From: [redacted]

Sent: 4/30/2014 7:41:01 PM +0000

To: "Strunk, Craig" <CITY OF OAKLAND/CITY ATTORNEY'S OFFICE/RECIPIENTS/STRUN9C>

Subject: Research on shotspotter and warrant less surveillance

Ms. Parker

As you may know I've been trying and trying again and again, to get anyone to comment on the research I have done on this company.

This system is coming up to a vote soon, and you will also discuss expansion.
After reading the article in the east bay express today. I am further concerned in this company's deceptive practices, and their unwillingness to be upfront in their dealings with the city council and the OPD . My repeated calls to them have been ignored as well. Maybe You are the one to bring up the matters that I am going to be bringing to you.

As the city's lawyer, I would like you to show me how this company can operate without a search warrant.

I would like to be present in these meeting with shotspotter officials, How can I do that?

I will have a handful of emails to come, please read them carefully. I have very serious concerns. These concerns have been brushed off by the OPD and I've been lied to directly by them. I am not OK with being lied to. I am not ok with being ignored by you either. PLEASE RESPOND

This first one will have to deal with WARRANT LESS SURVEILLANCE and the LAW.

Congress passed this act in 1968, trying to control warrant less surveillance.

https://en.wikipedia.org/wiki/Omnibus_Crime_Control_and_Safe_Streets_Act_of_1968

If I am understanding this law correctly, installing a surveillance microphone directly in front of my apartment and recording my voice violates my constitutional protection against unreasonable "search and seizure"_ A search and seizure is illegal without a search warrant **(7)**

Recording, Storing, and Reviewing conversations on my own street in front of my own apartment(and all around this city and country) violates the "expectation of privacy."**(8)** ***18 U.S. Code § 2518 - Procedure for interception of wire, oral, or electronic communications*** provides that a citizen such as myself is entitled to an "expectation of privacy" in speaking with a friend with nobody around, and that any law enforcement officials(or even worse private companies) using recording devices that can pick up these conversations are required to obtain warrants

I believe, We the people, deserve. Total disclosure.Transparent and available data, Not anecdotes.

WE deserve to see data that shows effectiveness of this expensive, intrusive system.

We deserve conversation about the capabilities of these microphones so we can make informed decisions.

After learning the capabilities of surveillance microphones, we would like to put in privacy policies.

After learning the capabilities of surveillance microphones, the public would most likely like to choose a location that is High above any street level conversation.

When I ask questions like this, I shouldn't be treated as an agitator, I should be treated like a concerned citizen and father of 2 daughters . I am concerned about their safety. I don't think when asking questions to city employees, whose salaries I'm paying,that I should be treated the way I am. Disgraceful.!

My research into this company is to follow. It is quite lengthy . I want to make sure I put in here ALL of my concerns. This information makes me uncomfortable. It shows me that the city doesn't do it's research. Doesn't know the actual laws. Doesn't even make the public aware of any concerns, or think that there is any, are manipulated by lobbyists.

Best practices, when "legally spying" is to put up signs to warn us that we MAY be recorded.

This is the bulk of my research with footnotes provided.

What I learned was pretty amazing.

1. These microphones have picked up people's conversations**(1)** ,

(1) http://www.southcoasttoday.com/apps/pbcs.dll/article?AID=/20120111/NEWS/201110339

as well as birds chirping and freeway noise*(2)*

(2)http://www.nytimes.com/2012/05/29/us/shots-heard-pinpointed-and-argued-over.html?pagewanted=all

a) The company denies this **(3)**

2. These microphones are always on, and has been described to be similar to a red light camera

http://records.oaklandnet.com/request/475

"This system is very similar to the red camera technology"

a) the company denies this **(4)**

3. This company's VP claims he can listen, record, store and review ANY noise , even if it isn't given to the police as an alert.
*" **For forensic purposes, all loud, impulsive noises are logged by ShotSpotter systems, even if they do not trigger an automatic alert, in case those noises needed to be reviewed after-the-fact**,"(5)*

4. I was told by assistant Oakland Police chief David Downing that recording conversations is okay "because it's like a video camera," I was also told this in a information request #2577 stating
"**There are no search warrants necessary as the equipment monitors areas that are in public space. It's the same as someone taking pictures in public". - Amber C Fuller (6)**

5. the shotspotter reports have logged 6 incidents in my police district. (12x)since october. This includes the busiest night of the year NYEve----
area 5 where shotspotter has been for close to 8 years had 1532 incidents from april 2013-january 2014. IN the New expansion area, Area 2., in the same time period has 79!!!! 1532-79 ! why the expansion? and why are they considering another expansion. we have the biggest coverage area in the country. 13.3 sq miles (times $40-$60K per sq mile)

http://www2.oaklandnet.com/oakca1/groups/police/documents/webcontent/oak045974.pdf

I went to http://www.justice.gov/ to do some research on the validity of these statements made about needing warrants. I came across some interesting things.

http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf

United States Attorneys Manual Title 9

28 Electronic Surveillance—Title III Applications

"A It must be prepared by an applicant identified as a law enforcement or investigative officer. The application must be in writing, signed by the United States Attorney, an Assistant United States Attorney, and made under oath

B.It must identify the type of communications to be intercepted...."Oral communications" are communications between people who are together under circumstances where the parties enjoy a reasonable expectation of privacy.

C It must identify the specific Federal offenses for which there is probable cause to believe are being committed.

D It must provide a particular description of the nature and location of the facilities from which, or the place where, the interception is to occur.

E.It must identify, with specificity, those persons known to be committing the offenses and whose communications are to be intercepted.

F It must contain a statement affirming that normal investigative procedures have been tried

and failed, are reasonably unlikely to succeed if tried, or are too dangerous to employ.

K. For original and spinoff applications, it should contain a request that the court's order authorize the requested interception until all relevant communications have been intercepted, ***not to exceed a period of thirty (30) days"***

http://www.justice.gov/usao/eousa/foia_reading_room/usab5501.pdf

In light of the case law, the Department requires that every wiretap application seeking to tap a new facility or a new location meet a baseline standard of probable cause by showing both of the following:

• Criminal use of the facility or location within six months of the Department's approval.
• Circumstantial evidence, such as phone records or physical surveillance showing, respectively, that the facility or the location has been used for criminal purposes within three weeks (twenty-one days) of the Department's approval.

http://massprivatei.blogspot.com/2012/06/new-police-gunshot-detection-system.html
It is not generally legal for law enforcement (or anyone else) to make audio recordings of conversations in which they are not a participant without a warrant.

Reading from the California penal code I found this.

632. *(a)* ***Every person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records the confidential communication****, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars ($2,500)*

As of now.

*We don't know what these surveillance microphones are capable of, unless I went to court.

http://records.oaklandnet.com/request/475
As for locations of sensors, amount of sensors, and effective range ***we will not disclose any of this information unless compelled by a court order*** *to release this information as it*

could hamper or hender ongoing or future investigations.

*ShotSpotter audio sensors -- **small computers** with microphones that record and time stamp a certain sound*

*There is NO data supporting efficacy.

http://records.oaklandnet.com/feedback/request/504
"The record you asked for does not exist"

*There are no reports on data including false alarms (Sgt. Holly Joshi said there were 0 false alarms!)

http://records.oaklandnet.com/feedback/request/2456
"This is not being tracked as there is no mechanism through radio or our report management system to produce or gather this data". - Amber C Fuller

*After 8 years in E.Oakland There is nothing to show, safer neighborhoods, less crime, less gun play.

http://www2.oaklandnet.com/oakca1/groups/police/documents/webcontent/oak044795.pdf

* Shotspotter still promotes it's company by saying it's a deterrent, and claims a protective bubble of safety.

http://www.shotspotter.com/press-releases/article/sst-inc.-introduces-breakthrough-gunfire-detection-technology-for-indoors
ShotSpotter gunfire location and alert solutions to provide a complete indoor/outdoor "bubble" of protection around any facility.
ShotSpotter Flex is used by law enforcement around the world to combat gun violence and ***restore public safety to communities afflicted with gun violence.***
The company's deep domain experience, along with cumulative agency best practice experience, **delivers measurable outcomes that contribute to reducing gun violence. SST is a proven solution provider with more than 90 installations across the United States and the world** (UNLIKE ME, SHOTSPOTTER DOESN"T SHOW THEIR WORK)

* Oakland already has the most area covered by SST 13.3 sq miles, and is considering another expansion.

* SST wants to add these inside our schools and certain businesses.

http://www.mercurynews.com/business/ci_24499230/shotspotter-offers-gunfire-detection-bay-area-schools-after

*SST sells fear to inner city neighborhoods, selling non-effective hi-tech tools, taking money from other more effective efforts such as "Cease Fire" and Foot/bike patrol.
"Sandy Hook was a bit of a wake-up call for the country," he said.(CEO Ralph Clark)

http://oaklandlocal.com/2014/03/ceasefire-sweeps-neighborhood-champion-awards/

FOOTNOTES

(2)

http://www.nytimes.com/2012/05/29/us/shots-heard-pinpointed-and-argued-over html?pagewanted=all

"Sgt. Eric Smith of the Richmond Police Department said that in ShotSpotter alerts, he has heard in the background "doors slamming, birds chirping, cars on the highway, horns honking."

(3)

http://www.southcoasttoday.com/apps/pbcs.dll/article?AID=/20120111/NEWS/201110339

The apparent ability of ShotSpotter to record voices on the street raises questions about privacy rights and highlights another example of how emerging technologies can pose challenges to enforcing the law while also protecting civil liberties.

*"James G. Beldock, a vice president at ShotSpotter, said that the system was not intended to record anything except gunshots and that cases like New Bedford's were extremely rare. "**There are people who perceive that these sensors are triggered by conversations, but that is just patently not true," he said. "They don't turn on unless they hear a gunshot."***

"*ShotSpotter officials say their acoustic sensors, set up to detect gunfire, are not designed to record conversations on the street."*
"
"This is a very unusual circumstance if (the sensors) actually picked up any voices," Barrett said. "In particular, I can't ever remember in the history of our technology the sensors ever hearing a fight or some kind of argument going on."January 11, 2012

http://www.mercurynews.com/business/ci_24499230/shotspotter-offers-gunfire-detection-bay-area-schools-after

"There is no way it can record voices,"(Ralph) Clark(shotspotter CEO) said. "It is just not possible technically.

"ShotSpotter's outdoor gunshot detection system helped solve a 2007 Oakland murder when the technology captured a dying man's last words *"*

(4)

http://www.southcoasttoday.com/apps/pbcs.dll/article?AID=/20120111/NEWS/201110339

James G. Beldock, a vice president at ShotSpotter, said"**They don't turn on unless they hear a gunshot." /**

*It's an acoustic sensor. **It's not a microphone**, and **it's only activated when a loud boom or bang happens**," said Barrett, who added: "**It's not listening. There is no listening.**"*

http://www.forbes.com/sites/alexknapp/2013/06/28/shotspotter-lets-police-pinpoint-exactly-where-a-gun-was-fired/
"We don't record everything," he continued. "We're just listening to the 'booms and bangs.'"

(5)

http://www.paloaltoonline.com/news/2010/02/19/shotspotter-system-records-tragic-plane-crash

For forensic purposes, all loud, impulsive noises are logged by ShotSpotter systems, even if they do not trigger an automatic alert, in case those noises needed to be reviewed after-the-fact, he said. (James Bedlock)....we assisted the East Palo Alto Police Department with **the retrieval and storage of the audio captured by their system's ShotSpotter sensors** for the seconds surrounding the impulsive noise

(6)

http://records.oaklandnet.com/feedback/request/2577

(7)

http://www.uscourts.gov/educational-resources/get-involved/constitution-activities/fourth-amendment/wiretaps-cell-phone-surveillance/facts-case-summary.aspx
"For the Fourth Amendment protects people, not places. *What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . .* ***But what he seeks to preserve as private even in an area accessible to the public, may be constitutionally protected," the Court stated. Building upon this reasoning, the Court held that it was the duty of the Judiciary to review petitions for warrants in instances in which persons may be engaging in conduct that they wish to keep secret, even if it were done in a public place"***

(8)
https://en.wikipedia.org/wiki/Katz_v._United_States
The Court's ruling refined previous interpretations of the unreasonable "search and seizure" clause of the Fourth Amendment to count ***immaterial intrusion with technology as a search***

(9)
http://www.uscourts.gov/educational-resources/get-involved/constitution-activities/fourth-amendment/wiretaps-cell-phone-surveillance/facts-case-summary.aspx

Although he agreed with the majority opinion of the Court, Justice Harlan went further to provide a test for what is a constitutionally protected search. He said it was necessary to clarify when private actions, conducted in a public place, may be constitutionally protected. Expanding upon the general principles enunciated by the majority opinion, Justice Harlan proposed the following two-pronged test to address this issue: "My understanding of the rule that has emerged from prior judicial decisions is that there is a twofold requirement, ***first that a person have exhibited an actual (subjective) expectation of privacy; and second, that the expectation be one that society is prepared to recognize as 'reasonable.'"***
