November 6, 2015

District Attorney Nancy E. O'Malley
Alameda County District Attorney's Office
1225 Fallon Street
Oakland, CA 94612

Re: Draft Policy for the Use of Cell-Site Simulator Technology

District Attorney O'Malley,

We have reviewed your draft Policy for the Use of Cell-Site Simulator Technology ("Policy") publicly released by your office on November 3, 2015. Cell-Site Simulator Technology, commonly marketed as devices called Stingrays, are a surveillance technology capable of intercepting information not only from a target cell phone but also from nearby phones that have nothing to do with any investigation. As such, it is important that this technology is governed by a narrow and clearly-drafted policy. We thank you for publicly releasing this draft in advance of the next meeting of the Board of Supervisors and for soliciting feedback.

What follows are the ACLU's suggestions to ensure this policy protects civil liberties and gives clear guidance to law enforcement. While we still think there are potentially significant Fourth Amendment concerns even under this Policy, this Policy with our suggested changes incorporated would be a major step in the right direction and mitigates a number of the concerns we have with warrantless Stingray use.

We look forward to seeing our suggestions incorporated into the Policy, and we encourage Alameda County to consider legislative solutions that can ensure that transparency, accountability, and oversight are the rule rather than the exception for all proposed surveillance technologies. The county should have consistent mechanisms in place to ensure transparent public processes, informed debate, and adoption of enforceable policies when this, or any other surveillance technology, is considered.[1]

1. **The Policy Should Strictly Limit When the Stingray May Be Used**

The Policy should specify exactly when the Stingray may be used to eliminate the possibility that it might be deployed in ways that citizens and public officials do not expect. As written, the Policy in various places states that the Stingray shall be used to apprehend fugitives or criminal

[1] For more information and a model ordinance designed to operationalize these processes, please see the ACLU of California's report, *Making Smart Decisions About Surveillance: A Guide for Communities*, *available at* https://www.aclunc.org/publications/making-smart-decisions-about-surveillance-guide-communities.

suspects, to locate at-risk people or missing children, in disasters and emergencies, and to provide search and rescue support. However, while the Policy discusses circumstances when the device *may* be used, it does not state that it *will not* be used for any other purpose. In addition, the terminology used in the Policy to describe these allowable uses is inconsistent and lacks specific protections to prevent the Stingray's use to investigate minor crimes or even monitor First Amendment-protected activities.

The Policy should therefore explicitly list the specific purposes for which this Stingray may be used, and should clarify that the allowable uses listed in the Policy are an exhaustive list (e.g., "The Stingray *shall only* be used as follows:"). Because of the potential to interfere with or intercept information from nearby cell phones, Stingrays should only be used in criminal investigations of serious or violent felonies. And to comply with the newly-enacted California Electronic Communications Privacy Act (S.B. 178 (2015)) (CalECPA), Stingrays should only be used in natural disasters or other emergencies if there is a risk of death or serious injury.[2] The Policy should include a definition of "emergency situation" that reflects this legal requirement.

In addition, the Policy should provide specific limitations on the use of the Stingray. The Stingray should be used only where there is no less intrusive means of obtaining the necessary information. It should also explicitly prohibit monitoring of conduct protected by the First Amendment, including public demonstrations and religious activities.

Finally, we remain concerned of the potential disruption to cellular service that the use of a Stingray may create. Citizens rely on cellular service to call police and fire departments, communicate private and public information, and connect with loved ones. The disruption of cellular service due to Stingray usage prevents these actions, risks exacerbating the effects of an emergency and the undermining of public safety objectives. The Policy acknowledges such disruptions may occur and requires that a warrant application reveal whether such disruption may occur. It should also require that any use of the Stingray be narrowly tailored to limit disruption of communication services.

2. The Policy Should Clearly State How the Stingray Will be Used

There is also a lack of clarity about how this device will be used. The Policy describes three different methods by which the Stingray may be used. Two of these uses are described under "Basic Uses" (p. 2): to locate a target device whose identifier is known to the government, and to locate (potentially unknown) victims in the wake of an emergency (for example, to identify and locate individuals in a building during a fire). Although not expressly referenced in the Policy's section on allowable uses, the Policy elsewhere suggests that the Stingray may be used in a third manner: "to determine the currently unknown identifiers of the target device" (p.6).

We understand this to mean that your Office intends to use the Stingray to obtain the unique numeric identifier associated with the device of a specific target of an investigation. If that is so, then this use should also be expressly identified in the allowable uses section of the Policy. If your Office does not contemplate using a Stingray to identify the unique numeric identifier of a

[2] SB 178 (2015), the California Electronic Communications Privacy Act [hereinafter "CalECPA"], *available at* https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB17, at § 1546.1(c)(5).

target phone, then it should remove the reference to this use on page 6 (and elsewhere in the policy).

3. The Policy Should Clarify the Legal Process Required Before or After Using the Stingray

The Policy appropriately requires a search warrant to use a Stingray under ordinary circumstances. CalECPA will establish such a requirement effective January 1, 2016. We applaud the Policy's inclusion of a warrant requirement in advance of CalECPA's effective date, coupled with the affirmative steps the Policy contains to ensure candor to the judiciary.

However, as written, the Policy suggests that a warrant will be obtained even in emergency circumstances. We believe this is an oversight. What follows are suggestions for amending the Policy to clarify the legal process that will be followed in emergencies. In addition, we ask that more information be provided about how your Office obtains device information from cellular carriers for use with the Stingray.

a. Describe an explicit process for emergency use

The Policy should clarify the process that the government will follow for emergency uses of Stingrays. We recognize that, in a narrow set of emergency circumstances, obtaining a warrant may be impossible because evidence of a crime is not sought or preventing death or serious bodily injury requires obtaining information without delay (for example, when the device is used to locate a person in a burning building). Yet currently Section III of the Policy states that the Stingray will be used *only* pursuant to a warrant.

If this is not the intention, the Policy should make that clear. It should also specify the process that will be followed in the event of an emergency use, including the individual(s) who have the authority to approve Stingray use in an emergency situation.

b. Describe the process for complying with CalECPA following an emergency

CalECPA imposes specific process requirements on warrantless use of Stingrays (or obtaining electronic information by other means) in emergency circumstances. Specifically, CalECPA requires a petition before a court seeking judicial affirmation of the emergency circumstances or retroactive approval of a warrant authorizing the information to be obtained.[3] The Policy should explain to the public that this process will be followed whenever information is obtained through warrantless use of the Stingray in emergencies.

c. Describe the process for obtaining information from cellular carriers

The Policy describes how a Stingray will be used "to help locate cellular devices whose unique identifiers are already known to law enforcement," but does not specify how those identifiers will be obtained. One way by which the government can learn a particular device's unique identifier is by requesting it from the relevant cellular carrier for that device. The Policy does not explain your Office's process for requesting this information. We ask that you describe in the Policy the process by which unique identifiers and other information is sought from cellular

[3] *Id.* at § 1546.1(h).

carriers, clarify the specific information your Office requests from carriers, and state that such information will only be sought with a warrant.

4. The Policy Should Describe How You Will Notify Affected Individuals

a. Describe the process for providing notice to targets and the public

The Policy should also address how your Office will provide notice to persons whose information is collected by the Stingray. Under CalECPA, the government is required to provide notice to individuals or file a report with the California Department of Justice, depending on how the Stingray is used. Specifically, the government must provide contemporaneous notice to the "identified targets" of any warrant or emergency use that must contain particular information about the nature of the investigation under which information is sought, unless the court has granted the government's request to delay notice.[4] If there is no identified target of a warrant or emergency request, the government must submit to the California Department of Justice all the above information within three days unless the court has granted the government's request to delay such notification.[5] Your procedures for complying with the above CalECPA notice requirements should be described clearly in this Policy.

b. Describe the process for providing notice to criminal defendants

In addition to describing how notice will be provided under CalECPA for persons subject to Stingray surveillance, the Policy should address the rights of criminal defendants. In other jurisdictions, the ACLU and journalists have revealed efforts by law enforcement to withhold such information from criminal defendants in possible violation of the Due Process Clause of the Fourteenth Amendment.[6] To reassure the public that no such information is withheld from criminal defendants in Alameda County, we recommend that the Policy specifically state that you will provide criminal defendants with information as required by law.[7] Such a statement would complement the Policy's overarching intent of providing transparency to both the public and the judiciary about the use of this device.

5. The Policy Should Require Annual Reporting to Promote Transparency

Members of the public should be able to access information about how the Stingray is used. With this information, the public and elected leaders can decide whether the public safety benefit provided by the Stingray outweigh fiscal and civil liberties costs. To provide the public with this information, we suggest adding the following provision to the Policy, which is based on a similar

---

[4] *Id.* at § 1546.2(a)-(b).
[5] *Id.* at § 1546.2 (c).
[6] *See, e.g.*, Justin Fenton, *Legal challenge alleges authorities withhold police use of stingray surveillance*, THE BALTIMORE SUN, Sept. 4, 2015, *available at* http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-challenge-20150904-story.html; Fred Clasen-Kelly, *Secrecy lifts in CMPD StingRay phone tracking*, THE CHARLOTTE OBSERVER, Feb. 15, 2015, *available at* http://www.charlotteobserver.com/latest-news/article10435436.html ("Defense attorneys said they did not know details about [the Charlotte-Mecklenburg Police Department's] cellphone surveillance until an Observer investigation.").
[7] *See Brady v. Maryland*, 373 U.S. 83 (1963).

provision found within the U.S. Department of Justice Policy Guidance on Cell-Site Simulator Technology:

> The District Attorney shall report to the Board of Supervisors on an annual basis records reflecting the total number of times a cell-site simulator is deployed in Alameda County; the number of deployments at the request of other agencies, including State or Local law enforcement; the number of times the technology is deployed in emergency circumstances; and the purpose for each use.[8]

The above information should be collected and affirmatively disclosed to the public by your Office no less than once a year, and shall be made available to the public on your website or via other means as well.

6. The Policy Should Be Additionally Amended to Protect Civil Liberties as Follows

We also suggest the following edits be made to the Policy. In the following bulleted paragraphs, we designate additional suggested language in **bold text** and suggested deletions in ~~strikethrough text~~.

- Data collected about innocent persons not suspected of any crime should *never* be used for investigatory purposes and should certainly not be used based on a *post hoc* justification to a court. Thus, we suggest the following edit at Section IV (p. 6): 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."

- At Section II (page 4), we ask that you clarify that the limitations on sharing with entities outside the District Attorney's office apply to *all* outside parties: "To the extent the District Attorney's Office shares the information collected through a cell-site similar with **any third party** ~~another local agency or other party~~…"

- The term "identifying information" appears throughout the Policy. This term is commonly understood to mean a device's unique numeric identifier, such as its electronic serial number or international mobile subscriber identity number. However, Stingrays also collect additional information, including information related to the location of a phone that is *not* typically referred to as "identifying information." To ensure that this information is also protected, the Policy should use the term "information" instead of "identifying information" wherever it is found in the Policy. Absent such a change, the privacy-protecting provisions of the Policy – such as those pertaining to deletion – will be significantly *less* privacy protective than we understand to be your intent, and we would have greater concerns about the Policy.

7. The Policy Should Be Enforceable to Ensure It Is Followed

[8] Department of Justice, Policy Guidance: Use of Cell-Site Simulator Technology, *available at* http://www.justice.gov/opa/file/767321/download.

This Policy should include provisions that ensure it is enforceable. It is necessary to add specific and strong enforcement mechanisms to the Policy to ensure its provisions obeyed and that individuals that act in violation of the Policy face consequences. In addition, while the Policy already mandates that any law enforcement partners that your Office supports with the Stingray must agree to abide by this Policy, it should spell out consequences including immediate termination of such cooperation if partner agencies violate this Policy.

8. The Policy Should Ensure Public Participation in Any Future Amendments

Finally, the Policy should also include provisions anticipating future amendments to the Policy in response to new information or changes to technology. Any process involving changes to this Policy should be expressly conditioned on informed public debate by which community members are provided with information about any proposed changes and the impact to local budgets and civil liberties and rights. The Policy should be amended to avoid confusion that your Office can unilaterally change the Policy, as is suggested on the last page of the current Draft ("[T]his Policy will be amended to reflect the current state of the law" (p. 8)).

Conclusion

Thank you for inviting the ACLU's feedback on this draft Policy. With our suggested changes incorporated, this Policy would be a step in the right direction and would mitigate a number of the concerns that we have with warrantless Stingray use. We look forward to seeing a revised policy that adequately protects civil liberties and civil rights. Please feel free to contact us if you have any questions about our feedback.

Sincerely,

Matt Cagle
Technology and Civil Liberties
Policy Attorney
ACLU of Northern California

Tessa D'Arcangelew
Leadership Development Manager &
Organizer
ACLU of Northern California