CITY OF OAKLAND

Privacy Advisory Commission

October 3, 2019 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor

Regular Meeting Agenda

Commission Members: ***District 1 Representative***: *Reem Suleiman,* ***District 2 Representative***: *Chloe Brown,* ***District 3 Representative***: *Brian M. Hofer,* ***District 4 Representative***: *Lou Katz,* ***District 5 Representative***: *Raymundo Jacquez III,* ***District 6 Representative***: *Gina Tomlinson,* ***District 7 Representative***: *Robert Oliver,* ***Council At-Large Representative***: *Henry Gage III,* ***Mayoral Representative***: *Heather Patterson*

Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.

1. Call to Order, determination of quorum

2. Open Forum/Public Comment

3. Review and approval of the draft September 5 meeting minutes

4. Surveillance Equipment Ordinance – OPD – ShotSpotter Impact Report and proposed Use Policy – review and take possible action

5. Adjournment at 7:00pm

CITY OF OAKLAND

Privacy Advisory Commission

September 5, 2019 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor

Regular Meeting Agenda

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian M. Hofer, **District 4 Representative**: Lou Katz, **District 5 Representative**: Raymundo Jacquez III, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Henry Gage III, **Mayoral Representative**: Heather Patterson*

Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.

1. Call to Order, determination of quorum

Quorum was met with following in attendance: Members Hofer, Suleiman, Katz, Jacquez, Tomlinson, Gage, and Patterson.

2. Open Forum/Public Comment

There were no Open Forum Speakers.

3. Review and approval of the draft August 1 meeting minutes

The minutes were approved unanimously.

4. Port of Oakland presentation – GoPort Program – Freight Intelligent Transportation System (FITS)

Representative from the Port provided a PowerPoint presentation on the GoPort Program which is designed to improve traffic flows around the Port which will help avoid costly delays, improve the air quality by reducing emissions, and reduce the problem of trucks waiting in West Oakland neighborhoods to gain access to the Port. The project includes gathering data on trucks accessing the Port and transmitting it to the Port's Emergency Operations Center (not the City's) and also allows for the transfer *of information to Caltrans and the City when there has been an accident or incident that may require a City or Caltrans response.*

Commissions had questions about what data is collected and shared and whether any surveillance or sensors will be used outside of the Port. The GoPort system is only at the Port and the only data transferred outside the Port would come in the form of the alerts mentioned above—no Personally Identifiable Information would be sent to the City or Caltrans.

This was an informational report so no action was taken.

5. Surveillance Equipment Ordinance – OPD – StarChase GPS Impact Report and proposed Use Policy – review and take possible action

Deputy Chief Holmgren presented the modified Use Policy and Impact Statement Based on his ad hoc meeting with PAC Members since the last meeting.

There was one public speaker: J.P. Masser raised concern about how the technology would be deployed during a high-speed chase, citing traffic safety (not privacy) concerns.

The PAC voted unanimously to forward the Policy to the City Council with full support.

6. Federal Task Force Transparency Ordinance – OPD – FBI's Joint Terrorism Task Force MOU – review and take possible action

Bruce Stoffmacher presented the draft MOU and DC Holmgren provide input to the questions raised by the PAC. The PAC asked that certain modifications be made, among them: Ensure the MOU aligns with the Draft resolution, ask for the removal of Asset Forfeiture language, add a definition of terrorism, add better language on participation protocols, and better delineate who has oversight over whom.

There were four public speakers who raised many of the same issues.

An ad hoc committee was set up to meet with OPD staff and the item was continued to October.

7. Surveillance Equipment Ordinance – OPD – Remote Camera Impact Report and proposed Use Policy – review and take possible action.

Captain Wingate presented to the PAC and explained OPD's evolving tactics in addressing large gatherings/protests and how remote Cameras can aid in that process. He noted that it's better to have one officer with a camera that provides situational awareness to a commander, with other officers on standby at a different location than to have 25 officers on a skirmish line or following a march. Cameras allow that flexibility to avoid a large officer presence escalating feelings within a crowd that they are being overpoliced. He raised concern about only being able to use a "Reasonable Suspicion" standard to use this technology and asked the PAC to offer an alternative standard to embrace situations such as explained above.
The item was tabled until October.

DEPARTMENTAL GENERAL ORDER

I-20: GUNSHOT LOCATION DETECTION SYSTEM

Effective Date: XX Apr 19

Coordinator: Ceasefire Division

The Oakland Police Department (OPD) strives to use technology that promotes accountability and transparency. This policy provides guidance and procedure for response, immediate actions, follow up, documentation, and auditing of OPD's Gunshot Location Detection (GLD) System incidents that occur within the City of Oakland.

All data, whether sound, image, or video data, generated by OPD's GLD System are for the official use of this department. Because such data may contain confidential information, such data is not open to public review.

A. Description of the Technology

Commented [BS1]: Purpose is covered here

OPD uses a GLD System (currently the ShotSpotter® Flex™ system, provided by ShotSpotter, Inc. "Shotspotter") to record gunshot sounds and use sensors to locate the origin of the gunshots. The GLD system enables OPD to be aware of gunshots in the absence of witnesses and/or reports of gunshots to OPD's Communications Division (Communications). The GLD system notifies Communications of verified gunshot events, which allows OPD to quickly respond to gunshots and related violent criminal activity.

A – 1. How Shotspotter Works

OPD's GLD system employs acoustic sensors strategically placed in specified areas (commonly referred to as a "coverage area.") When a gun is fired, the sensors detect the firing of the weapon. The audio triangulation of multiple installed sensors then pinpoints a gunfire location and sends the audio file and triangulation information to Shotspotter Headquarters (HQ) for gunshot verification. Verified gunshots and related information are then sent to Communications in real-time so that Communications may notify responding officers where guns were fired.

A – 2. The GLD System

There are three components to GLD system:

1. GLD Sensors: Sensors are installed in different coverage areas in Oakland. Oakland currently has five coverage areas (or phases) where sensors are installed to triangulate gunshots.

2. ShotSpotter Headquarters (HQ): Sensors send acoustic information to HQ where computer-based machine-learning algorithms are used to analyze the sound. If the sound and visual audio signature match gunfire, the incident file is then passed along to the Incident Review Center (IRC). Acoustic experts at the IRC review incidents within seconds and provide additional information (e.g. number of gunshots, number of guns, types of guns). Confirmed gunshots are pushed out to Communications (dispatch) as well as to the OPD Shotspotter software system within seconds.
3. The OPD Shotspotter Software System: This system is cloud-based and desktop-based; OPD authorized personnel can use internet browsers to connect to the Shotspotter system via OPD computers. Certain authorized personnel use desktop applications that connect to the Shotspotter system for more in-depth gunshot analysis.

B. General Guidelines

B – 1. Authorized Use

Commented [BS2]: Authorized Use covered here

The Chief of Police or designee shall provide necessary training and/or technical assistance for GLD usage. Only OPD personnel shall be granted access to OPD's GLD System. The GLD system shall only be used for locating gunshots. The system shall never be used to record human conversations except where such conversations are unintentionally recorded in connection with gunshot recordings.

B – 2. Restrictions on Use

Department members shall not use or allow others to use the GLDS acoustical recording equipment, software or data for any unauthorized purpose.

B-3. Data Access

Commented [BS3]: Data Access: The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;

1. Authorized personnel may access the GLD system via vehicle computers and receive notifications of verified GLD activations. OPD Communications may also notify authorized personnel of GLD activations. Authorized personnel may respond to such notifications based upon priorities as mandated by their supervisors.
2. The GLD system shall only be used for official law enforcement purposes.
3. Only specifically authorized personnel authorized by the Chief or Chief-designee (e.g. personnel with OPD's Ceasefire Unit and CID crime analysts) will have access to historical GLD system data via desktop GLD system applications.

   The GLD system may be used for authorized patrol and investigation purposes. Contacting individuals at locations where GLD activations occur shall be conducted in accordance with applicable law and policy.

4. Accessing data collected by the GLD system (currently Shotspotter) requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation or assignment to a unit which responds to gunshot calls (e.g. Patrol Division).

5. Members approved to access GLD system data may only use data for legitimate law enforcement purposes only, such as when the data relate to gunshots, a specific criminal investigation or department-related civil or administrative action.

6. All verified GLD system activations are entered into OPD's computer-aided dispatch (CAD) record management system (RMS) with GLD system-specific ID numbers. Authorized personnel can then query the CAD/RMS system for any and all GLD system activations.

C. Shotspotter Data

Commented [BS4]: Data Collection is covered here

C – 1. Data Collection and Retention

Commented [RH5]: From the Ordinance- Data Collection: the information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data;
[this info is missing]

Commented [BS6R5]: So data retention is covered here.

1. GLD acoustic data is recorded when three sensors all record sounds that match the acoustic signatures of gunshots. The sensors are constantly recording a total of 30 hours into acoustical digital .wav format files, and then deleting the data unless triggered to send the data to Shotspotter for analysis; the buffer allows OPD to request data within 24 hours.
2. The sensors delete all acoustic data after 30 hours unless the gunshot-like impulsive acoustic event sends the data to Shotspotter for analysis. Only verified gunshot data is maintained in perpetuity, both by Shotspotter HQ as well as on OPD desktop applications.

Commented [BS7]: "Maintenance" addressed here

C – 2. Data Security

Commented [RH8]: This should be titled "Data Protection." From the Ordinance- Data Protection: the safeguards that protect information from unauthorized access, including encryption and access control mechanisms;

Commented [BS9R8]: I think we need to address "data protection" as covered in the ordinance but we do not need to use that as a headline.

All data will be closely safeguarded and protected by both procedural and technological means:

1. Authorized personnel may access the browser-based GLD system via vehicle computers to only access the cloud-based system. Authorized personnel must always gain access through a login/password-protected system which records all login access.
2. OPD has no direct access to actual GLD (Shotspotter) sensors. Only

Shotspotter-specified support engineers can use a technology to access the data in the sensors prior to the 30-hour deletion period, if CID investigators need to search for previous gunshots.

Commented [RH10]: Similar to comment above – this needs to be moved to Data Access.

Commented [BS11R10]: Anything else to say about security?

C – 3. Releasing or Sharing GLD System Data

GLD system data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

Commented [RH12]: Need to include "need to know/right to know."

Commented [BS13R12]: I think this is addressed in #1 below

1. The agency makes a written request for the Shotspotter data that includes:

   a. The name of the requesting agency.
   b. The name of the individual making the request.
   c. The intended purpose of obtaining the information.

2. The request is reviewed by the Bureau of Services Deputy Chief/ Deputy Director or designee and approved before the request is fulfilled.

3. The approved request is retained on file.

Requests for Shotspotter data by non-law enforcement or non-prosecutorial agencies will be processed as provided in Departmental General Order M-09.1, Public Records Access (Civil Code § 1798.90.55) and per any interagency agreements.

Commented [BS14]: Public Access is covered here

D. GLD System Administration

OPD's GLD System is installed and maintained by Shotspotter in collaboration with OPD. Oversight of the system as well as data retention and access, shall be managed by OPD's Ceasefire Division. The sensors as well as the system are maintained by Shotspotter.

D – 1. GLD System Coordinator

The title of the official custodian of the GLD System (Shotspotter Coordinator) is the Captain of the OPD Ceasefire Division, or designee.

D – 2. GLD System Administrator

The Ceasefire Captain shall administer the GLD system, implementation and use, in collaboration with OPD's Criminal Investigations Division (CID). The Ceasefire Captain, or designee, shall be responsible for developing guideline, procedures, and processes for the proper collection, accuracy and retention of GLD System data.

D – 3. Monitoring and Reporting

The Oakland Police Department will monitor its use of the GLD system to ensure the accuracy of the information collected and compliance with all applicable laws, including laws providing for process, and time period system audits.

The Shotspotter Coordinator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report for the previous 12-month period. These reporting procedures will assist in evaluating the efficacy of this policy and equipment.

D – 4. Training

The Training Section shall ensure that members receive department-approved training for those authorized to use or access the Shotspotter system.

Trainings for Communications personnel (dispatchers and operators) may include training on how to acknowledge the GLD system activations and how to use the system software to identify activation locations so as to provide information to responding officers.

By Order of

Anne E. Kirkpatrick

Chief of Police Date Signed:

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.

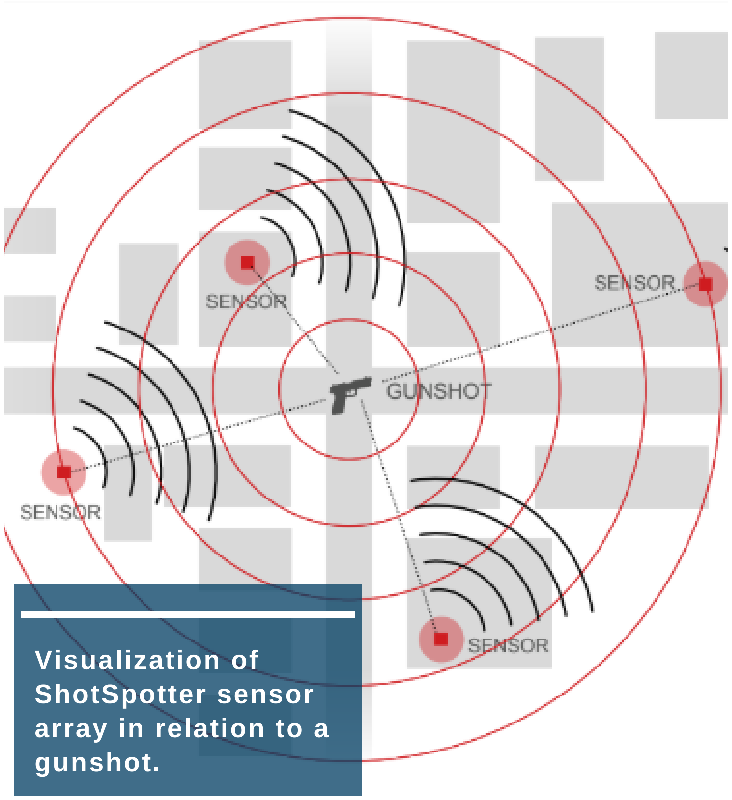
We have had complete control over the substance of our recommendations and the contents of this report. SST has reviewed it for factual errors only.

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.

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

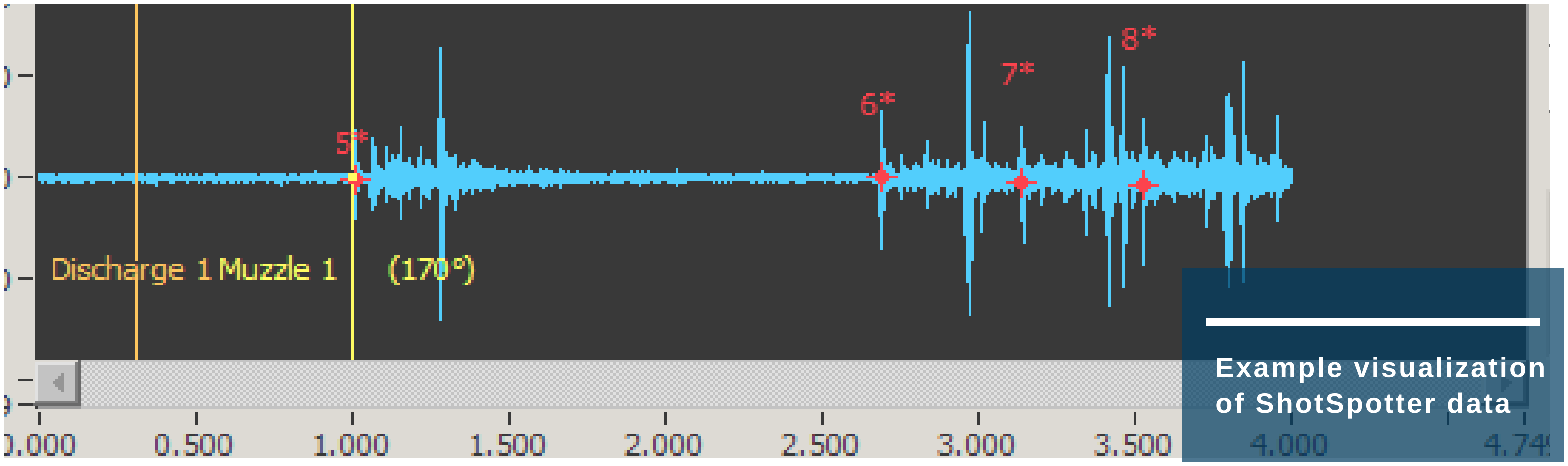
The IRC personnel's individualized review of each notification includes three components related to the captured audio:

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

OAKLAND POLICE DEPARTMENT

Surveillance Impact Use Report for the Gunshot Location Detection System

1. Information Describing the Gunshot Location Detection (GLD) System and How It Works

The Oakland Police Department (OPD)'s GLD system employs a network of acoustic sensors which are placed in historically high gun crime areas to provide to OPD alerts containing the location of gunshots as they occur. Currently, OPD contracts with ShotSpotter, Inc., the creator of the ShotSpotter® Flex™ system "ShotSpotter." ShotSpotter is the most widely used outdoor gunshot system in the United States with over 100 installations.

The GLD system sensors are designed to detect gunshots based on their acoustic signature (e.g. broad-frequency, impulsiveness and loudness). The utilization of multiple sensors at different distances from a gunshot sound allows the system not only to capture the sound but assign a probability that it is a gunshot and triangulate its precise location based on time difference of arrival. If the machine classifier in the "ShotSpotter Cloud" determines it is likely a gunshot based on computer-learning algorithms, the system will pull a short audio snippet from the sensors that detected it and send it to human analysts at the ShotSpotter Incident Review Center at its headquarters in Newark, CA. The analysts perform an auditory and visual assessment of the audio waveform to make a final determination as part of a two-phased classification process. If confirmed as a gunshot, an alert is published containing information such as street address, number of rounds fired, and a short audio snippet of the gunfire event– all within 60 seconds of the trigger pull (29 seconds on average).

OPD Communications Division and police vehicle terminals receive the alerts so that Communications may notify responding personnel (and personnel can use vehicle computers) of where gunshots were recently fired to generate a fast police response. The GLD System also consists of a cloud-based portal accessible to patrol vehicles, OPD computers and authorized phones via a secure mobile application.

Officers or other authorized personnel can receive real-time gunshot notification when logged into the system in addition to receiving notification from OPD Communications. Authorized personnel such as crime analysts and investigators use a desktop application that connects to the ShotSpotter system for more in-depth gunshot pattern analysis.

The ShotSpotter service also includes the option to receive Detailed Forensic Reports (DFR) which are court-admissible documents that show the exact timing, location and sequence of shots fired. This service is primarily used by the county District Attorney office as evidence in prosecution of gun crime defendants. The company provides expert witness testimonial to support the DFR in court upon request. DFR reports have been utilized by Oakland PD and Alameda County DA more than 100 times since 2012.

2. Proposed Purpose

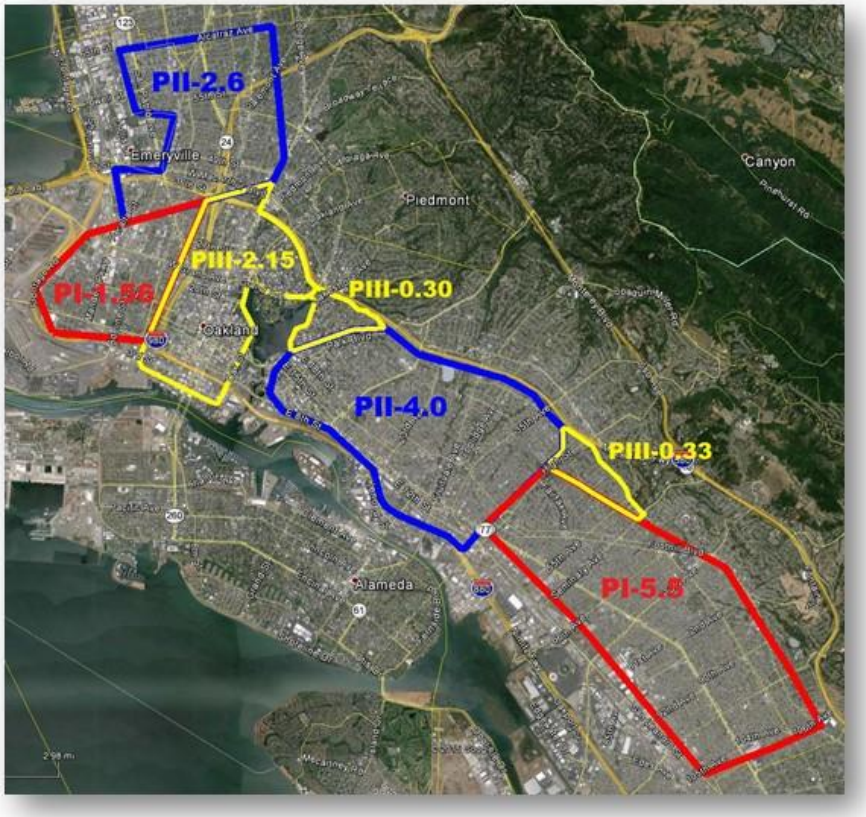
Hundreds of gunshots occur each month in Oakland; in September 2018 alone the system logged 395 total incidents (275 multiple gunshots, 92 single gunshots, and 28 possible gunshots). Police rely on the community to report gunshot incidents via 911. However, on average 80% of gunshot incidents in the United States go unreported resulting in police being unaware of most gun violence. In Oakland, only 5% of gunshot incidents were reported via 911[1] based on May 2019 analysis of verified gunshot notifications and 911 calls.

The purpose of GLD is to enable OPD to provide a higher level of the service to the community related to shootings. The system detects, locates and alerts officers of virtually all gunshots in a coverage area in less than 60 seconds enabling officers to respond to and investigate gunshots incidents they would not have known about and to respond to them much more rapidly than waiting for a 911 call. Personnel can better respond to gunshot activity and respond to possible armed individuals as well as to possible gunshot victims through this important real-time data.

3. Locations Where, and Situations in which GLD System may be deployed or utilized.

OPD has contracted with ShotSpotter to install GLD sensors in different areas in several parts of the City. The total coverage area for the current ShotSpotter system comprises over 16 square miles or approximately 27 percent of the City. OPD has chosen to install the sensors in areas most prone to gunshots based upon historical crime data. Many areas in East and West Oakland now benefit from the GLD system – the map below outlines the three phases or areas of ShotSpotter coverage in Oakland.

[1] based on May 2019 analysis of verified gunshot notifications and 911 calls.



After receiving OPD training authorized personnel are able to access the GLD system. The following table presents Part 1 Crime Data for January 1-May 31 Year to Date (YTD).

Part 1 Crimes	YTD 2015	YTD 2016	YTD 2017	YTD 2018	YTD 2019	YTD % Change 2018 vs. 2019	5-Year YTD Average	YTD 2019 vs. 5-Year Average
All Crimes	2,653	2,353	2,442	2,319	2,502	8%	2,454	2%
Homicide 187(a)PC	35	19	25	22	31	41%	26	17%
Aggravated Assault	1,150	1,061	1,160	1,188	1,347	13%	1,181	14%
Rape	80	93	96	88	71	-19%	86	-17%
Robbery	1,388	1,180	1,161	1,021	1,053	3%	1,161	-9%
Burglary	5,330	3,979	5,363	3,749	4,616	23%	4,607	0%
Vehicle Theft	3,200	3,359	3,144	2,633	2,551	-3%	2,977	-14%
Larceny	2,618	2,424	2,466	2,622	2,438	-7%	2,514	-3%
Arson	66	53	38	71	48	-32%	55	-13%

4. Impact

Public Privacy Impact

GLD has provided significant benefit to the OPD and the community around gun violence. This enhanced public safety value must be weighed, however, against its potential to violate the privacy rights of Oakland residents. The specific risk that must be assessed is the possibility that the system could be used for persistent or targeted audio surveillance – listening or recording voice conversations - given the system's sensors contain microphones that are used outdoors.

ShotSpotter acoustic sensors use ordinary microphones that are similar to ones found in cellphones. They are placed high above the street and are not positioned, tuned or specialized to pick up human voices. The sensors “listen” for gunshot-like sounds and trigger only when detecting an impulsive sound that is 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 ShotSpotter headquarters that includes 1 second of sound prior to the incident (to establish a baseline of ambient noise), the incident itself and 1 second after. 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. It is highly unusual for a human voice to be included in a snippet. For this to occur, the voice must be loud enough to be heard over the gunfire. In addition, there is no personally identifiable information in any audio snippet.

ShotSpotter made significant changes in its audio access and privacy practices starting in 2012. Prior to this time, police had unlimited access to sensor audio. Since 2012, only authorized ShotSpotter employees have access to audio from sensors, they can only access it under a strict set of conditions and can only provide police a short audio snippet.

In 2019 ShotSpotter commissioned an independent privacy audit by the Policing Project at NYU Law School[2]. This end-to-end assessment conducted by objective privacy professionals concluded that the ShotSpotter presents an “extremely low risk of audio surveillance”. The Policing Project based this finding upon the short amount of audio that is temporarily stored on sensors, the short length of audio snippets that are permanently stored as evidence and the internal controls the company uses to restrict access to audio for authorized employees only.

As the audit concludes: “While it is surely possible that ShotSpotter sensors will, on occasion, capture some intelligible voice audio related to a gunfire incident, we have little concern that the system will be used for anything approaching voice surveillance.”

Human voices and street noise 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. That being said, street noise that can include human voices could be captured by a sensor temporarily. All sensor audio, however, is permanently deleted after 30 hours and never heard by a human unless it was accompanied by a loud, impulse sound thought to be a gunshot. Live streaming of audio is not possible.

Public Safety Impact

As described earlier, without ShotSpotter, OPD would be aware of only a small fraction of shootings in Oakland because most are not called in via 911. This phenomenon is not limited to Oakland with an average of less than 20%

[2] https://www.policingproject.org/shotspotter

of gunshot incidents being called in.[3] In addition, even when incidents are called in, many minutes can pass before the first 911 call comes in and the information about shots fired location is often inaccurate. GLD System technology notifies OPD of gunshot incidents in less than 60 seconds with an accurate location. This helps OPD personnel to leverage their street presence and vehicle mobility to respond more quickly to gunshots and no longer be dependent on the public to call 911 and report them.

In summary, the benefits that OPD can directly attribute to using GLD include:

- Awareness of gunshot incidents that the department would not have known about
- Significant time savings in learning about a gunshot incident along with a precise location
- Ability to get to crime scene faster to provide or call in treatment for gunshot wound victims
- Ability to find and collect more ballistic evidence
- Ability to identify and interview more witnesses
- Better crime scene intelligence available in the form of data on timing, sequence and location of each shot fired in the incident
- Tactical intelligence provided for responding patrol officers to help them approach the crime scene safely (e.g. multiple shooters, automatic weapons)

Some critics of the system say that it does not enable OPD to consistently catch criminals at the scene and therefore the system doesn't help with gun violence. OPD cannot always respond immediately to gunshot activations. However, gunshot location information is very helpful even when OPD cannot respond immediately. The consistent collection of ballistic evidence (e.g. shell casings, found firearms) can be used to connect gun crimes. Also, responding to gunshot locations allows for a greater likelihood of finding witnesses who often disappear if police response is delayed and doesn't happen. Therefore, the use of ShotSpotter results in more suspects being identified, arrested and prosecuted for gun crimes, and ultimately contributing to a reduction in shootings.

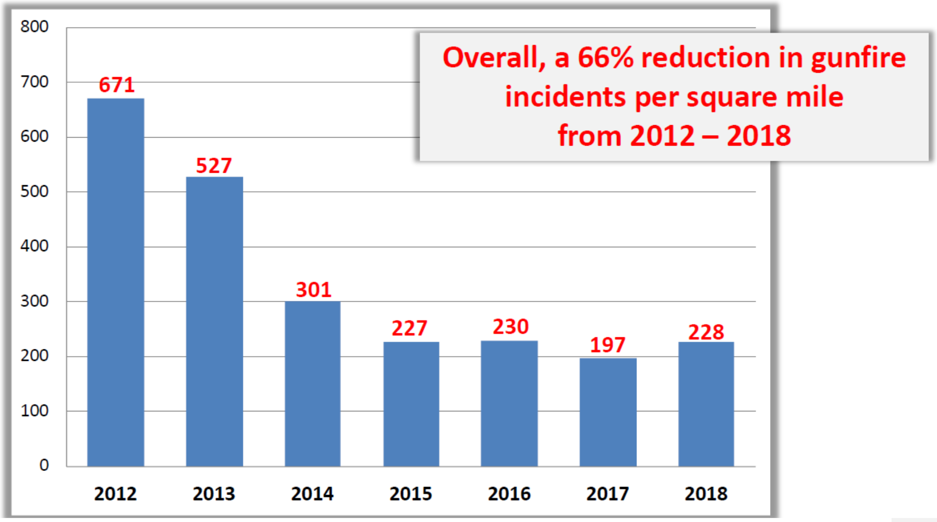
OPD is aware of an ongoing lawsuit stemming from the City of Rochester, New York's use of ShotSpotter[4]. The lawsuit relates to Rochester's use of ShotSpotter for evidentiary support for prosecutions. The "Purpose" section

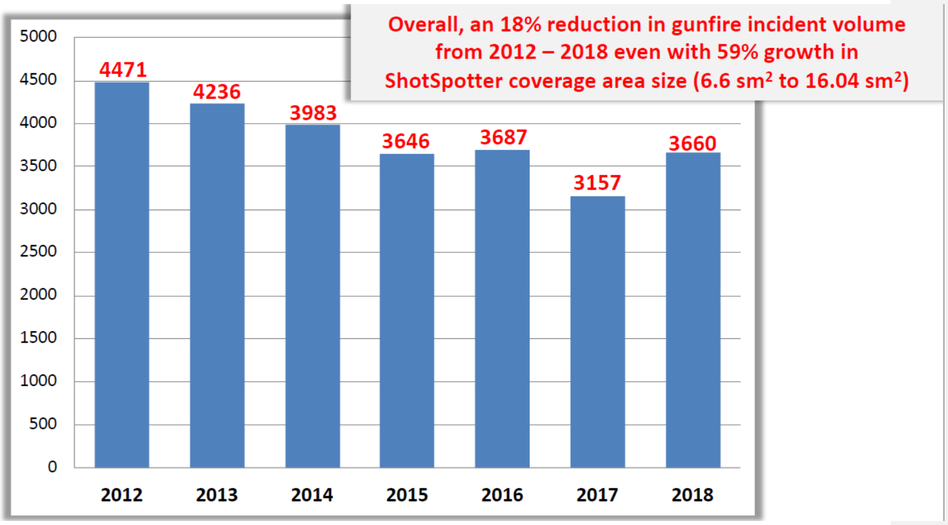
[3] The geography, incidence, and underreporting of gun violence: https://www.brookings.edu/research/the-geography-incidence-and-underreporting-of-gun-violence-new-evidence-using-shotspotter-data/

[4] Silvon S. Simmons vs. Joseph M. Ferrigno, II, Samuel Giancursio, Mark Wiater, Christopher Muscato, Robert Wetzel, Michael Ciminelli, John Does 1-20, City of Rochester, ShotSpotter, Inc., SST, Inc., John Does 21-30 and Paul C. Greene

above speaks to use of DFR Reports by OPD and the County of Alameda. In this case, the New York City-based Innocence Project, has filed a legal brief in a Rochester criminal case, challenging the reliability of ShotSpotter when it is used for more than a gunfire alert system. OPD will assess the eventual results of these legal proceedings. Current ShotSpotter use in Oakland continues to show that ShotSpotter provides a reliable tool for precise gunshot location detection.

In Oakland since 2012 there has been a 66% reduction in shooting incidents per square mile of ShotSpotter coverage (see charts below). OPD cannot directly attribute this significant gun crime reduction trend to ShotSpotter. However, OPD does believe that ShotSpotter plays a vital role in OPD's large gun crime reduction strategies.





Overall, an 18% reduction in gunfire incident volume from 2012 – 2018 even with 59% growth in ShotSpotter coverage area size (6.6 sm^2 to 16.04 sm^2)

OPD cannot draw direct causal relationships between the GLD system and gun crime activity. However, OPD's Ceasefire Unit (focused on diminishing the prevalence of gunshot activity) sees correlations between the use of the GLD system and gunshot activity; in 2014 there were 420 incidents of Assault with a firearm (criminal code 245(a)(2)PC)); 2015 saw 342 incidents; 2016 saw 331 incidents; 2017 saw 281 incidents and 2018 saw 277 incidents – a consistent five year decrease.

OPD views GLD as a community partnership building resource as well. GLD system data pinpoints exactly where to attempt to engage neighbors in areas where shots are being fired. Officers can use this information to introduce themselves to community members, ensure they are safe, and understand what they know related to shots being fired. These initial meetings related to gunfire serve as starting points for greater constructive contact between residents and OPD officers. In particular, OPD has been able to achieve a significant decrease in the incidence of celebratory gunfire around the July 4th and New Year's holidays using GLD to proactively engage with the community prior to these holidays about the dangers of celebratory gunfire.

Commented [BS1]: GLD for community outreach on celebratory gunfire

As OPD offers a consistent, positive response to gunshot incidents, there is a greater opportunity to improve trust with the community as they see police engaging.

5. Mitigations

OPD, in partnership with ShotSpotter has developed protocols to ensure that the

GLD system does not overly burden the public’s right to privacy.

OPD DEPARTMENTAL GENERAL ORDER (DGO) “I-20 Gunshot Location Detection System” Section B “General Guidelines” explains that:

- Only authorized users may access the GLD system;
- No one may access the system without training;
- Only specifically authorized personnel authorized by the Chief or Chief-designee (e.g. personnel with OPD’s Ceasefire Unit and CID crime analysts and investigators) will have access to historical GLD system data via desktop GLD system applications.

DGO I-20 Section D “Training” explains that: Training requirements for employees authorized to use the GLD system include completion of training by the GLD System Coordinator or appropriate subject matter experts as designated by OPD. Trainings shall be implemented through OPD’s digital policy and training platform.

Such training shall include:

- Applicable federal and state law
- Applicable policy
- Functionality of equipment
- Accessing data
- Safeguarding password information and data
- Sharing of data

Technology and operational mitigations by ShotSpotter:

Sensors are placed high above the ground typically on top of buildings or sometimes lampposts. At this height, there is more limited ability to pick up street level sounds clearly.

The sensors are not capable of audio streaming – neither ShotSpotter nor OPD can listen in on street level sounds in real-time.

The system permanently deletes all audio that is temporarily stored on the sensor after 30 hours.

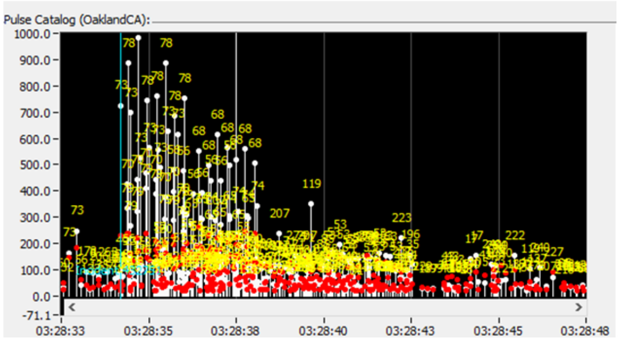
The system only triggers an incident to send downstream when 3 or more sensor hear a loud, impulsive sound. Sensors cannot be triggered by human voices because voices are not impulsive enough or loud enough to be heard by 3 sensors which may be 800 meters or more apart. Thus, the audio of a human voice that may be captured by 1 sensor would be permanently deleted after 30 hours and no police or ShotSpotter employee will have heard that sound.

If a sound is loud enough and sharp enough to possibly be a gunshot and is detected by 3 or more sensors and a location is able to be determined, the system pulls a short audio snippet of the sound plus 1 second of ambient noise prior to the incident and 1 second after. This is typically 10 seconds or less in total - not enough to transmit a conversation. This audio is interpreted by a machine at first and then reviewed by an acoustic analyst at ShotSpotter Headquarters who is only presented with the audio snippet and is under significant time pressure to process the incident as either a gunshot or to dismiss as a non-gunshot and get on to the next incident. All incidents, whether determined to be a gunshot or non-gunshot, are permanently and securely stored in the cloud to serve as both evidence and to train the machine classifier in the future.

ShotSpotter security protocols also mitigate gunshot detection data access. ShotSpotter, as mentioned above under "Impact / *Public Privacy Impact," does not provide* extended audio to OPD or any police agency; they will not provide this access even if requested. Additionally, ShotSpotter does not provide actual precise locations of the sensors to OPD.

As previously mentioned, the sensors are constantly listening for gunshot-like sounds and storing what is captured for 30 hours (was 72 hours before July 2019), and then deleting the data unless triggered to send the data to the ShotSpotter Cloud for analysis. The 30 hour buffer allows OPD to request data within 24 hours in cases where gunshots have been identified by police but not picked up by the system or if there is a need to verify if there were other gunshots prior to the authenticated event. ShotSpotter policy stipulates that only a limited number of authorized forensic engineers can access the storage buffer of a sensor to retrieve prior recorded data within that 30 hour window and search for other gunshot impulsive sound events. To avoid listening to recorded data on a sensor in a haphazard way, the search for a missing gunshot is first done visually through a secure interface looking for the prevalence of electrical "pulses" strong enough to be a gunshot that occurred around the time of the incident in question. See the screenshot below.

BROWSING PULSES



,

The system will download an audio snippet of one second before to one second after the gunshot sound incident and provide to OPD.

It is possible, but highly unusual, for a human voice to be heard within an audio snippet given the loud nature of the gunshot or gunshot-like sound that is occurring is the primary audio event of the snippet. Upon receiving a gunshot alert OPD authorized personnel may find that a voice has been recorded along with gunshot sound, but such voice data is only associated with the actual gunshot data and has no personally identifiable information built in. There is no way to tag any voice audio that is unintentionally recorded when connected to a gunshot.

6. Data Types and Sources

The GLD system uses acoustical digital data file recordings (.wav files) to send to the ShotSpotter Cloud for gunshot verification. Verified gunshot recordings stored on HQ servers can be reviewed by OPD personnel on desktop or mobile applications.

7. Data Security

OPD takes data security seriously and safeguards GLD System data by both procedural and technological means. The mitigation section above explains that only authorized and trained personnel will be permitted access to the GLD system. The system always requires user and password ID for login. Furthermore, as explained in the Mitigation Section above, only personnel specifically designated by the Chief or Chief-designee have access to the GLD system desktop applications which provide access to any historical downloadable data.

The GLD technology itself provides many layers of data security. The sensors detect loud, impulsive sounds; only when such sounds are recorded are audio files captured and sent to ShotSpotter HQ and then to OPD; other street sound recordings such as human conversations are thus constantly deleted.

8. Costs

OPD has been a ShotSpotter customer for majority of the last 13 years, ShotSpotter's delivery and pricing model has evolved from a traditional premise-based hardware/software capital cost + maintenance fees to a modern Software-as-a-Service (SAAS) subscription model without an upfront capital investment. Over the years, the company has occasionally raised its subscription fees based on increases in the cost of doing business, as summarized below:

Phase I:
OPD entered into the original contract (Resolution No. 80075 C.M.S.) with ShotSpotter in 2006 for the purposes of piloting the gunshot detection system in 6.2 square miles of the city. This initial contract authorized installation of the ShotSpotter GLD system in two areas of Oakland for approximately $70,000 per year. In October 2011, the City entered into a new contract with SST, Inc (ShotSpotter) for approximately $84,000 per year for Phase I to convert the coverage from the premise-based hardware/software model to the current SAAS model.

Phase II:
In November 2012, Oakland expanded the ShotSpotter coverage areas to include another 6.6 square miles, creating a total coverage area of 12.8 square miles. The Phase II expansion was priced at the then-current rate of $40,000 per square mile, bringing that expansion cost to $264,000.

Phase III:
In September 2015, Oakland further expanded ShotSpotter coverage by 2.78 square miles. This expansion was priced at slightly less than the then-current rate of $55,000 per square mile, for an expansion cost of $146,600.

Note that until 2017, there were no increases applied to the subscription renewals despite the fact that the City's rates were well below ShotSpotter's market rate, and the City continues to enjoy rates that are significantly below ShotSpotter's current annual market rate of $65,000 per square mile of coverage. Table A below outlines Oakland's current price per square mile:

Table A

Contract Phase	Coverage Area Size (mi^2)	Current Annual Price	Subscription Renewal Date	Current Price Per mi^2
Phase I	6.2	$92,610	April 18, 2020	$14,937

Phase II	6.6	$291,060	June 30, 2020	$44,100
Phase III	2.78	$161,627	June 30, 2020	$58,139
CURRENT TOTAL ANNUAL FEE:		**$545,297**		**Average Price Per mi^2 $34,999**

Current Contract for 2018-2021:

In April 2018, the City adopted a resolution that continued the ShotSpotter service for all three phases of ShotSpotter for a year and also allowed extension for all phases for an additional two years with a nominal 5% increase per year. That resolution resulted in a contract for an amount not to exceed $1,637,188 for a three-year period (2018-2021) for all three ShotSpotter contract phases of 15.58 square miles. This represents an average annual subscription fee of $35,028 per square mile.

9. Third Party Dependence

OPD, as mentioned in Section 1 above, Currently, OPD contracts with ShotSpotter, Inc., the creator of the ShotSpotter® Flex™ system "ShotSpotter." ShotSpotter is the most widely used outdoor gunshot system in the United States with over 100 installations.

10. Alternatives Considered

OPD officers and investigators rely primarily on traditional members of the public to report gunshot crimes whether or not there are associated gunshot victims. Members of the public, when they witness or hear gunshots (and if they choose to report incidents) often report inaccurate locations due to limitations of the human ear as sound echoes off buildings, trees and other objects. GLD systems have revolutionized real-time intelligence for police. OPD believes that there is no alternative to a modern GLD system other than having exponentially greater numbers of sworn personnel covering many areas throughout the City and/or using more intrusive forms of recording equipment.

ShotSpotter is the leading GLD provider with over 100 cities installed. There are several other gunshot detection systems available such as Shooter Detection Systems (SDS), AmberBox and Boomerang. Many of these systems, like AmberBox and SDS, are for indoor purposes only and would not address most shootings that occur in Oakland. The non-ShotSpotter outdoor systems suffer from serious deficiencies that make them poor fits for Oakland. They do not have the ability to locate gunshots accurately; they do not provide a second phase of gunshot verification with human review and suffer from high false positives; they do not have proven citywide deployments; and they do not provide the post incident reporting to help locate shell casings and/or court admissible reporting for timing, sequence and number of rounds fired.

OPD does not consider any of these systems to offer a reasonable solution – OPD needs an outdoor GLD that provides coverage to multiple areas where gunshot activity regularly occurs.

Other alternatives would be to continue to rely on less frequent and accurate information provided by the public and to have less information about real-time gunshots. These alternatives are not considered useful given the volume of gunshot incidents which occur in Oakland.

11. Track Record of Other Entities

ShotSpotter states that its system is now used in over 100 cities across the United States, and in parts of the Caribbean and South Africa. Nearly half of the top 50 metros use ShotSpotter including Baltimore, Washington D.C., Chicago, New York, Denver and San Francisco[5]. There are 14 cities in California using the system.

Sample results reported from other cities:

- Chicago cites a drop of over 40% in shootings in the Englewood District in the first year after installation[6]
- Cincinnati cites a 48% reduction in shootings in first year[7]
- Camden County, NJ - 46% reduction in homicides by shooting[8]
- Rochester, NY - 40% reduction in shooting incidents[9]
- Denver - 103 arrests and 84-gun recoveries over the course of 3 years[10]
- Bakersfield - 22 arrests in first 9 months[11]
- Pittsburgh – 48 arrests and 83 victims found with help of ShotSpotter

[5] OPD understands that some police agencies have chosen not to renew their contacts with ShotSpotter. OPD believes that for some law enforcement agencies the decision is based on value and budget issues rather than efficacy or privacy issues. Many cities do not have the same level of gun crime density as OPD so for some cities the need for a GLD system may not justify the cost.

[6] https://www.chicagotribune.com/news/breaking/ct-met-superintendent-eddie-johnson-chicago-violence-20171116-story.html

[7] https://www.wcpo.com/news/crime/shootings-down-nearly-50-percent-in-cincinnati-this-year-police-say

[8] https://www.phillymag.com/news/2015/04/02/camden-reduces-gunfire-by-48-percent/

[9] https://www.democratandchronicle.com/story/news/2016/09/06/shotspotter-technology-gun-violence/89764672/

[10] https://www.thedenverchannel.com/news/crime/denver-police-to-test-shotspotter-system-in-4-different-neighborhoods-with-live-gunfire

[11] https://bakersfieldnow.com/news/local/is-shotspotter-working-in-bakersfield

in 3 years[12]

- 2018 Las Vegas Metro Police pilot report indicates 342 gunshot incidents were identified by ShotSpotter in first 9 months of use that the PD would not have known about. Recommends continuing ShotSpotter in current coverage area and expanding coverage to all known hotspots.[13]
- NYC 2018 Police Commissioner's Report – "ShotSpotter alerts officers to the scene to suppress further violence; to gather ballistic evidence; to locate relevant surveillance video; and to canvas the neighborhood for people who may have seen or heard something. Any of this evidence might provide decisive when investigators are trying to build a case against gang members or other violent criminals in the area."[14]Peoria, IL Police Department in 2016 increased their ShotSpotter coverage area to from three to six miles. They cite the systems usefulness in terms of having better information about where to find shell casings related to gunshot activity. The Chief of Police has stated that the system has improved the department's public image as the public sees the department enhancing its ability to respond to crime through use of the system. The system helps with gun tracing – shell casings are entered into the ATF's National Integrated Ballistic Information Network (NIBN) for tracing; when guns are also recovered based on ShotSpotter location data, the guns can then be matched through NIBIN to other gun casings, ultimately helping to connect different shootings to a single.

[12] https://www.post-gazette.com/local/city/2018/03/14/Pittsburgh-City-Council-ShotSpotter-expansion-Wendell-Hissrich-North-Side-Jason-Lando-Darlene-Harris-Deborah-Gross/stories/201803140183

[13] https://www.shotspotter.com/wp-content/uploads/2019/08/LVMPD-ShotSpotter-Assessment-V102418.pdf

[14] https://www.shotspotter.com/wp-content/uploads/2018/09/2018-Police-Commissioners-Report-SST-Section.pdf

6

Oakland Forensic Reports

As of 2019-09-06 17:17:21 • Generated by Paul Di Lella

Filtered By
Show: All cases

Case Record Type ↑	Date/Time Opened ↑	Account Name	Subject
DFR	CY2012	Oakland, CA	OAK DFR request
		Oakland, CA	OAK - OIS
		Oakland, CA	Oakland - DFR Incident 3455
		Oakland, CA	Oakland - Forensic Request Audio
		Oakland, CA	RE: OIS
		Oakland, CA	OAK DFR req 3/28/2012
		Oakland, CA	Oakland Expert Testimony
		Oakland, CA	Oak - Public Defenders office request for dfr
	Subtotal Count	8	
	CY2013	Oakland, CA	People v. C.S.-Murder Trial
		Oakland, CA	OAK - DFR req 06/06/2012
		Oakland, CA	OAK - DFR req 07-23-10 13:30 hrs
		Oakland, CA	OAK - DFR Request 02/14/13
		Oakland, CA	OPD - DFR req Incident 4430
		Oakland, CA	OAK - DFR req 03/27/2013
		Oakland, CA	Customer request copy of DFR for OIS
		Oakland, CA	OAK - DFR req 07/24/2013
		Oakland, CA	OAK - DFR req
		Oakland, CA	OAK - DFR req 03/02/2013
		Oakland, CA	OAK - DFR request - 04/052013
		Oakland, CA	Oak - DFR req 10/07/2013
		Oakland, CA	Oak - DFR req 06/09/2013
		Oakland, CA	OAK - DFR req 2013-11-02
		Oakland, CA	OAK - DFR req 08/27/2012
		Oakland, CA	OAK - DFR req - 11/25/13
		Oakland, CA	OAK - DFR req - 11/23/2013
		Oakland, CA	OAK DFR req 07/31/2013
	Subtotal Count	18	
	CY2014	Oakland, CA	OAK - DFR Req - OIS - 01/21/2014
		Oakland, CA	OAK - OIS
		Oakland, CA	CHP OIS #2
		Oakland, CA	OAK - DFR req 02/26/2014
		Oakland, CA	OAK - DFR req 04/15/2014
		Oakland, CA	DFR - Oakland OIS - January 21, 2014

		Oakland, CA	OAK - DFR req - 03/25/2014 - Flex 95665
		Oakland, CA	OAK - DFR req - 10/04/2014 - 135120/135122 (outside coverage)
		Oakland, CA	OAK - DFR req - 08/05/2014 - 131949
		Oakland, CA	Audio & DFR Requests - Oakland
Subtotal	Count	10	
CY2015		Oakland, CA	Oakland - DFR req - 02/02/2015 - 143604
		Oakland, CA	OAK - OIS
		Oakland, CA	OAK - OIS
		Oakland, CA	OAK - DFR req - 07/06/2012
		Oakland, CA	Oakland-DFR Requests
		Oakland, CA	DFR request
		Oakland, CA	DFR Request
		Oakland, CA	OAK - DFR Request - Homicide
		Oakland, CA	OAK - OIS
		Oakland, CA	OAK DFR Request
		Oakland, CA	OAK DFR Request
		Oakland, CA	OAK DFR request
		Oakland, CA	OAK DFR Request
		Oakland, CA	OAK DFR Request
		Oakland, CA	OAK DFR Request
		Oakland, CA	OAK - OIS
		Oakland, CA	OAK - DRR - Homicide
		Oakland, CA	OAK - DFR Request
		Oakland, CA	OAK - DFR Request
		Oakland, CA	OAK - OIS
		Oakland, CA	OAK - DFR
		Oakland, CA	OAK - DFR Request - Homicide
Subtotal	Count	22	
CY2016		Oakland, CA	OAK - DFR Request
		Oakland, CA	OAK - DFR Request
		Oakland, CA	OAK - DFR
		Oakland, CA	OAK - DFR
		Oakland, CA	OAK - DFR - Homicide
		Oakland, CA	OAK - DFR - Homicide
		Oakland, CA	OAK - DFR - Homicide
		Oakland, CA	OAK - DFR - Homicide
		Oakland, CA	OAK - DFR Request
		Oakland, CA	OAK - DFR Request
		Oakland, CA	DFR for Oakland Incident #210103
		Oakland, CA	DFR Request Oakland # 207112
		Oakland, CA	OaklandCA - DFR req - 2015-06-27 - Flex 160198-160199
		Oakland, CA	DFR Request
		Oakland, CA	Alameda County DA's Office Request
		Oakland, CA	Oakland, CA - DFR Request
		Oakland, CA	DFR_FlexID 250163
		Oakland, CA	DFR Oakland

		Oakland, CA	Request for Shotspotter Info. (doc # 617447)
		Oakland, CA	Detailed Forensic Report Flex 254426
		Oakland, CA	OaklandCA - DFR req - 09/25/2016 - Flex 255122
		Oakland, CA	DFR- Oakland CA - Flex ID 255335
		Oakland, CA	DFR Request for Oakland, CA Incident #256853
		Oakland, CA	Shotspotter Forensic report Re: Docket 16-CR-7289
		Oakland, CA	DFR Oakland Incident 256181 , Homicide Requesting Audio
Subtotal	Count	25	
CY2017		Oakland, CA	OaklandCA - DFR - 01/12/2017 - Flex ID 264928
		Oakland, CA	Oakland-DFR-01/19/2017-Flex ID 265279
		Oakland, CA	Oakland-DFR-01/19/2017-Flex ID 265281
		Oakland, CA	DFR Request-OaklandCA-SF14089
		Oakland, CA	OaklandCA-DFR-FLEX 267618
		Oakland, CA	Oakland CA - DFR - 2000 E 21st St.
		Oakland, CA	OaklandCA- DFR- 02/15/2017- Flex 267826
		Oakland, CA	OaklandCA -- OIS
		Oakland, CA	OaklandCA DFR- 12/28/2016- Flex 261062
		Oakland, CA	OaklandCA - DFR - Flex ID: 147233 - 04/14/2015
		Oakland, CA	OaklandCA - DFR - 03/31/2017 - Flex 269457
		Oakland, CA	DFR-- FlexID #135615 10/13/2014
		Oakland, CA	Oakland Expert Testimony Req: DFR, incident 141689; 01012015
		Oakland, CA	OaklandCA - DFR - P. v. City of Oakland - 11/15/2015 - Flex 195744
		Oakland, CA	OaklandCA - DFR - 12/26/2016 - Flex ID 260946
		Oakland, CA	OaklandCA - DFR- 5/21/2017- Flex 271488
		Oakland, CA	OaklandCA - DFR - 05/30/2017
		Oakland, CA	OaklandCA-Flex #150325 DFR Request
		Oakland, CA	OaklandCA - DFR - 12/28/2016 - Flex 261062
		Oakland, CA	OaklandCA-DFR request Flex #269252
		Oakland, CA	OaklandCA - DFR - 06/23/2017 - Flex 280217
		Oakland, CA	OaklandCA - DFR - 12/28/2016 - Flex 261064
		Oakland, CA	OaklandCA - DFR Request - 8/30/2017 - Flex ID# 285081
		Oakland, CA	OaklandCA- DFR- 1/20/15
		Oakland, CA	OaklandCA- DFR- 9/1/17- FID 317557
		Oakland, CA	OaklandCA: DFR req incident 10102017, 1951h;
		Oakland, CA	OaklandCA-DFR request-10/15/17-Flex #'s 320197 & 320198
		Oakland, CA	OaklandCA-DFR Request-11/22/2017-0300hrs
		Oakland, CA	OaklandCA-DFR-12/23/2017-
Subtotal	Count	29	
CY2018		Oakland, CA	OaklandCA - DFR (OIS) - 1/3/2018 - Flex 329257
		Oakland, CA	OaklandCA - DFR - OIS - Flex 195744 -
		Oakland, CA	OaklandCA - DFR - 07/24/2016 - Flex 250163
		Oakland, CA	OaklandCA-OIS-DFR-03/11/2018-Flex ID 334454-
		Oakland, CA	OaklandCA - DFR - People v J.K. - 12/17/2016 - Flex ID: 260258
		Oakland, CA	OaklandCA- DFR- 12/31/17- Flex ID 326011
		Oakland, CA	OaklandCA - DFR - Court Date 06/15/2018 - Flex 325041 - 12/26/2017
		Oakland, CA	Oakland, CA - DFR Request - (OaklandCA) - FID 259179

			Oakland, CA	Oakland, CA - DFR Request - (OaklandCA) - FID 259184
			Oakland, CA	OaklandCA - DFR - 5/17/2018 - FID 336652
			Oakland, CA	Oakland CA- DFR-12/31/2017- Flex ID 326394
			Oakland, CA	Oakland CA-DFR- 12/31/2017- Flex ID 326451
			Oakland, CA	OaklandCA - DFR - 08/26/2018 - Flex 386374 & 386375
			Oakland, CA	OaklandCA - DFR - 08/28/18 - Flex ID 386637
			Oakland, CA	OaklandCA - DFR - 08/27/2018
			Oakland, CA	OaklandCA - DFR - 06/09/2018
			Oakland, CA	OaklandCA - OIS - DFR - 10/19/2018- Flex ID 394755
			Oakland, CA	OaklandCA - DFR - 11/01/2018
			Oakland, CA	OaklandCA- DFR - People v P. - 5/27/2018 - Flex 338170
	Subtotal	Count	19	
	CY2019		Oakland, CA	OaklandCA - DFR - People v T.F. - 02/11/2017 - Flex 267618 - Alameda Cnty Public Defender
			Oakland, CA	OaklandCA - DFR - 1/31/2019 - 0115hrs
			Oakland, CA	OaklandCA - DFR - 08/26/18 - Flex 386405
			Oakland, CA	OaklandCA - DFR - 4/24/2019 - Incident 428545
			Oakland, CA	OaklandCA - DFR - OIS - 05/22/2019
			Oakland, CA	OaklandCA - DFR - People v D.J. and J.B. - 04/03/2016 - Flex 205617
			Oakland, CA	OaklandCA - DFR - 03/29/2016 - ID 95-205395
			Oakland, CA	OaklandCA - DFR - 08/03/2018 - Flex 383478
	Subtotal	Count	8	
Subtotal		Count	139	

OAK Expert Testimony

As of 2019-09-12 11:41:25 • Generated by Paul Di Lella • Sorted by Date/Time Opened (Ascending)

Filtered By
Show: All cases
Units: Hours
Case Record Type equals Expert Testimony
Account Name contains oakland

Case Owner	Account Name	Subject	Date/Time Opened
Support	Oakland, CA	OAK - Expert testimony - People v. Steen - Duvernay - Defense	1/30/2013 5:49 PM
Paul Greene	Oakland, CA	OAK - Expert testimony - People v Barrientos - 08/27/10 - Brouhard	2/12/2014 11:55 AM
Paul Greene	Oakland, CA	OAK - Expert testimony - People v Johnson - 07/08/2007 - Bates	2/12/2014 12:54 PM
Paul Greene	Oakland, CA	OAK - Expert testimony - People v Omar Ward - 03/09/2008 - Johnson	2/12/2014 1:03 PM
Paul Greene	Oakland, CA	OAK - Expert testimony - 8/6/2012	2/12/2014 1:18 PM
Paul Greene	Oakland, CA	OAK - Expert testimony - 4/28/2014 - Beltramo	4/28/2014 5:12 PM
Paul Greene	Oakland, CA	OAK - Expert testimony - People v Tabron- 03/02/2013 - Santos	11/6/2014 1:21 PM
Support	Oakland, CA	OAK - Expert testimony - People v. Wallace and Carroll	2/23/2016 10:35 AM
Walter Collier III	Oakland, CA	OaklandCA - Expert testimony - People v Michael Armond Enoch	4/11/2016 2:10 PM
Paul Greene	Oakland, CA	OaklandCA - Expert testimony - People v Michael Horace - 04/29/2015 - McGuiness	7/14/2016 10:38 AM
Paul Greene	Oakland, CA	OaklandCA - Expert testimony - People v James Frank Bowen - 09/20/2014 - Cavagnaro	10/24/2016 2:34 PM
Jason Dunham	Oakland, CA	OaklandCA - Expert testimony - People v Nathaniel Jackson	4/20/2017 12:01 PM
Mike Will	Oakland, CA	OaklandCA - Expert Testimony - People v. Andre Poole	4/25/2017 10:24 AM
Mike Will	Oakland, CA	OaklandCA - Expert testimony - Oakland Flex IDs 145730, 145731	5/8/2017 9:18 AM
Ron Cayabyab	Oakland, CA	OaklandCA - Expert testimony- 1/20/15-12th/Campbell St- 1524hrs - Wendt	9/22/2017 2:48 PM
Paul Greene	Oakland, CA	OaklandCA - Expert testimony - OIS - Perkins v City of Oakland - 11/15/2015 - Flex 195744 - Loebs	10/11/2017 12:13 PM
Paul Greene	Oakland, CA	OaklandCA - Expert Testimony - People v Honorio Hernandez-Meza - 07/24/2016 - Wendt	1/4/2018 3:56 PM
Paul Greene	Oakland, CA	OaklandCA - Expert Testimony - People v Jasiri Katari - Beltramo	3/12/2018 7:35 PM
Paul Greene	Oakland, CA	OaklandCA - Expert Testimony - 3/23/2012 - Oh	3/13/2018 11:45 AM
Paul Di Lella	Oakland, CA	OaklandCA - Expert Testimony - People v Bobby Henry - Tienken	4/16/2018 7:35 AM
Paul Greene	Oakland, CA	OaklandCA - Expert testimony - People v Honorio Hernandez-Meza - Wendt	5/8/2018 9:25 AM
Walter Collier III	Oakland, CA	OaklandCA - Expert Testimony - People v Cohrion Arnold Malone - Beltramo	8/21/2018 4:41 PM
Paul Di Lella	Oakland, CA	OaklandCA - Expert Testimony - People v. Shiheim Johnson - Wagstaffe	10/17/2018 11:35 AM
Paul Greene	Oakland, CA	OaklandCA - Expert testimony - People v Porter - Ching	12/28/2018 1:56 PM
Paul Greene	Oakland, CA	OaklandCA - Expert testimony - People v Tavon Foster - Cediel - Defense	1/9/2019 3:20 PM
Paul Greene	Oakland, CA	OaklandCA - Expert testimony - People v Spruell - Roisman	4/2/2019 10:26 AM
Paul Greene	Oakland, CA	OaklandCA - Expert testimony - People v Damarie Jones and John Blacknell - Wagstaffe	6/2/2019 1:04 PM
Paul Greene	Oakland, CA	OaklandCA - Expert testimony - 8/3/2018 - Hernandez	7/23/2019 3:21 PM
Total Count	29		

8. Costs

OPD has been a ShotSpotter customer for majority of the last 13 years, ShotSpotter's delivery and pricing model has evolved from a traditional premise-based hardware/software capital cost + maintenance fees to a modern Software-as-a-Service (SAAS) subscription model without an upfront capital investment. Over the years, the company has occasionally raised its subscription fees based on increases in the cost of doing business, as summarized below:

Phase I:
OPD entered into the original contract (Resolution No. 80075 C.M.S.) with ShotSpotter in 2006 for the purposes of piloting the gunshot detection system in 6.2 square miles of the city. This initial contract authorized installation of the ShotSpotter GLD system in two areas of Oakland for approximately $70,000 per year. In October 2011, the City entered into a new contract with SST, Inc (ShotSpotter) for approximately $84,000 per year for Phase I to convert the coverage from the premise-based hardware/software model to the current SAAS model.

Phase II:
In November 2012, Oakland expanded the ShotSpotter coverage areas to include another 6.6 square miles, creating a total coverage area of 12.8 square miles. The Phase II expansion was priced at the then-current rate of $40,000 per square mile, bringing that expansion cost to $264,000.

Phase III:
In September 2015, Oakland further expanded ShotSpotter coverage by 2.78 square miles. This expansion was priced at slightly less than the then-current rate of $55,000 per square mile, for an expansion cost of $146,600.

Note that until 2017, there were no increases applied to the subscription renewals despite the fact that the City's rates were well below ShotSpotter's market rate, and the City continues to enjoy rates that are significantly below ShotSpotter's current annual market rate of $65,000 per square mile of coverage. Table A below outlines Oakland's current price per square mile:

Table A

Contract Phase	Coverage Area Size (mi^2)	Current Annual Price	Subscription Renewal Date	Current Price Per mi^2
Phase I	6.2	$92,610	April 18, 2020	$14,937
Phase II	6.6	$291,060	June 30, 2020	$44,100
Phase III	2.78	$161,627	June 30, 2020	$58,139
CURRENT TOTAL ANNUAL FEE:		**$545,297**		**Average Price Per mi^2** **$34,999**

Current Contract for 2018-2021:

In April 2018, the City adopted a resolution that continued the ShotSpotter service for all three phases of ShotSpotter for a year and also allowed extension for all phases for an additional two years with a nominal 5% increase per year. That resolution resulted in a contract for an amount not to exceed $1,637,188 for a three-year period (2018-2021) for all three ShotSpotter contract phases of 15.58 square miles. This represents an average annual subscription fee of $35,028 per square mile.