



February 3, 2017

**VIA E-MAIL ONLY**

Hon. Desley Brooks (dbrooks@oaklandnet.com)  
Hon. Annie Campbell Washington (acampbellwashington@oaklandnet.com)  
Hon. Noel Gallo (ngallo@oaklandnet.com)  
Hon. Lynette Gibson McElhaney (lmcElhaney@oaklandnet.com)  
Hon. Abel Guillen (aguillen@oaklandnet.com)  
Hon. Dan Kalb (dkalb@oaklandnet.com)  
Hon. Rebecca Kaplan (atlarge@oaklandnet.com)  
Hon. Larry Reid (lreid@oaklandnet.com)  
Oakland City Council  
1 Frank H. Ogawa Plaza  
Oakland, CA 94612

Re: Cell Site Simulator Policy

Dear Honorable Members of the Oakland City Council:

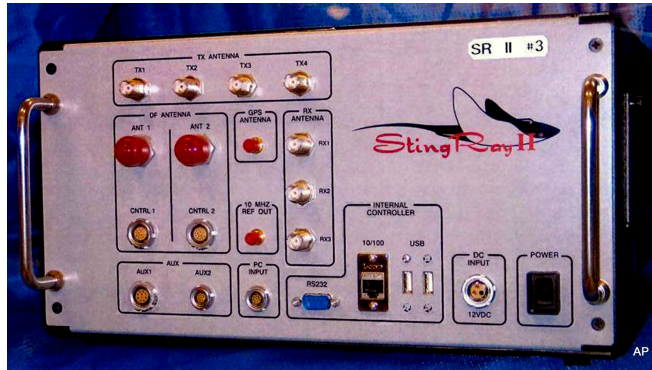
I write to comment on the proposed cell-site simulator policy proposal before you on February 7, 2017. The Privacy Advisory Commission approved the policy by unanimous vote. The Public Safety Committee approved the policy by unanimous vote on January 24, 2017. The following comments are my own.

As a reminder, myself and other members of Oakland Privacy threatened to sue the city over the Domain Awareness Center. Today, I still believe a cell site simulator, or Stingray as its commonly known, is the most controversial device known to us in use by municipal police. I want to share how I got to a comfort level with this policy, and describe to you what a Stingray is and can do. I apologize for not briefing Public Safety beforehand, but my day job got a bit hectic prior to January 24.

***What Is A Stingray, and How Will It Be Used?***

A Stingray mimics a cellphone tower, and causes phones within range to connect to it. Cellphones are constantly searching for towers, and Stingrays exploit this weakness (or feature, depending on how you look at it), by sending out the strongest signal to “capture” your phone.

During this process of “catch and release”, a unique identifier on all our phones is received by the Stingray (IMSI – International Mobile Subscriber Identity).



A Stingray can capture all IMSI codes in range, in a dragnet feature called Registration Mode. Per the policy before you, this mode may only be used in a natural disaster search and rescue scenario, when a Stingray might be used to locate victims trapped in a collapsed building during an earthquake, for but one example.

The second, more common “catch and release” mode, will be always pursuant to a warrant, and only initiated when law enforcement already knows the IMSI code it is looking for (the dragnet feature cannot be used to generate IMSI codes for future law enforcement purposes). The software is programmed to scan the available IMSI codes in range, and it automatically discards the codes it is not looking for. No retention of IMSI codes in either mode is allowable under our policy.

The device, along with a power amplifier and antennas to extend the range (the signal can penetrate walls, and has a range perhaps up to 1 mile), is mounted in the back of a pickup truck. Once the IMSI code is located, the truck drives around the general location, narrowing down the range, until more certainty as to the phone’s exact location is known. Presumably the next step would be an arrest (if the suspect is with the phone), or simply location of the phone if it has been dumped.

Stingrays are connected to laptops, and paired with various software. The software capabilities are where most of our concerns arise. When paired with certain software, a Stingray can intercept the communications (voice, text, images) from all phones within its range. Both Federal, State, and our own policy prohibit this capability.

### ***Why Is Oakland’s Policy The New Gold Standard?***

There is no policy regarding cell site simulators in existence even remotely close to Oakland’s, as to the narrowness of allowable use, oversight, and transparent reporting. Although I was proud of what we accomplished with Alameda County in breaking new ground, the Oakland policy far exceeds all standards at the federal, state, or local level:

1. Content interception is prohibited.
2. A warrant for each use. The warrant application must inform the Court of the technology being used, and how it operates. This was previously not done, leading to judicial authorization of something unknown to them.
3. A deployment log, containing the name of each user, the reason for each use, and the results of each use, including accuracy of information.
4. An annual report that includes:
  - a. The deployment log
  - b. The number of times the equipment was requested and used.
  - c. The number of times outside agencies received info from OPD and vice versa.
  - d. Information regarding any policy violations.
  - e. Total costs.
  - f. Results of internal audits, and any corrective action taken.
  - g. The number of times the equipment was used to make or attempt an arrest; locate an at-risk person; aid in search and rescue efforts. These are the narrow, allowable uses.
  - h. The type of crime.
  - i. The effective in assisting in investigations.
  - j. Location of use

This annual report will come to both the Privacy Advisory Commission and the Council, and for the first time provide for informed decision making. The Oakland City Council has not previously approved acquisition or use of Stingrays in Oakland. OPD obtained its own Stingray at least as early as 2007 (we no longer possess this outdated device). The annual report submission to Council, and establishment of the Privacy Commission, now provides for true oversight of this controversial device, as each use will be examined going forward.

There is only one of these devices (the new upgraded model is called Hailstorm, and used because most phones are now on 4G networks) in Alameda County. Each use has three levels of oversight required due to the shared nature of the Stingray, owned by Alameda County. First, OPD Chief or Assistant Chief approval must be given, next OPD must seek Alameda County District Attorney approval, and finally Judicial authorization must be granted by approving the warrant application.

Furthermore, and this was key to my own vote – there is no Non-Disclosure Agreement for either Alameda County or OPD. Previously, the FBI required that an entity enter an NDA to acquire and use the equipment. The existence of the NDA, clearly inappropriate, led to terrible results in criminal matters, as prosecutors both voluntarily and involuntarily dropped serious charges (including homicide) during trials, rather than reveal the technology to the courts or defense attorneys.

As to frequency of use, keeping in mind the shared nature of this single device for the county, in the past we have some guidance as to how OPD used their own Stingray. In at least 2007-2009, OPD released summary information in the annual CID reports, such as this 2009 report example:

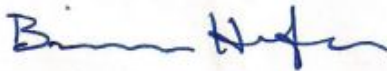
**Stingray Operations/ESU Arrests**

- Nine (9) subjects wanted for 187 PC
- Three (3) subjects wanted for 664/187 PC
- Two (2) subjects wanted for 245(a)(2) PC (ADW shooting)
- Four (4) subjects wanted for 211 PC
- One (1) subject wanted for 207 PC (kidnapping)
- One (1) subject wanted for 136.1(c)(1) PC (intimidation of a witness)

Use has been sparing and reserved for serious penal code violations, and I expect that this will remain the trend. However, we have some egregious examples of abuse, such as by the Baltimore Police Department, which has admitted in court documents to using a Stingray at least 4,300 times, including for searching for a suspect involved in the petty theft of \$50. Our annual report metrics will be key to reigning in the use of this controversial device, which when used narrowly and pursuant to our policy, can be used legitimately.

The good-faith efforts of OPD, especially Tim Burch and Deputy Chief Darren Allison, who sat through three hours of cross-examination by the Commission and three months of meetings, and robust reporting metrics, have raised the floor for what is possible regarding cell site simulator oversight and transparency reporting. If this policy is adopted, Oakland will again lead the nation in true, systemic reform of surveillance equipment use.

Sincerely,



Brian Hofer  
Member, Oakland Privacy Working Group  
Chair, City of Oakland's Privacy Advisory Commission

cc: tburch@oaklandnet.com; jdevries@oaklandnet.com