WASHINGTON
LEGISLATIVE OFFICE

Federal Recommendations on the Use of Cell Site Simulators

In recent years, federal, state, and local officials have increasingly used mass surveillance technologies for domestic criminal and immigration enforcement – raising significant constitutional, privacy, and civil liberties concerns. Specifically, authorities are now using cell site simulators[i] – originally designed for military use –domestically as a way of collecting unique information about mobile devices in a given area, tracking the location of phones, and intercepting the content of certain communications.[ii] The Department of Justice (DOJ), Department of Homeland Security (DHS), and more than 50 state and local agencies have purchased these devices.[iii]

Cell site simulators transmit electronic signals to all cell phones and other mobile devices within range – whether out in the open, stored in a handbag, or sitting in a home. The technology generally functions by impersonating legitimate cell phone towers operated by U.S. telecom companies, such as AT&T and Verizon. The mobile devices are instead forced to connect to the cell site simulator, transmitting their unique electronic serial numbers. By tracking these transmissions, cell site simulators can locate cell phones and other mobile devices precisely. Even when the government has the specific intention of locating a particular suspect's phone, the technology also sweeps up information about bystanders' phones in the area, and in doing so, sends probing signals into the homes and offices of innocent people to reach phones inside. Some agencies attach these devices to planes, helicopters, and other aircraft, increasing the impacted geographic area. In addition, some versions of the technology also permit law enforcement to intercept metadata about ongoing calls and text messages or, in some cases, even the content of communications.[iv]

Policies governing the use of these devices fail to comply with the Fourth Amendment,[v] raise significant civil liberties and privacy concerns, and undermine effective judicial and Congressional oversight. Specifically:

- **The federal government provides funding to state and local law enforcement to purchase these devices**, without ensuring that they have appropriate privacy policies in place. DHS Port Security grants, DOJ Law Enforcement grants, DHS Urban Security Initiative grants, and civil asset forfeiture funds have been used to purchase cell site simulators. The grants do not appear to require recipients to adhere to stringent privacy policies.[vi]

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

MICHAEL W. MACLEOD-BALL
ACTING DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

- **Law enforcement agencies routinely violate the Fourth Amendment by using cell site simulators without obtaining a search warrant based on probable cause**. For example, DHS and many state and local law enforcement agencies use pen register/trap and trace orders which only require a showing that information obtained will likely be relevant to an ongoing investigation.[vii]

- **The use of cell site simulators takes advantage of known vulnerabilities in U.S. communications networks**, leaving all consumers vulnerable to exploitation by foreign intelligence services and criminals.[viii]

- **In approving orders for the use of such devices, requesting agencies often fail to inform judges** how the devices operate, the information they collect, or the number of innocent users likely to be impacted. For example, from 2009 to early 2014, judges in Tacoma, Washington, unwittingly signed over 170 orders authorizing the collection of information, without ever being informed that that cell site simulators were being utilized.[ix]

- **The federal government deliberately hides information regarding the devices** from judges and the public, undermining effective oversight. For example, the federal government has requested that states refer to information from Stingrays as from a "confidential source" in court filings, requested that prosecutors dismiss cases where defendants will be able to compel disclosure of information about cell site simulator use, and forced states and localities to sign non-disclosure agreements prohibiting the release of information about these devices and requiring affirmative withholding of information from judges and defense attorneys.[x]

- **These devices function, in many cases, by jamming 3G and 4G networks**, disrupting the functionality of phone networks, and potentially preventing people in the vicinity from being able to make or receive calls.[xi]

Policy Recommendations

In order to address these concerns, DOJ, DHS, and the Federal Communications Commission (FCC) should adopt the following reforms. While these modifications may not fully resolve the fundamental constitutional problems associated with the use of cell site simulators, they represent important first steps towards greater privacy and civil rights protections.

Department of Justice and Department of Homeland Security

The FBI has been charged with coordinating the use of cell sit simulators by law enforcement agencies nationwide. In addition, DHS and DOJ use these devices for law enforcement purposes and provide financial assistance to states to purchase cell site simulators. Unfortunately, current policies at these

agencies are opaque and, based on the available information, fail to comply with constitutional requirements. To address these concerns, DHS and DOJ should amend existing policy to:

- **Require a search warrant based on probable cause** prior to using a cell site simulator that will impact any phone located in a private space, such as a purse, pocket, business, or home; gather location information about a target phone over time; collect content; or impact third parties who are not surveillance targets. Particularly given the impact on third parties, such a warrant should be obtained even in cases where a judge may have already issued an arrest warrant for an individual.

- **Require the immediate purging of all non-target information collected through the use of cell site simulators.** Such a policy should also include a prohibition on the use or dissemination of non-target information.

- **Prohibit requests to states and localities to deliberately mask or withhold reference** to the use of cell site simulators in court filings or testimony. As part of this policy, the FBI should stop requiring states and localities to sign a cell site simulator non-disclosure agreement, which has been used to justify the withholding of information from judges, defense attorneys, and the public.

- **Mandate that all warrant applications for the use of cell site simulators contain** (1) information regarding the type of technology being deployed, the manner in which it operates, and its impact on innocent third parties, (2) an estimate of the number of individuals to be impacted by the technology, (3) procedures to purge or minimize the information of non-targets, and (4) sufficient facts to demonstrate that alternative, less privacy-invasive methods of investigation and surveillance are inadequate to achieve the same purposes.

- **Require all states and localities receiving federal financial assistance** for the purchase or use of cell site simulators to, at a minimum, comply with federal policies governing the use of the devices, as proposed by these recommendations.

- **Track and make public information about cell site simulators including** the number of times deployed; a breakdown of the purposes for which the devices have been deployed; the number of times the devices have been deployed without a warrant; and the number of non-target devices whose information has been collected.

- **Publicly disclose all policies** governing when cell site simulators can be used; whether a warrant or other approval must be obtained prior to use; information that must be included in warrant applications prior to use; and requirements that state and localities must meet to receive federal financial assistance to purchase cell site simulators.

The Federal Communications Commission

As the agency charged with regulating our communications networks, the FCC plays an important role in the use of cell site simulators. Specifically, the FCC is responsible for approving equipment authorizations for companies that manufacture cell site simulators and notifying consumers regarding vulnerabilities in communications networks that compromise the security of their communications. As part of its unique role and in response to congressional inquiries, the FCC also created a task force to assess the threat posed by the use of cell site simulators by criminal actors or foreign intelligence services. However, current FCC policies fail to regulate cell site simulators sufficiently or protect consumers from the use of these devices by bad actors. To address these concerns, the FCC should:

- **As part of its equipment authorization process for cell site simulators, the FCC should require and make public analysis into the effect of maintaining vulnerabilities** in communications networks that permit the use of cell site simulators.

- **The FCC should disclose the vulnerabilities within existing communications networks** that expose the public to the use of cell site simulators by foreign governments or bad actors and provide the public with clear advice on what they can do to protect themselves.

- **As part of the existing task force, the FCC should issue a public report regarding steps the government and private sector can take to protect consumers** against the use of cell site simulators by bad actors.

- **Request an investigation by the Inspector General into the granting of an equipment authorization to the Harris Company,** the largest manufacturer of cell site simulators in the US. According to recent reports, the FCC may have relied on misleading statements from the company when granting their equipment authorization.[xii]

[i] These devices are also commonly referred to as Stingrays, dirtboxes, and International Mobile Subscriber Identity (IMSI) catchers.

[ii] *See* Ryan Gallagher*Meet the Machines that Steal Your Phones Data*, ARSTECHNICA (Sep. 25, 2013), http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/2/

[iii] Currently, we know that law enforcement officials at the Department of Justice, the Department of Homeland Security, and at least 49 state and local agencies use these devices. *See Stingray Tracking Devices: Who's Got Them,* ACLU, https://www.aclu.org/maps/stingray-tracking-devices-whos-got-them (last visited Apr. 4, 2015). The Department of Justice is charged with coordinating the use of cell site simulators by state and local law enforcement agencies.

[iv] For example, software called "Fishhawk" and "Porpoise" used in conjunction with Stingrays permit eavesdropping on calls and interception of text messages. *See* Gallagher, *supra* note iii.

[v] Given the expansive nature of these devices and their impact on third parties, in certain circumstances, use of these devices even with a warrant and appropriate oversight may still fail to comply with constitutional requirements.

[vi]Memorandum from Joshua Fudge, Interim Fiscal & Budget Administrator, Milwaukee County, to Supervisor Marina Dimitrijevic, Chairwoman, Milwaukee County Board of Supervisors (July 1, 2013), http://legis.wisconsin.gov/lfb/jfc/passive_review/Documents/2013_09_23_Milwaukee%20County%20District%20Attorney%27s%20office.pdf at 15–18 (describing Milwaukee County's application for DOJ Edward Byrn Memorial Justice Assistance Grant to purchase Stingray); Memorandum from Detective Jeffrey Shipp, Tacoma Police Department, to Kathy Katterhagen, Procurement and Payables Manager, City of Tacoma (Mar. 3, 2013), available at https://www.documentcloud.org/documents/1280700-unredacted-purchmemo-hailstorm.html (explaining Tacoma Police Department's purchase of cell site simulator in 2007 using DOJ Law Enforcement Grant Award and receipt of DHS Port Security Grant in 2013 to upgrade cell site simulator); Letter from Andrew A. Dorr, Assistant Director for Grants Administration, Office of Community Oriented Policing Services, U.S. Dep't of Justice, to Sheriff John Rutherford, Jacksonville, FL (Dec. 17, 2007), available at https://www.aclu.org/files/assets/floridastingray/07.01.2014%20-%20PRR%2019037%20RESPONSE%20TO%20CUSTOMER.pdf (approving Jacksonville Police Department's use of DOJ grant to purchase and install cell site simulator);Anne Arundel County, Maryland, Contract Awards $25,000 and Over 12 (Mar. 14, 2014), http://www.aacounty.org/CentServ/Purchasing/Resources/Contracts_Spreadsheet_February%2014.pdf (listing purchase of Hailstorm cell site simulator using grant funding); andCharlotte, NC, City Council Meeting Minutes 49 (Mar. 26, 2012), available at http://charmeck.org/city/charlotte/cityclerk/councilrelated/documents/agenda%20attachments/2012/03-26-2012/03-21-12%20agenda.pdf (discussing Charlotte-Mecklenberg Police Department's use of DHS Urban Area Security Initiative grant to purchase cell site simulator);

[vii] *See* Letter to Attorney General Holder and Secretary Johnson from Senator Chuck Grassley and Senator Patrick Leahy (Dec.23, 2014), *available at* http://www.grassley.senate.gov/sites/default/files/news/upload/2014-12-23%20PJL%20and%20CEG%20to%20DOJ%20and%20DHS%20%28cell-site%20simulators%29.pdf; In the Matter of an Application for the State of Maryland for an Order Authorizing the Installation and Use of a Device Known as a Pen Register/ Trap and Trace, No. 1:14-cr-00170-CCB (filed Oct. 10, 2014) , *available at* https://www.documentcloud.org/documents/1371716-29-1-prtt-applic-and-order.html (authorizing Stingray use through the pen trap and trace statute)

[viii] *See* Ashkan Soltani & Craig Timberg, *Tech Firms Try to Pull Back the Curtain on surveillance efforts in Washington*, WASH. POST (Sept. 17, 2014), http://www.washingtonpost.com/world/national-security/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f_story.html. Stephanie Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH 1 (2014).

[ix] Adam Lynn, *Tacoma Police Change How They Seek Permission to Use Cell Phone Trackers*, THE NEWS TRIBUNE (Nov. 15, 2014), http://www.thenewstribune.com/2014/11/15/3488642_tacoma-police-change-how-they.html?rh=1.

[x] FBI Non-Disclosure Agreement (June 29, 2012), *available at* http://www.nyclu.org/files/releases/Non-Disclosure-Agreement.pdf Email from North Port Police Dept. (Apr. 15, 2009), *https://www.aclu.org/sites/default/files/assets/aclu_florida_stingray_police_emails.pdf;* Email from the Sacramento County Sheriff's Department (Feb. 19, 2014), *available at* https://www.aclunc.org/sites/default/files/stingrays/sacramento_email_response_to_pra_2014.pdf;

[xi] Kim Zetter, *Feds Admit Stingrays Can Disrupt Cell Service of Bystanders,* WIRED (March 1, 2015), http://www.wired.com/2015/03/feds-admit-stingrays-can-disrupt-cell-service-bystanders/

[xii] Nathan Freed Wessler & Nicole Ozer, *Documents Suggest Maker of Controversial Surveillance Tool Misled the FCC*, ACLU (Sept. 17, 2014), https://www.aclu.org/blog/national-security-technology-and-liberty/documents-suggest-maker-controversial-surveillance.