WASHINGTON
LEGISLATIVE OFFICE

Oct. 20, 2015

Dear Member of Congress,

On behalf of the American Civil Liberties Union[1] ("ACLU"), we submit this statement for the record to the House of Representatives Committee on Oversight Subcommittee on Information Technology hearing titled "Examining Law Enforcement Use of Cell Phone Tracking Devices."

Over the last several decades, federal, state, and local officials have increasingly used mass surveillance technologies for domestic criminal enforcement – threatening the rights of Americans to be free from unconstitutional, generalized surveillance of their personal information. Specifically, since the mid-nineties,[2] authorities have used cell site simulators[3] (hereinafter "Stingrays") – originally designed for military and intelligence agency use – domestically as a way of identifying and tracking the location of phones.[4] The Department of Justice ("DOJ"), Department of Homeland Security ("DHS"), and more than 50 state and local agencies have purchased these devices.[5]

Despite their widespread use, the federal government has made a deliberate, concerted effort to conceal Stingray use, undermining effective oversight by Congress, state and local officials, and judges. In August, following several high profile media reports and subsequent congressional inquiries, the DOJ finally created and publicly released guidelines governing the Department's use of the devices.

Though it has positive elements, the DOJ guidance contains problematic gaps - including exceptions to the warrant requirement, lack of notice to individuals impacted by Stingrays, and failure to meaningfully restrict state and local officials. As a result, the guidance falls short of protecting Americans from indiscriminate use of Stingrays or other technologies that permit law enforcement to collect location, device, or content information.

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

KARIN JOHANSON
DIRECTOR

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

[1] With more than a million members, activists, and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico, and Washington, D.C., for the principle that every individual's rights must be protected equally under the law, regardless of race, religion, gender, sexual orientation, disability, or national origin.

[2] *See* Tsutomu Shimomura, *Catching Kevin*, WIRED, (Feb. 1996), at 124, http://www.wired.com/wired/archive/4.02/catching_pr.html (Describing how Infamous computer hacker Kevin Mitnick was located in 1995 by FBI agents using a combination of an cell site simulator and aTriggerFish, a digital analyzer manufactured by the Harris Corporation. The cell site simulator was able to page Mitnick's phone without causing an audible ring, after which the TriggerFish was used to locate the phone.).

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

[4] *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/.

[5] *See Stingray Tracking Devices: Who's Got Them,* ACLU, https://www.aclu.org/maps/stingray-tracking-devices-whos-got-them (last visited Oct. 20, 2015). The Department of Justice is charged with coordinating the use of Stingrays by state and local law enforcement agencies.

Accordingly, we urge Congress to pass legislation, beginning with the GPS Act, which would impose a warrant requirement and other protections for any device that collects such information. In addition, we urge the Executive Branch to (1) issue comprehensive guidance requiring federal agencies to obtain a warrant and adopt other privacy protections when using current or future technologies that collect such information, and (2) strengthen the current DOJ guidance to eliminate loopholes to the warrant requirement, provide notification to individuals whose information is collected by Stingrays, require states and localities to adhere to privacy protections, further restrict retention of information, and increase transparency.

I. Stingray Technology

Stingrays 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 functions by impersonating legitimate cell phone towers operated by U.S. telecommunications companies, such as AT&T and Verizon.

Depending on the particular features of the device and how the operator configures them, Stingrays can be used to identify nearby phones,[6] to locate them with extraordinary precision,[7] and even to block service, either to all devices in the area or to particular devices.[8] They operate by sending probing signals into all homes and offices in range, which forces nearby cell phones to emit identifying signals that transmit their unique electronic serial numbers. By tracking these transmissions, Stingrays can precisely locate cell phones and other mobile devices. Even when the government is only trying to locate a particular suspect's phone, the technology, by design, sweeps up information about all bystanders' phones in the area.

Some agencies, such as the US Marshall Service,[9] attach these devices to planes, helicopters and other aircraft, increasing the impacted geographic area and the number of innocent people whose telephones are forced to reveal identifying information to the government.[10] In addition, some versions of the technology permit law enforcement to intercept metadata about ongoing calls and text messages, or the

---

[6] A number of companies in addition to the Harris Corporation produce and sell cell site simulator equipment. *See, e.g.*, CellXion Ltd., *UGX Series 330: Transportable Dual GSM / Triple UMTS Firewall and Analysis Tool*, http://s3.documentcloud.org/documents/810703/202-cellxion-product-list-ugx-optima-platform.pdf (last visited Oct. 20, 2015) (including as features, "[c]omprehensive identification of IMSI, IMEI and TMSI information" and "[s]imultaneous high speed acquisition of handsets (up to 1500 per minute), across up to five networks").

[7] *See, e.g.*, Mem. from Stephen W. Miko, Resource Manager, Anchorage Police Department, to Bart Mauldin, Purchasing Officer, Anchorage Police Department (June 24, 2009), http://files.cloudprivacy.net/anchorage-pd-harris-memo.pdf ("[The] system allows law enforcement agencies . . . the ability to . . . [i]dentify location of an active cellular device to within 25 feet of actual location anywhere in the United States.").

[8] *See, e.g.*, CellXion Ltd., *UGX Series 330: Transportable Dual GSM / Triple UMTS Firewall and Analysis Tool*, *available at* http://s3.documentcloud.org/documents/810703/202-cellxion-product-list-ugx-optima-platform.pdf (last visited Oct. 20, 2015) (including as features, "[c]omprehensive identification of IMSI, IMEI and TMSI information"and "[s]imultaneous high speed acquisition of handsets (up to 1500 per minute), across up to five networks") (describing device's ability to "[d]isable all handsets except operationally friendly"); Miko Mem., *supra* note 7 ("[The] system allows law enforcement agencies . . . the ability to . . . [i]nterrupt service to active cellular connection [and] [p]revent connection to identified cellular device.").

[9] U.S. Immigration and Customs Enforcement (ICE) has also purchased equipment to mount Stingrays on aerial devices.. Purchase Order, U.S. Immigration and Customs Enforcement (pp.44), *available at*, https://www.documentcloud.org/documents/479397-#document/p44.

[10] Barrett Devlin, *Americans Cell Phones Targeted in U.S. Secret Spy Program* (Nov. 13, 2014), WALL STREET JOURNAL, http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533

content of communications in some cases.[11] Newer versions of this technology also appear to have the capability to deliver malware to phones, remotely enabling microphones or permitting surveillance in other ways.

II. Constitutional Concerns

Stingrays permit the government to collect information in bulk – raising significant Fourth Amendment concerns even in cases where the government obtains a warrant. For example, it would be unconstitutional to search the homes of everyone within a city to identify someone who may have stolen a cell phone.[12] Similarly, there may be cases where the use of a Stingray would not be reasonable, due to the number of innocent third parties impacted. Given this, there must be strong oversight of Stingrays to determine whether their use is in the public interest and comports with the Constitution. If a Stingray is used, at a minimum, the Fourth Amendment requires that law enforcement obtain a warrant and that the collection and retention of data be narrowly constrained.[13]

Stingrays broadcast invisible signals that intrude into private spaces, such as homes and offices, which are protected by the Fourth Amendment. This forces cell phones within those spaces to transmit data to the government that they would not otherwise reveal, and allows agents to determine facts about the phone and its location that would not otherwise be known without physical entry or seizure. By pinpointing suspects and third parties while they are inside constitutionally protected spaces, Stingrays invade reasonable expectations of privacy.[14]

In addition, Stingrays can pinpoint an individual within an accuracy of meters, also triggering a warrant requirement under the Fourth Amendment."[15] For example, in one case, a Tallahassee police officer testified that using a handheld Stingray, he "quite literally stood in front of every door and window" in a large apartment complex "evaluating all the handsets in the area" until he narrowed down the specific apartment in which the target phone was located.[16] Similarly, in Baltimore, police reportedly used a Stingray to track a person within a single city block, and were able to determine that the person carrying

---

[11] 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 4.

[12] *See, e.g.*, *Stanford v. Texas*, 379 U.S. 476, 481-82 (1965) (discussing that one purpose of the Fourth Amendment is to prohibit "general warrants" that give "officials blanket authority to search where they please[]").

[13] *Compare Berger v. New York*, 388 U.S. 41, 57–59 (1967) (requiring, in addition to issuance of a warrant, strict minimization and retention protections in use of wiretaps "so as to prevent unauthorized invasions of privacy" inflicted by "general searches by electronic devices").

[14] *See Kyllo v. United States*, 533 U.S. 27, 34 (2001) (thermal imaging to detect heat from home constituted search); *United States v. Karo*, 468 U.S. 705, 715 (1984) (monitoring of beeper placed into can of ether that was taken into residence constituted search). By way of additional illustration, take the Supreme Court's recent observation that "nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower." *Riley v. California*, 134 S. Ct. 2473, 2490 (2014).

[15] *See, e.g.*, PKI Electronic Intelligence GmbH, *GSM Cellular Monitoring Systems*, 12, http://www.pki-electronic.com/2012/wp-content/uploads/2012/08/PKI_Cellular_Monitoring_2010.pdf (device produced by a competitor to the Harris Corporation can "locat[e] ... a target mobile phone within an accuracy of 2 m[eters]").

[16] Transcript of Suppression Hr'g 14, 17, *State v. Thomas*, No. 2008-CF-3350A (Fla. 2d Cir. Ct. Aug. 23, 2010) [hereinafter "*Thomas* Transcript"], *available at* https://www.aclu.org/files/assets/100823_transcription_of_suppression_hearing_complete_0.pdf.

the phone was in fact riding on a bus.[17] Accurate electronic location tracking of this type requires a warrant because it intrudes on reasonable expectations of privacy.[18]

Moreover, Stingrays search the contents of people's phones by forcing those phones to transmit their electronic serial number and other identifying information held in electronic storage on the device, as well as the identity of the (legitimate) cell tower to which the phone was most recently connected and other stored data. As the Supreme Court has explained in no uncertain terms, searching the contents of a cell phone requires a warrant.[19]

III. Cybersecurity and Safety Concerns

In addition to constitutional concerns, the use of Stingrays raises cybersecurity and public safety concerns. Stingrays exploit a long-standing cybersecurity vulnerability in cellular phones — namely that phones have no way to differentiate between a legitimate cell tower owned or operated by the target's wireless carrier and a rogue device impersonating a carrier's base station.[20] Foreign governments and hackers, who can acquire a Stingray with ease at a low cost, can also exploit such vulnerabilities.[21] For example, the *Washington Post* has reported the presence of Stingrays near the White House, the Capitol, foreign embassies and the cluster of federal contractors near Dulles International Airport, suggesting malicious actors may be utilizing the devices. In 2014, the Federal Communications Commission created a task force to examine the threat posed by Stingrays, but has yet to make any findings public. In light of the real threat posed by such actors, the Federal Communications Commission, the wireless carriers, and the national security community should collectively work to fix these flaws – rather than exploit them – thereby improving the cybersecurity of our national telecommunications network.

In addition, Stingrays also raise public safety concerns. As a side effect of their normal use, Stingrays disrupt the ability of phones in the area to make calls and adversely affect phone networks. Harris Corporation, the company that manufactures the Stingray, and at least one of its competitors, has apparently taken steps to ensure that 911 emergency calls are not disrupted.[22] However, emergency calls to doctors, schools, psychologists, and family members may be blocked while a Stingray is in use nearby. This can have enormous consequences for anyone in an emergency situation trying to make an urgent call for assistance, not to mention the myriad of day to day uses in non-emergency circumstances.

IV. DOJ Guidance and Recommended Improvements

---

[17] Justin Fenton, *Judge Threatens Detective with Contempt for Declining to Reveal Cellphone Tracking Methods,* THE BALTIMORE SUN (Nov. 17, 2014), http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-officer-contempt-20141117-story.html.

[18] *See United States v. Jones*, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in the judgement) ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."); *id.* at 955 (Sotomayor, J., concurring); *Tracey v. State*, 152 So.3d 504, 526 (Fla. 2014) ("[T]he use of [a suspect's] cell site location information emanating from his cell phone in order to track him in real time was a search within the purview of the Fourth Amendment for which probable cause was required.").

[19] *Riley v. California*, 134 S. Ct. 2473 (2014).

[20] *See generally* 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).

[21] *Id.* 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.

[22] Barrett, *supra* note 10.

In August, the DOJ released policy guidelines on the use of cell site simulator technology, which left gaping holes in privacy protections, including failure to require a warrant in all circumstances, failure to provide adequate notice to defendants, and failure to restrict the activities of state and local officials in any meaningful fashion. The guidance requires only that officials:[23]

- Obtain a warrant prior to using a cell-site simulator, with the exception of exigent circumstances, undefined "exceptional" situations, and when the Department acts pursuant to the Foreign Intelligence Surveillance Act ("FISA");
- Include information about how the device operates in warrant applications;
- Purge data within one day in cases where law enforcement seeks to locate a known device, and within 30 days in cases where law enforcement is trying to locate an unknown device; and
- Track the number of times cell-site simulators are used, including the number of times it is deployed without a warrant in "exceptional" circumstances.

Though it has some positive elements, the DOJ must take steps to address the problematic gaps in the guidance. Specifically, the DOJ should (a) narrow exceptions to the warrant requirement; (b) provide notice to individuals, including criminal defendants, whose information is collected by Stingrays; (c) apply the guidance to states, localities, and other federal agencies; (d) further limit the retention of information; and (e) increase transparency by requiring that Congress and the public be provided information on the use of the devices.

a. Warrant Exceptions

The DOJ guidance creates a default requirement that officials obtain a warrant before using Stingrays. However, there are several concerning loopholes to this requirement.

One, DOJ permits use of the devices without a warrant in "exceptional" circumstances. However, the guidance does not specify what constitutes an "exceptional" circumstance, or even the factors that lead to such a determination.

Two, DOJ components are permitted to proceed without a warrant in exigent circumstances, which include preventing the imminent destruction of evidence or escape of a suspect. There may be the need for an exception in narrowly-defined emergencies when there is not time to obtain a warrant, as defined in case law concerning the exigency exception to the Fourth Amendment's warrant requirement. However, in such cases, law enforcement should reasonably believe that probable cause exists to obtain a warrant, and should be required to make such a showing within 48 hours. Without these protections, there is a danger of abuse in the use of the exigency exception. Unfortunately, the guidance does not contain such protections. Instead, law enforcement personnel are required to demonstrate only that they believe that the information sought is relevant to an investigation, and apply for a pen register/trap and trace order under this lower standard following the exigency.

Three, the guidance does not require a warrant in criminal investigations conducted pursuant to FISA, which would permit use of these devices without probable cause in certain criminal investigations.

To close these loopholes, the DOJ guidance should be amended to define what constitutes an exceptional circumstance; narrow the definition of exigent circumstances to those recognized in existing case law; require that a probable cause standard be met immediately following an exigent circumstance; and require a warrant in FISA investigations.

[23] The guidance also states that the DOJ does not use Stingrays to collect the content of communications.

b. Notice

Another conspicuous gap in the guidance is the failure to provide notice to criminal defendants and other individuals whose information is collected by Stingrays. This is particularly concerning given that the DOJ appears to withhold such information from criminal defendants deliberately. Emails obtained by the ACLU found that the federal government has requested that states refer to information from stingrays as information from a "confidential source" in court filings, preventing defendants from raising legitimate legal challenges. Recently, a representative of the Maryland Public Defender's office asserted a belief that such disclosure was withheld in several hundred cases in Maryland.[24] In addition, the guidance does not address the prosecutors' obligations under *Brady*[25] to turn over exculpatory information that may be gathered by Stingrays, nor does it require notification to non-target individuals whose information is collected by Stingrays, similar to the notice requirement contained in wiretap statutes.[26]

The DOJ should amend its policy to specify the obligation of prosecutors' to provide notice to individuals in all criminal cases or administrative proceedings where a Stingray is used to obtain evidence, identify witnesses, or apprehend an individual, and disclose information pursuant to *Brady*. In addition, similar to the wiretap statute requirements, the DOJ should require notification of individuals who are not targets of an investigation and have their information collected.

c. States, Localities, and Other Federal Agencies

The current guidance applies only to DOJ components, notably excluding other federal agencies, states, and localities. This is particularly concerning, given that the federal government has funded the purchase of Stingrays by states and localities through civil asset forfeiture funds, DHS Port Security grants, DOJ Law Enforcement grants, and DHS Urban Security Initiative grants.[27]

---

[24] Computers, Freedom, Privacy Conference 2015, *Not Just the NSA: How Local Police and Law Enforcement Use Stingrays to Track Our Phones*, LIVESTREAM (Oct. 14, 2015), http://livestream.com/internetsociety/CFP2015-2/videos/102080869.

[25] *Brady v. Maryland*, 373 U.S. 83 (1963).

[26] *See* 18 U.S.C. § 2518(8)(d)

[27] 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).

Pursuant to the terms of the licensing agreement granted by the Federal Communications Commission ("FCC") to the leading vendor of Stingray technology, states and localities who wish to purchase stingrays must coordinate with the DOJ. As part of this process, the DOJ requires that states and localities sign non-disclosure agreements, which prohibit states and localities from releasing information about the devices, require withholding information from judges and attorneys, and encourage states to dismiss charges in cases where defendants challenge the constitutionality of the devices.[28] Despite these arduous secrecy requirements, the DOJ has taken no similar steps to ensure that states and localities adhere to the Fourth Amendment as part of this approval process.

To address this deficiency, DOJ should require all localities that request permission or receive federal funding to purchase Stingrays, to comply with the August guidance. In addition, the guidance should be adopted by all federal agencies, including DHS.

d. Retention

Given the large amount of information collected by Stingrays, it is critical that there be strict limits on the retention of information. All information of non-targets should be purged immediately to prevent improper access. While the guidance contains this requirement in some circumstances, it permits retention for up to thirty days in cases where law enforcement is attempting to locate an unidentified phone. Such a lengthy retention period is concerning, given that Stingrays may gather the information of thousands of individuals at any given time.

To address this concern, officials should be required to obtain permission from a judge to retain information longer than three days, for a maximum of thirty days.

e. Transparency Reporting

To date, the public and members of Congress have little information about how often and in what circumstances Stingrays are used. While the DOJ requires the department to track the number of times that Stingrays are used, including deployments in "exceptional circumstances," it does not require that such information be provided to the public and members of Congress. Given the history of secrecy surrounding such devices, it is critical that information be disclosed to permit appropriate oversight.

To ensure appropriate transparency, the DOJ should commit to tracking and making public information about the number of times Stingrays are deployed, including the number of times in which a warrant is not obtained.

V. Conclusion

As technology evolves, we will increasingly encounter new devices that provide law enforcement the ability to collect device, location, and other sensitive information. To address this privacy threat, Congress must pass legislation that places strict limits on the collection of such information, regardless of the technology employed. The existing DOJ guidance – which contains loopholes to the warrant

[28] 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), *available at*, 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.

requirement and does not address notice obligations of the government – is insufficient to protect the Fourth Amendment right of Americans. Accordingly, this guidance must also be strengthened and expanded to cover other technologies that permit similar collection of information.

If you have any questions, please feel free to contact Legislative Counsel, Neema Singh Guliani at 202-675-2322 or nguliani@aclu.org.

Sincerely,

Karin Johanson
Director, Washington Legislative Office

Neema Singh Guliani
Legislative Counsel