protections.

SST provides law enforcement customers with a variety of documents that touch on privacy-related issues, such as Best Practices, Strategies & Recommendations and Model Policy Elements. We think it is important that SST provides this type of

13. For reference, ShotSpotter's previous privacy policy, dated March 31, 2015, is available at https://www.shotspotter.com/apps/privacy/.
14. It is a core tenet of the Policing Project that new policing technologies should be adopted transparently and with public input. Although this is not technically part of our privacy audit, we applaud SST for urging its customers to engage the public in a discussion about the acquisition and use of its products as the first principle of its privacy policy.

support. In fact, we think it irresponsible for technology companies to provide surveillance technologies to law enforcement agencies without a draft use policy. We have suggested that SST revise these documents to emphasize many of the same principles outlined in its new privacy policy—specifically, that its technology cannot be used for voice surveillance, that the sensor audio storage cannot be used to obtain "extended" or "additional" audio but only can be used to search for missed gunshots and that subpoenas for audio will be contested.

SST has adopted this recommendation and has already made these changes.

11 Whenever possible, avoid placing sensors on particularly sensitive locations.

Although ShotSpotter is not especially calibrated to record human voice and SST takes measures to avoid this occurrence—for example, by not using particularly sensitive microphones, placing sensors high above the ground, and ensuring that only gunshot-like sounds trigger an IRC notification—there remains the possibility that voice will be captured by a sensor incidentally. Knowing this, we raised with SST a general concern about the location of sensors. Specifically, we raised whether SST could minimize the impact of incidental voice capture (and also allay public concerns) by avoiding placing sensors in locations that present concerns for the surrounding community based on protected First Amendment characteristics, prior experience with policing, or other social vulnerabilities. For example, our conversations with SST included discussions of public housing campuses, where residents often are already subjected to a great deal of surveillance, and houses of worship, particularly those that have been subject to unlawful government surveillance in the past. Other examples of sensitive locations may include hospitals, healthcare clinics, or schools.

SST explained that an absolute ban on these types of locations simply cannot be implemented without major disruption of ShotSpotter's coverage and performance. For example, SST explained that there are occasions when it must use certain public buildings, including government-owned housing, in order to maintain the consistency of its detection system. In fact, many jurisdictions that choose to use ShotSpotter suffer from gun violence in close proximity to public housing. SST explained that placing sensors quite high, often on rooftops, could mitigate incidental voice capture, but entirely avoiding those structures would severely limit ShotSpotter's utility to these jurisdictions. The best across-the-board commitment SST can make in this context is to instruct its personnel to make reasonable efforts to avoid sensitive locations when less sensitive locations are possible.

Deciding between these trade-offs is a classic example of the value of benefit-cost analysis. Jurisdictions that have decided to utilize ShotSpotter plainly believe in its utility in detecting and alerting law enforcement to gunfire. Given that, and the relatively minimal concerns with privacy that we believe ShotSpotter presents, it makes sense to place sensors where they will be effective. As noted above, ShotSpotter will seek to minimize those locations when possible.

I. DATA SHARING WITH THIRD PARTIES

As discussed above, ShotSpotter generates two categories of data as it operates: First, other than the limited audio used to improve its gunshot detection algorithm,[15] the only audio data SST retains are the short audio snippets of loud "impulsive" sounds detected by three or more sensors. Second, for each detected gunshot, SST retains metadata, including detailed date, time, GPS location, and certain gunfire characteristics (e.g., number of shots). In aggregate, SST maintains the most comprehensive data set of gunfire information in the country.

Under current contractual arrangements, in all but a few cases, SST retains ownership of this data. As a practical matter, this means that in addition to sharing data with its customer, SST has the legal authority to share, license, or sell the data as it pleases. SST's position is that it is within its right to control and share this data because it is a private company using proprietary technology to offer a service to law enforcement. On the other hand, there are those who have expressed concern with this model, insisting that because ShotSpotter is used by law enforcement, its data, like other law enforcement data, should be public.[16] We do not take a position on this debate, but do offer our views about situations in which SST might share ShotSpotter data beyond its local law enforcement customers.

Although not technically a matter of personal privacy and thus somewhat outside the scope of our assessment, we have chosen to comment on this complex issue because we feel it is essential that SST take steps to clarify its third-party data sharing practices. SST has disclosed to us that it shares data with hospitals and researchers. SST has also informed us that, due to contractual arrangements, it cannot share the identity of all other third parties with which it shares such data. We obviously cannot comment on the implications of SST sharing data with unknown entities. Nor can we anticipate all the possible situations where third-party sharing may arise in the future. Knowing this, we have done our best to offer some general guidance on this issue based on our experience:

First, we consider it absolutely bedrock that jurisdictions have access to not only gunfire alerts but also their own aggregate data (*i.e.* data from gunfire alerts aggregated in a manner that easily allows jurisdictions to see how often, when, and where gunfire is occurring). Access to clear, aggregate gunfire data is vital so that the public can make informed public safety decisions. Moreover, realizing that jurisdictions often lack the internal capability to analyze the data in rigorous ways, we believe SST should allow

15. See *supra* note 8.
16 See, e.g., Jason Tashea, *Should the public have access to data police acquire through private companies?*, AMERICAN BAR ASSOCIATION JOURNAL (Dec. 1, 2016). http://www.abajournal.com/magazine/article/public_access_police_data_private_company.

jurisdictions to share their data with outside researchers, so long as the work is in furtherance of local public safety objectives.

At the same time, we understand there may be compelling public safety reasons why SST feels it should hold back certain detailed information. If so, SST should make those reasons clear and public. For example, one could imagine that for privacy and safety reasons law enforcement or victims might not want precise GPS data regarding specific incidents made public. Similarly, there is a plausible concern that certain third parties could make use of precise GPS data in ways that undermine communities (see discussion below regarding insurers). The conclusions SST reaches on this issue should be explained in its written policies, so the merits can be evaluated.

Second, although our understanding is that SST does not currently share audio snippets with any third parties, SST must address if, when, and how it will do so in the future. In addressing this issue, we suggest that sharing audio snippets with third parties should be subject to at least the same safeguards as with law enforcement customers, if not more.[17] Because we see little risk to personal privacy when the snippets are generated to begin with, we see little additional risk when it comes to sharing these snippets. Still, we think impacted communities may rightfully expect more details about SST's audio-sharing practices going forward.

Third, we suggest SST develop and make public its principles on when it will share non-audio data (*e.g.*, gunfire time and location) with third parties. Unlike audio data, which SST does not currently share, SST does share gunfire alert data.

This data can take multiple forms—from sharing alerts in real-time, similar to what law enforcement receives, to sharing only high-level aggregate data. In our view, sharing alerts in real-time raises significantly different concerns than sharing aggregate data, and we urge SST to exercise great caution when considering doing so. We raise this caution for the simple reason that real-time alerts can trigger a variety of real-time responses, over which SST will not have any control (and which we cannot predict). For example, it is one thing, if a hospital uses real-time alerts to deploy ambulances; it is quite another thing if a news agency uses real-time alerts to deploy camera crews. Even sharing alerts with outside law enforcement agencies creates the possibility for additional law enforcement response.

Whether real-time alerts or aggregate data, we believe that SST should address how and whether it will inform jurisdictions that data from their communities is being shared. SST has a range of options here, from asking jurisdictions for consent to share the data to sharing the data without notice. In our view, the degree of transparency that is appropriate depends on the specificity of the data being shared:

17. To be perfectly clear, we view sharing access to raw sensor audio as completely unacceptable (as we would if law enforcement were given such access). SST does not do this, not with customers and not with third parties.

On one end of the spectrum, real-time alerts with full metadata should reasonably involve the same degree of transparency and public engagement as the decision to implement ShotSpotter to begin with. On the other hand, when it comes to including a jurisdiction's information in an aggregate, nation-wide report, we see little need for specific notice.[18]

What's more, the identity of the third party seeking access to SST's data is critically important. In certain communities, for example, any information sharing with U.S. Immigration and Customs Enforcement (ICE) would be a non-starter. In fact, there are those who may view information sharing with any federal law enforcement agency quite differently than sharing with local law enforcement as local communities have much more of a say in crafting local enforcement priorities (*e.g.*, sanctuary policies, decriminalizing low-level offenses) than they do over federal law enforcement.[19]

Sharing with private parties is equally complex. For example, there are those third parties whose efforts are aimed at strengthening communities such as through improved public health and public safety (*e.g.*, hospitals). Sharing with these third parties is unlikely to cause concern. Moreover, we cannot understate the importance of providing researchers with quality data. There remains a tremendous knowledge gap in the public safety sphere.[20] At the same time, we think SST should avoid sharing data with third parties who likely would use the data to target or undermine the very communities that SST's technology avers to benefit. By way of example, we can imagine insurance companies using gunshot data as some have used race—as a proxy for actuarial risk and charging minority communities higher insurance rates or even denying coverage.[21]

These are complicated issues and we do not claim to have all the answers. In truth, the answers may vary from community to community. But just as SST has taken the burden upon itself to implement and make public its robust personal-privacy practices, we fully expect it will do the same when it comes to data sharing.

18. One example of this type of high-level reporting is the aggregate data SST includes in its National Gunfire Index. See ShotSpotter Inc., 2017 National Gunfire Index, https://www.shotspotter.com/2017NGI/.
19. We refer here to federal law enforcement agencies, not federal research institutions. One could imagine, for example, a time in the future when the Center for Disease Control might once again be permitted to conduct research into gun violence, and might find SST's data useful.
20. See, e.g., Barry Friedman & Kate Mather, Policing, *U.S. Style: With Little Idea of What Really Works*, JUST SECURITY (July 10, 2019), https://www.justsecurity.org/64865/policing-u-s-style-with-little-idea-of-what-really-works/. Although SST may want to vet the credentials of researchers who want SST's data to ensure their work is generally of high quality, we believe the country would greatly benefit from rigorous social science research that utilizes SST's gunfire data.
21. See, e.g., Julia Angwin, et al., *Minority Neighborhoods Pay Higher Car Insurance Premiums Than White Areas With the Same Risk*, PROPUBLICA (April 5, 2017), https://www.propublica.org/article/minority-neighborhoods-higher-car-insurance-premiums-white-areas-same-risk.

VII. CONCLUSION

ShotSpotter gunshot detection technology offers law enforcement a tool to improve their response to gun violence, including responding to gun-fire incidents that previously went unreported. But nearly every public safety tool comes with privacy and civil liberties tradeoffs. It is incumbent on law enforcement and the communities they serve to understand these tradeoffs before acquiring any new technology.

It is both inappropriate and unfair to place the entire burden of developing costs and benefits on the public. It is essential that technology providers both make these tradeoffs clear (by transparently explaining how their products operate) and by taking meaningful steps to improve their technology's design and operation to maximize public safety benefits while minimizing intrusions on civil liberties. We hope that this report helps accomplish both of those goals regarding ShotSpotter.

In response to this report, SST has undertaken significant internal efforts to implement our recommendations and make ShotSpotter more privacy protective. These changes were not costless, and in some cases significantly impacted the technology's operation. Still, SST made a conscious decision to embrace this tradeoff. Other policing technology companies should follow SST's leadership and proactively embrace their responsibility in protecting individual liberty.

Other policing technology companies should follow SST's leadership and proactively embrace their responsibility in protecting individual liberty.

VIII. MORE ABOUT THE POLICING PROJECT

The Policing Project at New York University's School of Law is an independent nonprofit research and public policy organization focused on ensuring just and effective policing through democratic accountability. The Policing Project works across a host of issues—from use of force and racial profiling, to facial recognition, to reimagining public safety—in close collaboration with stakeholders who typically find themselves at odds. We bring a new approach to these fraught areas—one grounded in democratic values and designed to promote transparency, racial justice, and equitable treatment for all.

Our work is focused on policing "accountability," but also on changing what people mean when they demand accountability. When people unhappy with policing talk about a lack of "accountability," they typically mean that when an officer harms someone, or surveillance techniques are deployed inappropriately, no one is held responsible—officers are rarely disciplined or criminally prosecuted, courts admit evidence the police have seized illegally, and civil lawsuits are not successful. This is back-end accountability. It kicks in only after something has gone wrong, or is perceived to have gone wrong. Back-end accountability is important, but it can only target misconduct. As such, there is a limit to what it can accomplish to guide policing before it goes awry.

Our work focuses on ensuring accountability and democratic participation on the front end. Front-end or democratic accountability involves promoting public voice in setting transparent, ethical, and effective policing policies and practices *before* the police or government act. The goal is achieving public safety in a manner that is equitable, non-discriminatory, and respectful of public values. This is how we think of accountability in most of government, yet this is all too rare in policing. We are working to change that.

Today, the Policing Project partners with civic leaders, law enforcement agencies, grassroots community organizations, and advocacy groups across the country to promote public safety through transparency, equity, and democratic engagement. Our work is carried out through demonstration projects, researching and evaluating existing oversight models, engaging in public advocacy, convening conferences and roundtables with academics and law enforcement personnel, and engaging in targeted litigation around policing issues.

Learn more about us at **www.PolicingProject.org**.


Policing
Project
NYU School of Law