VIA EMAIL ONLY

November 5, 2015

Hon. Scott Haggerty (scott.haggerty@acgov.org)
Hon. Wilma Chan (wilma.chan@acgov.org)
Hon. Nate Miley (nate.miley@acgov.org)
Hon. Keith Carson (keith.carson@acgov.org)
Hon. Richard Valle (richard.valle@acgov.org)
Alameda County
1221 Oak St., Suite 536
Oakland, CA 94612

Re: District Attorney Draft Stingray Use Policy

Dear Hon. Supervisors:

I write to comment on the proposed Stingray use policy as drafted by District Attorney Nancy O'Malley's office. While a commendable first draft, the policy has serious shortcomings, ambiguities, and is in conflict with itself.

The Board should not let the possibility of lost UASI funds force it into making a hasty decision on an insufficient policy. The Oakland Domain Awareness Center was funded by UASI, and received or reprogrammed monies for thirteen grant rounds from 2008 to 2015. The Phase II contract, the main focus of my own personal involvement, had its deadline extended from May 2014 to August 2015. The money will be there.

1. Limitations on use

The policy claims in the first paragraph that the Stingray will "only be utilized when authorized by a search warrant…" This is not true as the policy is currently written, as express allowances have been created for use in natural disaster and search and rescue scenarios[1]. In these scenarios, a warrant will not issue as there is no suspicion of criminal wrong doing. It is not illegal to get lost in the woods. Secondly, the District Attorney is not involved in search and rescue matters, in the traditional sense (absent suspected kidnapping). I again recommend further discussion as to the appropriate uses of this equipment, as it is clear that a firm vision is still not in place (warrant vs. no warrant; restricted to crime fighting vs. unrestricted use).

The lack of specific allowable uses is the policy's biggest weakness. If the 4th Amendment and right to privacy are to be infringed upon, the allowable uses must be limited, substantive in nature, and enumerated in the policy to prevent mission creep.

[1] It also appears an allowance for exigent use has been created, discussed further below.

To see an example of such a policy provision, please see the attached FLIR (thermal imaging camera used by OPD's helicopter) policy, Section VI A. "Allowable Uses." The committee I chaired sat down with OPD's helicopter pilot team and quizzed them on anticipated uses. We found it is much better to enumerate how surveillance equipment can be used, than to prohibit and try to anticipate inappropriate uses.

If a tool isn't regulated, it will be used frequently. We have only to look to the Baltimore Police Department for a real world example of unregulated Stingray use. They have admitted in Court to using a Stingray at least 4,400 times, for petty theft, recovery of a stolen phone, recovery of a stolen laptop, and very minor drug deals, among more significant uses.[2] The department's concealment of its Stingray use has resulted in criminal charges against multiple defendants being dropped at trial, and evidence excluded necessary for conviction.

2. Basic Uses

On October 13, 2015, the District Attorney represented to the Board during its deliberation that her office would have sole custody of the Stingray, and only her investigators would operate it. This conflicts with the policy in multiple paragraphs.[3]

Furthermore, the requirement that a warrant be obtained in most situations is not a high hurdle for an office that prolifically issues warrants and where use is not restricted. The District Attorney lacks the ability to track warrants its office issues, and how often it has authorized Stingray use in the past. This is not reassuring, and the draft policy does not address these problems. The public will gain no assurances as to the hopefully limited use of this controversial equipment if the policy remains as is.

In her September 2014 response to my public record requests regarding Stingray, the District Attorney produced only the grant application and withheld all other documents[4]. Of note, she informed me that they "do not track or distinguish those cases that involve any particular type of law enforcement technique or arrest, including Stingray Technology. This Office has processed more than 300,000 referrals from Police Agencies in the time period you refer to, and there is no practical means of retrieving that information if it is in our possession at all."[5] This again gets back to my main concern – that while the policy may state the Stingray "will only be deployed in a fraction of cases," the District Attorney has not implemented any controls to make this true,

---

[2] http://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/

[3] *What They Do and Do Not Obtain* – "cell site simulators used by the District Attorney's Office and any authorized law enforcement agency…"; Section II 1. "The District Attorney's office, and any authorized law enforcement personnel with access to the simulator…"; Section VII "Every law enforcement agency requesting use of the cell-site simulator…"

[4] The 2013 UASI grant application submitted by the District Attorney indicates a deeper understanding of the technology than was represented to the Board on October 13, 2015: "the Alameda County District Attorney's Office is requesting the purchase of a full intercept system manufactured by Pen-Link. This equipment is capable of capturing incoming and outgoing phone numbers, along with the duration of calls…" Pg. 2, 1.e. Project Description. Pen-Link is the third-party software possessed by OPD and referenced in my previous letter.

[5] September 5, 2014 District Attorney Nancy O'Malley response to Hofer CPRA

and without limited enumerated uses imposed by the Board, Alameda County will do as Baltimore has done.

3. What They Do and Do Not Obtain

The use of "will not", "will be", and "do not" must be replaced in each instance in this paragraph by "shall not" or "shall be" as appropriate. Stating that a Stingray will not be used to intercept content is not a prohibition, e.g. "shall not be used to collect the contents of any communication…", and "this identifying information shall be limited." The US DOJ's policy uses "may not."[6]

4. Management Controls, Authorization for Use, and Accountability

It is unclear who will do the training and supervision referenced in Section II 1. If the District Attorney's office is to have sole custody and supervision of the equipment, the policy needs to reflect this throughout.

Any memorandum of understanding entered into pursuant to this Section should be made public as part of an annual report, discussed further below. Transparency can help dispel suspicion about this very controversial equipment.[7]

In the third paragraph, it appears that an allowance for use of a Stingray in exigent circumstances has been created[8]. On October 13, 2015, the District Attorney represented to the Board and specifically to Sup. Miley that she would require a warrant in all circumstances. This paragraph needs to be modified to make clear the prohibition on exigent use of a Stingray.

The final sentence in this section should be amended to clarify that training will occur prior to use of the Stingray. In addition, the US DOJ's revised policy requires that each agency identify its training protocols. It would be wise to do so here as well.

---

[6] "Moreover, cell-site simulators used by the Department must be configured as pen registers, and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3)." DOJ Cell-Site Simulator Policy 9-3-15.

[7] The District Attorney's refusal to produce any documents except for the grant application is a good example of why transparency is needed. While the refusal to produce was perhaps lawful as to certain categories requested, disclosure is not prohibited under the Public Record Act, but rather discretionary. The Board should be encouraged to be as transparent as possible due to the intrusiveness of this equipment. See attached FLIR Policy Section X for sample language regarding public record requests.

[8] "Any emergency use of a cell-site simulator must be approved by a Lieutenant of Inspectors or above." Draft policy, Section II 3.

5. Applications For Use Of Cell-Site Simulators

Section IV 2 requires that an application inform the court that "all operations will be conducted to ensure the minimal amount of interference to non-target devices." The policy should provide guidance on how this is to be done, here or above in Section II.

Section IV 3 is legally problematic, and appears to endorse the concept of a general warrant as to possible future use of "any non-target data." A warrant must be particularized, and any non-target data scooped up in the dragnet phase of Stingray use is not authorized pursuant to a warrant searching for something else. The current language does not comply with our constitutional right to privacy, nor long standing due process rules. This is a grave concern. As a practical matter, this provision also conflicts with Section V 1, which requires the immediate deletion of all data as soon as the target device is located.

6. Audits, Monitoring, Data Collection, And Disposal

Section V 1 addresses data deletion when a Stingray is used to locate a known cellular device, but is silent on deletion when locating an unknown device. The US DOJ policy addresses both, requiring that in both scenarios, "all data must be deleted as soon as" either the known device is located, or the previously unknown target device is identified. If the Board determines that the initial dragnet use of a Stingray is appropriate, it must ensure that non-target data is immediately deleted. Challenges to Stingray use are slowly working their way through the Court system, and Alameda County taxpayers do not need to incur legal fees for unlawful use of surveillance equipment.

The second paragraph in this section provides no justification as to retaining data for up to ten days in a search and rescue or natural disaster scenario. Absent reasonable justification, the retention limit should match the other provisions, and require daily deletion of data. As the policy acknowledges, third party data will be collected by the Stingray in this scenario. Retaining it for up to ten days is unacceptable, creates the opportunity for a general warrant, and is a gross invasion of privacy.

While we strongly encourage audits to take place, they are somewhat meaningless if not presented to the public. Audits should be made part of an annual public report on Stingray use and efficacy. See Section VII D in the attached FLIR policy as to the information an annual report should include.

7. Policy Application

Section VI states that the policy applies to all instances in which the District Attorney's office uses the Stingray, but is silent as to other law enforcement agencies.

Section VII states that other authorized law enforcement agencies using the Stingray "shall provide the Policy" to all relevant employees. This language should be clarified to state that all law enforcement agencies "shall abide by the Policy".

8. Enforcement

A policy is reduced to a mere collection of words that can be ignored if there is no enforcement mechanism. The District Attorney's apparent abandonment of sole custody and operation of the Stingray in a mere matter of weeks shows how quickly this Policy can become something other than what was originally intended. Without enforcement by a third party, we can only rely on individual actors to voluntarily comply with its provisions. This policy should be turned into an enforceable ordinance by the Board. Enforcement builds trust, and lends credibility that this controversial equipment will be used lawfully.

Sincerely,

Brian Hofer
Member, Oakland Privacy Working Group
Chair, Oakland Domain Awareness Center ad hoc privacy committee

CC: District Attorney Nancy O'Malley (nancy.omalley@acgov.org)

Encl: FLIR use policy - Oakland

Alameda County District Attorney's Policy for Use of Cell-Site Simulator Technology

Cell-site simulator technology provides valuable assistance in support of important public safety objectives. Whether deployed as part of a fugitive apprehension effort, to locate at-risk people or missing children, or to provide search and rescue support in natural disasters and emergencies, cell-site simulators fulfill critical operational needs. This technology will only be utilized when authorized by a search warrant signed by a judicial officer that has been reviewed through the judicial process.

As with any law enforcement capability, the Alameda County District Attorney's Office (the District Attorney's Office") must use cell-site simulators in a manner that is consistent with the requirements and protections of the Constitution, including the Fourth Amendment, and applicable statutory authorities, including the Pen Register Statute and Government Code Section 53166 (Senate Bill 741, Acts 2015). Moreover, any information resulting from the use of cell-site simulators must be handled in a way that is consistent with the array of applicable statutes, regulations, and policies that guide law enforcement in how it may and may not collect, retain, and disclose data.

As technology evolves, the District Attorney's Office must continue to assess its tools to ensure that practice and applicable policies reflect the District Attorney's Office's law enforcement and public safety missions, as well as the District Attorney's Office's commitment to uphold every individuals' privacy and civil liberties. The District Attorney's Policy for Use of Cell-Site Simulator Technology (the "Policy") provides additional guidance and establishes common principles for the use of cell-site simulators and privacy protections for the information gathered.

I. BACKGROUND

Cell-site simulators have been the subject of misperception and confusion. This section provides information about how the District Attorney's Office intends to use the equipment and defines the capabilities that are the subject of this Policy.

Basic Uses

The District Attorney's Office shall maintain custody and control of the cell-site simulator technology as set out herein and oversee all requested uses of that technology in order to ensure full compliance with this Policy, as well as state and federal law. Law enforcement agents can request use of cell-site simulators to help locate cellular devices whose unique identifiers are already known to law enforcement. This technology will only be utilized for this purpose when authorized by a search warrant signed by a judicial officer that has been reviewed through the judicial process.

The District Attorney's Office may also use the cell-site simulator technology in the wake of a natural disaster or an emergency, where the ability to locate a victim's cell phone can assist first responders to narrow the area of search, locate victims and render aid in the shortest possible time frame. All such uses of this technology would be in compliance with state and federal law.

Cell-site simulator technology is but one tool among many traditional law enforcement techniques, and will only be deployed in a fraction of cases in which the technology is best suited to achieve specific public safety objectives.

How They Function

Cell-site simulators, as governed by this Policy, will function by transmitting as a cell tower. In response to the signals emitted by the simulator, cellular devices in the proximity of the simulator identify it as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would with a networked tower.

A cell-site simulator will receive these signals and use an industry standard unique identifying number assigned by a device manufacturer or cellular network provider to distinguish between incoming signals until the targeted device is located. Once the cell-site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular phone, rejecting all others. Although the cell-site

simulator initially receives signals from multiple devices in the vicinity of the simulator while attempting to locate the target device, it does not display the unique identifying numbers of those other devices for the operator. Any identifying information regarding the non-targeted devices, to the extent that it might exist in the simulator memory, will be purged at the conclusion of operations in accordance with Section V. of this Policy.

When used in a natural disaster or emergency situation, or to aid search and rescue efforts, the cell-site simulator will obtain signaling information from all devices in the simulator's target vicinity for the limited purpose of locating persons in need of assistance or to further recovery efforts. Any identifying information received from the cellular devices during this time will only be used for these limited purposes and all such information received will be purged at the conclusion of the effort in accordance with section V. of this Policy.

What They Do and Do Not Obtain – The Authorized Purposes of the District Attorney's Use of a Cell-Site Simulator

By transmitting as a cell tower, cell-site simulators acquire the identifying information from cellular devices. As employed by the District Attorney's Office, this identifying information will be limited. Cell-site simulators will provide only the relative signal strength and general direction of a subject cellular telephone. They will not function as a GPS locator, as they will not obtain or download any location information from the device or its applications. Moreover, cell-site simulators used by the District Attorney's Office and any authorized law enforcement agency will be configured as pen registers, and will not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3). This limitation will be made an express part of any search warrant sought by the District Attorney's Office. The simulator will not remotely capture emails, texts, contact lists, images or any other data contained on the phone. In addition, the District Attorney's Office cell-site simulators do not collect subscriber account information *(for example, an account holder's name, address, or telephone number).*

II. MANAGEMENT CONTROLS, AUTHORIZATION FOR USE, AND ACCOUNTABILITY

Cell-site simulators require training and practice to operate correctly. To that end, the following management controls and approval processes will help ensure that only knowledgeable and accountable personnel will use the technology.

1. The District Attorney's Office, and any authorized law enforcement personnel with access to the simulator in accordance with this Policy, will be trained and supervised appropriately. All such law enforcement personnel shall be sworn peace officers as defined in California Penal Code section 830.1. Cell-site simulators will be operated only by personnel who have been authorized by the District Attorney's Office to use the technology and who have been trained by a qualified agency component or expert.

2. To the extent the District Attorney's Office shares the information collected through a cell-site simulator with another local agency or other party, such local agency or other party will enter into a memorandum of understanding or other agreement (MOU) with the District Attorney's Office regarding the uses and restrictions from sharing information, including the purposes of, processes for, and limitations from sharing information. The terms of each MOU will be consistent with the Policy.

3. Prior to deployment of the technology, use of a cell-site simulator by the District Attorney's Office must be approved by the Chief of Inspectors or the Assistant Chief of Inspectors. Any emergency use of a cell-site simulator must be approved by a Lieutenant of Inspectors or above.

This Policy will include training on privacy and civil liberties under state and federal law.

III. LEGAL PROCESS AND SEARCH WARRANTS

The use of cell-site simulators will be permitted only as authorized by this Policy and pursuant to a search warrant signed by a judicial officer.

Law enforcement officers seeking to use cell-site simulators must either: (1) obtain a warrant that contains all information required to be included in a pen register order pursuant to 18 U.S.C. § 3123 (or the state equivalent); or (2) seek a warrant and a pen register order concurrently. The search warrant affidavit also must reflect the information noted in Section IV of this Policy ("Applications for Use of Cell-Site Simulators").

IV. APPLICATIONS FOR USE OF CELL-SITE SIMULATORS

When making any application to a court, members of the District Attorney's Office and law enforcement officers must disclose appropriately and accurately the underlying purpose and activities for which an order or authorization is sought. Law enforcement officers must consult with prosecutors in advance of using a cell-site simulator, and applications for the use of a cell-site simulator must include sufficient information to ensure that the courts are aware that the technology may be used.

1. Regardless of the legal authority relied upon, at the time of making an application for use of a cell-site simulator, the application or supporting affidavit should describe in general terms the technique to be employed. The description should indicate that investigators plan to send signals to the cellular phone that will cause it, and non-target phones on the same provider network in close physical proximity, to emit unique identifiers, which will be obtained by the technology, and that investigators will use the information collected to determine information pertaining to the physical location of the target cellular device or to determine the currently unknown identifiers of the target device. If investigators will use the equipment to determine unique identifiers at multiple locations and/or multiple times at the same location, the application should indicate this also.

2. An application or supporting affidavit should inform the court that the target cellular device (e.g., cell phone) and other cellular devices in the area might experience a temporary disruption of service from the service provider. The application may also note, if accurate, that any potential service disruption to non-target devices would be temporary and all operations will be conducted to ensure the minimal amount of interference to non-target devices.

3. An application for the use of a cell-site simulator should inform the court about how law enforcement intends to address deletion of data not associated with the target phone. The application should also indicate that law enforcement will make no affirmative use of any non-target data absent further order of the court, except to identify and distinguish the target device from other devices.

V. AUDITS, MONITORING, DATA COLLECTION, AND DISPOSAL

The District Attorney's Office is committed to ensuring that law enforcement practices concerning the collection or retention of data are lawful, and appropriately respect the important privacy interests of individuals. As part of this commitment, the District Attorney's Office will operate in accordance with rules, policies, and laws that control the collection, retention, dissemination, and disposition of records that contain personal identifying information. As with data collected in the course of any investigation, these authorities apply to information collected through the use of a cell-site simulator. Consistent with applicable existing laws and requirements, including any duty to preserve exculpatory evidence, the District Attorney's Office's use of cell-site simulators shall include the following privacy practices:

1. When the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is located and no less than once daily.

2. When the equipment is used following a disaster, or in a search and rescue context, all data must be deleted as soon as the person or persons in need of assistance have been located, and in any event no less than once every ten (10) days.

3. Prior to deploying equipment for another mission, the operator must verify that the equipment has been cleared of any previous operational data.

The District Attorney's Office shall implement an auditing program to ensure that the data is deleted in the manner described above. This audit shall take place not less than once every six (6) months.

VI. FEDERAL STATE AND LOCAL PARTNERS

The District Attorney's Office often works closely with its Federal, State or Local law enforcement partners and provides technological assistance under a variety of circumstances. This policy applies to all instances in which the District Attorney's Office use cell- site simulators in support of other Federal, State or Local law enforcement agencies. As noted above, to the extent the District Attorney's Office shares the information collected through a cell-site simulator with another local agency or other party, such local agency or other party shall enter into a MOU with the District Attorney's Office regarding the uses and restrictions from sharing information, including the purposes of, processes for, and limitations from sharing information.

VII. TRAINING AND COORDINATION, AND ONGOING MANAGEMENT

Accountability is an essential element in maintaining the integrity of the use of this technology by the District Attorney's Office. Every law enforcement agency requesting use of the cell-site simulator shall provide this Policy and training, as appropriate, to all relevant employees who would be involved in the use of this technology. Periodic review of this Policy and training shall be the responsibility of the Assistant Chief of Inspectors with respect to the way the equipment is being used (e.g., significant advances in technological capabilities, the kind of data collected, or the manner in which it is collected). Officers will familiarize themselves with this Policy and comply with all orders concerning the use of this technology. Moreover, as the law in this area evolves, this Policy will be amended to reflect the current state of the law.

It is vital that all Deputy District Attorneys familiarize themselves with the contents of this Policy, so that their court filings and representations are accurate and consistent with both the intent and scope of this Policy.

VIII. CONCLUSION

Cell-site simulator technology significantly enhances the Alameda County District Attorney's Office's efforts to achieve its public safety and law enforcement objectives. As with other capabilities, the District Attorney's Office must always use this technology in a manner that is consistent with the Constitution and all other legal authorities. This policy provides additional principles and guidance to ensure that the District Attorney's Office deploys the cell-site simulator in an effective and appropriate manner consistent with authorizing law.