Written Testimony of Neema Singh Guliani on behalf of the American Civil Liberties Union Before the U.S. House of Representatives Committee on Oversight and Government Reform

Hearing on

"Geolocation Technology and Privacy"

Wednesday, March 2, 2016 at 10:00am

Submitted by the
ACLU Washington Legislative Office

For further information, please contact Neema Singh Guliani, Legislative Counsel, at nguliani@aclu.org or 202.675.2322

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee:

Thank you for the opportunity to testify on behalf of the American Civil Liberties Union (ACLU).[1] As technology has advanced, consumers increasingly rely on electronic devices to work, communicate, surf the internet, or even hail a taxi. Many of these devices, including mobile phones, track and collect sensitive location information. Unfortunately, our laws have not kept pace with these new technological developments – resulting in confusion among the courts, law enforcement officials, and the public over the protections that apply to location information. As a result, law enforcement officials across the country routinely collect location information without a probable cause warrant or other appropriate privacy protections. For example:

- The Department of Justice (DOJ) has taken the position that a warrant is not required to collect historical cell site location information – even for a period spanning over seven months.[2]
- U.S. Attorney's Offices in the District of New Jersey and the Southern District of Florida have obtained precise mobile phone location data without a probable cause warrant, despite DOJ policy that recommends obtaining a warrant in such cases.[3]
- Numerous states and localities use cell phone tracking devices known as Stingrays, often funded by federal dollars, to collect location information without obtaining a warrant, adopting appropriate retention policies, or providing required notice to criminal defendants.

Congress and the Administration must act to remedy these deficiencies. We urge Congress to pass comprehensive legislation, beginning with the Geolocation Privacy and Surveillance Act, which requires law enforcement officials to obtain a probable cause warrant to obtain real-time or historical location information unless narrow exceptions apply. Until such legislation, this committee should ensure that the DOJ adopts a policy requiring a probable cause warrant before law enforcement can collect such information. In addition, this committee should demand that the DOJ publicly release unredacted

[1] For nearly 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and laws of the United States guarantee everyone in this country. 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., to preserve American democracy and an open government.

[2] Supplemental En Banc Brief of Appellee, United States v. Graham, 796 F.3d 332 (4th Cir. 2015) (rehearing en banc granted).

[3] Letter from William G. Stewart II, Assistant Director, Office of Information and Privacy, U.S. Dept. of Justice to Catherine Crump, Staff Attorney, American Civil Liberties Union (Dec. 31, 2008) *available at,* https://www.aclu.org/sites/default/files/pdfs/freespeech/cellfoia_released_074132_12312008.pdf (responding to FOIA request for mobile phone tracking information from the U.S. Attorney's Office for the District of New Jersey); Letter from William G. Stewart II, Assistant Director, Office of Information and Privacy, U.S. Dept. of Justice to Catherine Crump, Staff Attorney, American Civil Liberties Union (Dec. 31, 2008) *available at,* https://www.aclu.org/sites/default/files/pdfs/freespeech/cellfoia_released_074135_12312008.pdf (responding to FOIA request for mobile phone tracking information from the U.S. Attorney's Office for the Southern District of Florida).

copies of the memoranda that provide the Department's interpretation of the Supreme Court's decision in *U.S. v. Jones* and all existing guidance governing the collection of location information.

I. Current Technology Enables Invasive Tracking of Americans' Movements

A. Mobile phone data

In today's world, owning a cell phone is not a luxury. More than 90% of American adults have a cell phone,[4] and landline phones are becoming obsolete.[5] Americans increasingly rely on mobile phones to communicate, surf the internet, or even read the news. Americans carry mobile phones with them to a variety of sensitive or private locations, including homes, churches, doctor's offices, domestic abuse shelters, or even gun rallies. As the Supreme Court has noted, "nearly three-quarters of smart phones 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."[6]

Mobile phones have revolutionized the way that Americans live their daily lives – but they have also provided law enforcement an unprecedented new surveillance tool. With the assistance of mobile phone carriers, at any given time, the government now can inexpensively obtain historical and real-time location information associated with any of the over 320 million U.S. mobile phone accounts.[7] Mobile phones yield information about users' past and present location, including Global Positioning System data and cell site location data.

1. Global Positioning System (GPS) data

Service providers can precisely locate cell phones in real time in two ways: by accessing information from the GPS receiver hardware built into a cell phone to determine the phone's coordinates based on signals from global positioning satellites, and by triangulating the phone's precise location using cell phone signals received by multiple cell towers in the area. This capability stems from rules adopted in 1996 and implemented by 2001, under which the Federal Communications Commission (FCC) required cell phone providers to have "the capability to identify the latitude and longitude of a mobile unit making a 911 call."[8] Although intended as a public safety tool for use in locating 911 callers, most service providers have made the same precise real-time location data available to law enforcement investigators as

---

[4] Lee Rainie, *Cell Phone Ownership Hits 91% of Adults*, PEW RESEARCH CENTER (June 6, 2013), http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/.

[5] STEPHEN J. BLUMBERG, PH.D. & JULIAN V. LUKE, WIRELESS SUBSTITUTION: EARLY RELEASE OF ESTIMATES FROM THE NATIONAL HEALTH INTERVIEW SURVEY, JANUARY-JUNE 2015, NATIONAL CENTER FOR HEALTH STATISTICS (Dec. 2015), *available at* http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201512.pdf.

[6] Riley v. California, 134 S. Ct. 2473, 2490 (2014) (citing 2013 MOBILE CONSUMER HABITS STUDY (CONDUCTED BY HARRIS INTERACTIVE), JUMIO (2013), *available at* http://pages.jumio.com/rs/jumio/images/Jumio%20-%20Mobile%20Consumer%20Habits%20Study-2.pdf).

[7] Cecilia Kang, *Number of Cellphones Exceeds U.S. Population: CTIA Trade Group*, W.S.J., Oct. 11, 2011, https://www.washingtonpost.com/blogs/post-tech/post/number-of-cell-phones-exceeds-us-population-ctia-trade-group/2011/10/11/gIQARNcEcL_blog.html.

[8] Report and Order and Further Notice of Proposed Rulemaking, *In re* Revision of the Communications Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Sys., 11 F.C.C. Rcd. 18676, 18683-84 (1996).

well. In January 2015, the FCC adopted new rules designed to increase precision when identifying the location of individuals indoors, including identification of the floor where a mobile device is located. The GPS systems of some mobile phones can pinpoint location with an accuracy of up to 3 meters,[9] and researchers are reportedly developing new technology that can pinpoint location to within centimeters.[10]

2. Cell site location data

Service providers also collect "cell site" data or "cell site location information," which identifies the location of the cell tower ("cell site") to which the phone is connected, the direction of the phone relative to the tower's antennas (the cell site "sector") and, in some instances, the phone's distance from the cell site. This data is generated because whenever individuals have their mobile phones on, the phones automatically and frequently communicate with nearby cell towers in order to facilitate the routing of calls, text messages, and other communications. In some circumstances, mobile carriers may be able to provide this ongoing registration information to law enforcement. More commonly, any time a phone makes or receives a call or sends or receives a text message, the service provider logs and retains a record of the cell site and sector to which the phone was connected. Service providers may also retain location information for passive data activities (e.g. weather notifications or e-mail synchronizations). In addition to tower and sector information, mobile carriers can now log more precise historical location information than before, including the estimated distance of the phone from the nearest tower, or the phone's precise location based on "triangulation," which entails collecting and analyzing data of the precise time and angle at which the mobile phone's signal arrives at multiple cell towers.

The precision of cell site location information depends, in part, on the size of the coverage area of each cell tower. This means that as the number of cell towers installed in cities and towns has increased and the coverage area for each cell tower has shrunk, cell site location information has become more precise. The latest generation of cellular towers now may cover an area as small as a tunnel, a subway, a specific roadway, a particular floor of a building, or even an office.[11] In addition, customers with poor cell phone coverage in their homes can even ask their carrier to provide them a "femtocell," a small cellular base station, which can cover just one home.

B. Internet connected devices and applications

As technology develops, consumers are embracing a host of internet-connected devices that log

---

[9] *What is GPS?* GARMIN (Feb. 25, 2016), http://www8.garmin.com/aboutGPS/.

[10] Press release, University of Texas at Austin, New Centimeter-Accurate GPS System Could Transform Virtual Reality and Mobile Devices (May 5, 2015), *available at* http://news.utexas.edu/2015/05/05/engineers-develop-centimeter-accurate-gps-system.

[11] *Hearing on Electronic Communications Privacy Act Reform and the Revolution in Location Based Technologies and Services Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on Judiciary*, 111th Cong. 5 (2010) (statement of Professor Matt Blaze), *available at* http://judiciary.house.gov/hearings/pdf/Blaze100624.pdf; Thomas Farely, *Cellular Telephone Basics: AMPS and Beyond*, PRIVATE LINE (Jan. 1, 2006), http://www.ccs.neu.edu/home/futrelle/teaching/com1204sp2001/Farley/Cellbasics.html .

location information. For example, as people use smart cars, medical devices, and wearable fitness devices more often, those devices collect more and more of consumers' location information. In addition, applications supported on smartphones, such as weather, restaurant, shopping, or even dating apps, often rely on and log location information. This location information is often stored by third party app providers in the cloud, not just locally on the consumer's device. The number of these applications and devices is only expected to grow. As of July 2015, there were over 3 million applications available just through the Google Play and Apple App Store.[12] Thus, as smartphones continue to advance and the "Internet of Things" becomes a more dominant reality, the availability of precise location information is likely to extend far beyond mobile carriers to other third parties. Despite these developments, the laws governing law enforcement access to location information held by these third parties remains unclear.

II. Law Enforcement Agencies Routinely Access Americans' Location Information

A. Information requests to mobile carriers

Law enforcement agents can request three types of location information from mobile carriers: historical cell site data, which can be used to retrace previous movements; prospective cell phone location data, which can be used to track mobile phones in real time; and "tower dumps," which provide the data of all the people whose phones were using a particular cell phone tower at a particular time. In recent years, law enforcement agencies have demanded this data from mobile carriers in a significant number of cases. For example:

- In 2015, AT&T received 76,340 requests for cell phone location information; 58,189 were for historical cell site location information.[13]
- In the second half of 2015, Verizon received approximately 20,289 requests for cell phone location data, and 4,558 requests for "tower dumps."[14]
- In the first half of 2015, Sprint received approximately 35,528 requests for real-time location data.[15]

The availability of historical information and the length of time this information is stored varies with the policies of each mobile phone carrier. Verizon has reported storing location information for one year;[16] T-Mobile keeps historical cell site information for six months;[17]

---

[12] *Number of Apps Available in Leading App Stores as of July 2015*, STATISTA (2015), http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/.

[13] AT&T, TRANSPARENCY REPORT 4 (2016), *available at* http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_Transparency%20Report_Jan%202016.pdf.

[14] *Verizon's Transparency Report for the 2nd Half of 2015*, VERIZON, http://transparency.verizon.com/us-report?/us-data (last visited Feb. 22, 2016).

[15] SPRINT CORPORATION TRANSPARENCY REPORT, SPRINT (July 2015), http://goodworks.sprint.com/content/1022/files/TransaparencyReportJuly2015.pdf.

[16] Letter from William B. Peterson, General Counsel, Verizon Wireless to the Honorable Edward J. Markey, United States Senator 3 (Oct. 3, 2013), *available at* http://www.markey.senate.gov/imo/media/doc/2013-12-09_VZ_CarrierResponse.pdf.

[17] U.S. Dep't of Justice, *Retention Periods of Major Cellular Service Providers* (Aug. 2010), *available at* https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart.

Sprint reportedly stores information from 18 to 24 months,[18] and AT&T retains location information for up to five years.[19]

B. Use of IMSI Catchers ("Stingrays")

The DOJ, Department of Homeland Security ("DHS"), Internal Revenue Service, and at least 60 state and local agencies have also purchased IMSI catchers – devices capable of gathering location information of all cell phones within range.[20] IMSI catchers, also known as cell site simulators or Stingrays,[21] function by impersonating legitimate cell phone towers operated by U.S. telecommunications companies. Depending on the particular features of the device and how the operator configures them, Stingrays can be used to identify nearby phones, to locate them with extraordinary precision,[22] and even to block service, either to all devices in the area or to particular devices.[23] They operate by sending probing signals into all homes and offices in range, which forces nearby cell phones to emit identifying signals which transmit their unique electronic serial numbers. By tracking these transmissions, Stingrays can locate cell phones and other mobile devices precisely.

Even when the government is only trying to locate a particular suspect's phone, Stingray technology, by design, sweeps up information about all bystanders' phones in the area. Some agencies, such as the U.S. Marshals Service,[24] attach these devices to planes, helicopters and

---

[18] *Id.*

[19] Letter from Timothy P. McKone, Executive Vice President, Federal Relations, AT&T to the Honorable Edward J. Markey, United States Senator (Oct. 3, 2013), *available at* http://www.markey.senate.gov/imo/media/doc/2013-10-03_ATT_re_Carrier.pdf.

[20] *See Stingray Tracking Devices: Who's Got Them,* ACLU, https://www.aclu.org/maps/stingray-tracking-devices-whos-got-them (last visited Feb. 22, 2016). The Department of Justice is charged with coordinating the use of Stingrays by state and local law enforcement agencies. IMSI catchers are so named in reference to the unique identifier—or international mobile subscriber identity—of wireless devices that they track.

[21] "StingRay" is the name for one cell site simulator model sold by the Harris Corporation, the leading vendor of the technology to U.S. law enforcement agencies. Other models include the "TriggerFish," "KingFish," and "Hailstorm." *See* Ryan Gallagher, *Meet the Machines That Steal Your Phone's Data*, Ars Technica, Sept. 25, 2013, bit.ly/1mkumNf. Other companies selling cell site simulators to domestic law enforcement agencies include Boeing subsidiary Digital Receiver Technology (DRT). *See* Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program*, W.S.J., Nov. 13, 2014, http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533. A number of companies in addition to the Harris Corporation produce and sell cell site simulator equipment. *See* 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 Feb. 22, 2016) (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").

[22] *See* Memorandum from Stephen W. Miko, Resource Manager, Anchorage Police Department, to Bart Mauldin, Purchasing Officer, Anchorage Police Department (June 24, 2009), *available at* 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.") [hereinafter Miko Memorandum].

[23] *See*, CELLXION LTD., *supra* note 21 (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"); *See* Miko Memorandum, *supra* note 22 ("[The] system allows law enforcement agencies . . . the ability to . . . [i]nterrupt service to active cellular connection [and] [p]revent connection to identified cellular device.").

[24] U.S. Immigration and Customs Enforcement (ICE) has also purchased equipment to mount Stingrays on aerial

other aircraft, increasing the impacted geographic area and the number of innocent people whose telephones reveal identifying information to the government.[25] Though comprehensive information is not available, it appears that many agencies are using Stingrays not just occasionally, but frequently. For example,

- The Baltimore Police Department has used the devices in approximately 4,300 investigations since 2007,[26] and the Baltimore County Police Department has used them 622 times over five years.[27]
- The U.S. Marshals service has used cell site simulators in nearly 6,000 cases over a still undisclosed period of time.[28]
- The Sacramento Sheriff's Department initially estimated that it used cell site simulators in about 500 criminal cases, but later said it could be as many as 10,000.[29]

III. Law Enforcement Should be Required to Obtain a Warrant to Access Historical or Real-Time Location Information

Law enforcement should be required to obtain a probable cause warrant to access historical or real-time location information. Location tracking enables law enforcement to capture details of someone's movements for months on end, unconstrained by the normal barriers of cost and officer resources.[30] In *United States v. Jones*,[31] the Supreme Court held that a Fourth Amendment search occurred when the government placed a GPS tracking device on the defendant's car and monitored his whereabouts non-stop for 28 days.[32] A majority of the Justices also stated that "the use of longer term GPS monitoring . . . impinges on expectations of privacy" in the location data downloaded from that tracker.[33] As Justice Alito explained, "[s]ociety's expectation has been that law enforcement agents and others would not -- and indeed, in the

---

devices. PURCHASE ORDER, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT 44, *available at* https://www.documentcloud.org/documents/479397-#document/p44. The FBI has acknowledged operating IMSI catchers aboard aircraft at least five times. Eileen Sullivan, Jack Gillum, & Eric Tucker, *FBI: Surveillance Flights by the Book, Rarely Track Phones*, A.P., June 18, 2015, http://bigstory.ap.org/urn:publicid:ap.org:1240a8a42edf4a86aff72a0246525a95.

[25] Barrett Devlin, *supra*, note 21.

[26] Justin Fenton, *Baltimore Police Used Secret Technology to Track Cellphones in Thousands of Cases*, BALTIMORE SUN, Apr. 9, 2015, http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-case-20150408-story.html.

[27] Alison Knezevich, *Baltimore Co. Police Used Secretive Phone-Tracking Technology 622 Times*, BALTIMORE SUN, Apr. 9, 2015, http://www.baltimoresun.com/news/maryland/crime/bs-md-co-county-stingray-20150409-story.html.

[28] Brad Heath, *U.S. Marshals Secretly Tracked 6,000 Cellphones*, USA TODAY, Feb. 23, 2016, http://www.usatoday.com/story/news/2016/02/23/us-marshals-service-cellphone-stingray/80785616/ .

[29] *New Developments in Sacramento "Stingray" Case*, ABC 10, Jan. 8, 2016, http://legacy.abc10.com/story/news/local/sacramento/2016/01/08/new-developments-sacramento-stingray-case/78541240/.

[30] *See* United States v. Pineda-Moreno, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, J, dissenting from denial of rehearing en banc) ("The modern devices used in Pineda- Moreno's case can record the car's movements without human intervention—quietly, invisibly, with uncanny precision. A small law enforcement team can deploy a dozen, a hundred, a thousand such devices and keep track of their various movements by computer, with far less effort than was previously needed to follow a single vehicle.").

[31] United Sates v. Jones, 132 S. Ct. 945, 954 (2012)

[32] *Id.* at 954.

[33] *Id*. at 953-64 (Sotomayor, J., concurring); *see also id.* at 964 (Alito, J., concurring).

main, simply could not -- secretly monitor and catalog every single movement of an individual's car, for a very long period."[34]

Justice Sotomayor emphasized the intimate nature of the information that might be collected by the GPS surveillance, including "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."[35] While even the limited collection of geolocation information can reveal intimate and detailed facts about a person, the privacy invasion is multiplied many times over when law enforcement agents obtain geolocation information for prolonged periods of time. As the D.C. Circuit Court of Appeals has observed, "[a] person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts."[36]

There have always been facets of American life which have been uniquely safeguarded from the intrusive interference and observation of government. Location tracking threatens to make even those aspects of life an open book to government. As Justice Sotomayor pointed out in *Jones*, "Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."[37] Further, location information from cell phones can reveal people's locations and movement within their homes and other spaces that receive heightened protection under the Fourth Amendment.[38] As the Supreme Court has noted, cell phone location data can "reconstruct someone's specific movements down to the minute, not only about town but also within a particular building."[39]

While privacy rights are often conceptualized as belonging to individuals, they are also important because they ensure a specifically calibrated balance between the power of individuals on the one hand and the state on the other. When the sphere of life in which individuals enjoy privacy shrinks, the state becomes all the more powerful:

> The net result is that GPS monitoring--by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track--may alter the relationship between citizen and government in a way that is inimical to democratic society.[40]

---

[34] *Id.* at 964 (Alito, J., concurring).
[35] *Id.* at 955 (Sotomayor, J., concurring) (quoting *People v. Weaver*, 12 N.Y.3d 433, 442 (N.Y. 2009)).
[36] United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd sub nom. Jones*, *supra* note 31.
[37] *Jones*, *supra* note 31 at 956 (Sotomayor, J., concurring) (quotations omitted).
[38] *See* Tracey v. State, 152 So.3d 504, 524 (Fla. 2014) ("We cannot overlook the inexorable and significant fact that, because cell phones are indispensable to so many people and are normally carried on one's person, cell phone tracking can easily invade the right to privacy in one's home or other private areas.").; *see also* In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304, 318 (3d Cir. 2010).
[39] *Riley*, *supra* note 6 at 2490.
[40] *Jones*, *surpa* note 31 at 956 (Sotomayor, J., concurring) (quotations omitted).

Furthermore, while the government has argued that records of a person's prior movements deserve less privacy protection than records of where a person travels in real time, this is a meaningless distinction. As one judge has noted, "[t]he picture of [a person]'s life the government seeks to obtain is no less intimate simply because it has already been painted."[41] Historical records provide the government with a new power, a veritable time machine that allows it to learn sensitive information about a person's movements and activities months and even years into the past.

While the *Jones* case dealt with long-term tracking of movements, even single points of mobile phone location data can intrude upon reasonable expectations of privacy– a single GPS data point revealing that someone is in the waiting room of a psychiatrist's office, at a church, or at an AA meeting can reveal information that is highly sensitive.[42] The Supreme Court has held that location tracking even using relatively crude "beeper" trackers implicates reasonable expectations of privacy where it "reveals information that could not have been obtained through visual surveillance from a public space."[43] For this reason, and because law enforcement agents often will not know whether a particular piece of mobile phone location data will implicate a person's privacy interest in their location in private spaces, the better rule is an across-the-board requirement that law enforcement agents obtain a warrant based on probable cause for location data.

IV. Current Laws Fail to Protect Americans' Privacy

There is confusion among law enforcement agents, courts, and members of the public regarding what legal standard law enforcement agents must meet to obtain location data – underscoring the need for legislation. This is due in part to the fact that the principal law that governs law enforcement access to records regarding electronic communications, the Electronic Communications Privacy Act of 1986, does not expressly address law enforcement access to location data. As a result, location tracking is governed by a patchwork of state and local laws, non-binding policies, and inconsistent court cases.

Twelve states – California, Indiana, Illinois, Maine, Maryland, Minnesota, Montana, New Hampshire, Utah, Virginia, Washington, Wisconsin – have passed laws requiring police to get a warrant to obtain real-time location information.[44] Six of these states require a warrant for collection of historical cell site information.[45] In addition, at least seven states require a warrant

[41] *In re* Application of the United States for an Order Authorizing Release of Historical Cell-Site Information, 736 F.Supp.2d 578, 585 (E.D.N.Y. 2010).

[42] United States v. Davis, 754 F.3d 1205, 1216 (11th Cir. 2014) ("[E]ven on a person's first visit to a gynecologist, a psychiatrist, a bookie, or a priest, one may assume that the visit is private if it was not conducted in a public way. . . . Thus, the exposure of the cell site location information can convert what would otherwise be a private event into a public one. . . . [E]ven one point of cell site location data can be within a reasonable expectation of privacy."), *rev'd* 785 F.3d 498 (11th Cir. 2015) (en banc).

[43] United States v. Karo, 468 U.S. 705, 707 (1984).

[44] Cal. Penal Code § 1546; 16 Maine Rev. Stat. § 648; Md. Code, Criminal Procedure 1-203.1(b)(1); Minn. Stat. §§ 626A.28(3)(d), 626A.42(1)(d); Mont. Code § 46-5- 110(1)(a); N.H. Stat. § 644-A; Va. Code § 19.2-56.2; Wash. Rev. Code § 9.73.260.725; Ill. Comp. Stat. 168/10; Ind. Code § 35-33-5-12; Wis. Stat. § 968.373(2); Utah Code § 77-23c-102.

[45] Cal. Penal Code § 1546; 16 Maine Rev. Stat. § 648; Minn. Stat. §§ 626A.28(3)(d), 626A.42(1)(d); Mont. Code § 46-5-110(1)(a); N.H. Stat. § 644-A; tah Code § 77-23c-102.

before installing an electronic tracking device, and Washington, Virginia, and California have passed legislation limiting Stingray use.[46] While these laws alone are not sufficient to protect the rights of all individuals, they reflect a growing consensus among Americans that location information should be afforded a high degree of protection.

Not surprisingly, given the variations in law, law enforcement agencies' practices also vary widely. In August 2011, 35 ACLU affiliates submitted public records requests with state and local law enforcement agencies around the nation seeking information about their policies, procedures, and practices for obtaining mobile phone location data.[47] Over 200 local law enforcement agencies responded. While the overwhelming majority engaged in at least some cell phone tracking, the legal standards they met varied widely. For example, police in Lincoln, Nebraska, obtained even GPS data without a warrant based upon probable cause. Police in Wilson County, North Carolina, obtained historical cell site location information by proffering only that the data is "relevant and material" to an ongoing investigation. Some police departments, including police in the County of Hawaii, Wichita, and Lexington, secured warrants based upon probable cause to obtain mobile phone location data.

U.S. Attorney's Offices have also acted inconsistently. DOJ recommends that law enforcement agents obtain a warrant based upon probable cause to access precise real-time location data.[48] However, litigation by the ACLU and Electronic Frontier Foundation revealed that U.S. Attorney's Offices in the District of New Jersey and the Southern District of Florida have obtained even what DOJ classifies as precise mobile phone location data without obtaining a warrant or showing probable cause.[49]

The courts have only provided incomplete guidance on the protections that should apply to law enforcement requests for location information. In *United States v. Jones*, the Supreme Court held that attaching a GPS device to a car and tracking its movements is a search under the Fourth Amendment. *Jones*, however, left unresolved how its holding would apply to surveillance performed with other technologies such as mobile phone tracking or Stingrays. The DOJ has issued two guidance memoranda setting out its view of how *Jones* affects the constitutionality of various forms of location tracking; unredacted copies of these memos have not been made public despite an ACLU request for them under the Freedom of Information Act and numerous Congressional inquiries.

Circuit courts, interpreting the *Jones* decision, have provided inconsistent guidance on the appropriate standard governing law enforcement access to location information. With regard to historical location information, the Fifth Circuit has ruled that a warrant is not required, as

[46] Cal. Penal Code § 637.7; Del. Code § 1335(a)(8); Haw. Rev. Stat. § 803- 42(a)(8); Minn. Stat. § 626A.35; Tenn. Code § 39-13-606; Tex. Penal Code § 16.06; Va. Code § 18.2-60.5.; Wash. Rev. Code § 9.73.260.

[47] Supporting documentation demonstrating the factual assertions throughout this section can be found at, *Cell Phone Location Tracking Public Records Request*, ACLU, http://www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-public-records-request (updated Mar. 25, 2013).

[48] *The Electronic Communications Privacy Act: Government Perspective on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on Judiciary*, 125th Cong. 7 (2011) (statement of James A. Baker, Associate Deputy Att'y Gen., U.S. Dep't of Justice), *available at* https://www.gpo.gov/fdsys/pkg/CHRG-112shrg70856/pdf/CHRG-112shrg70856.pdf.

[49] *ACLU v. Department of Justice: ACLU Lawsuit To Uncover Records of Cell Phone Tracking,* ACLU https://www.aclu.org/cases/aclu-v-department-justice (updated Feb. 19, 2014).

has the en banc Eleventh Circuit, which reversed a unanimous three-judge panel of that court holding that a warrant is required. In the Fourth Circuit, a three-judge panel held that a warrant is required, but that decision is being reconsidered by the en banc court. The Third Circuit has ruled that magistrates have the discretion to demand a warrant for location information; a case is pending in the Sixth Circuit; and the government has dropped its appeal to a Ninth Circuit case in which a lower court ruled that a warrant was required.[50] As to real-time cell phone location tracking, the Florida Supreme Court has held that a warrant is required for even short-term tracking, while the Sixth Circuit held that, at least in some circumstances, no warrant is required.[51] Most federal magistrate judges to consider the issue have held that a warrant is required for real-time tracking as a statutory matter, but have not addressed the constitutional questions involved.[52] Thus, absent a Supreme Court examination of this issue, there will continue to be a lack of uniformity among lower courts on the protections that apply to location information. And, courts may continue to lag one step behind the privacy threats that face Americans daily.

V. Congress Should Pass the Geolocation Privacy and Surveillance Act

Given that it will likely take years before the Supreme Court once again considers the constitutionality of location tracking, Congress must act now to ensure that Americans' privacy is protected. For this and the many other reasons set forth herein, the ACLU supports passage of the Geolocation Surveillance and Privacy Act.

Importantly, the Geolocation Surveillance and Privacy Act (H.R. 491) would require a warrant to obtain historical or real-time location information from any entity, unless specific exceptions apply. As such, the bill reflects the long-standing preference by the Supreme Court to "provide clear guidance to law enforcement through categorical rules."[53] Such an approach is preferable to the current environment, where there is inconsistent guidance at the federal and state levels. In addition, this formulation also anticipates future technological developments, in which a variety of third parties are likely to collect and store location information for varying purposes. Thus, the bill allows law enforcement to access this data – but only with appropriate standards.

In addition, the H.R. 491 includes exemptions to the warrant requirement, which preserve the ability of law enforcement to operate in special circumstances. For example, the bill provides exceptions to the warrant requirement to retrieve a lost or stolen phone; where there is not time to secure a warrant; in emergencies where it is reasonable to believe that the life or safety of an individual is threatened; or with consent. Moreover, the bill includes appropriate suppression remedies, in cases in which location information is improperly collected.

---

[50] I*n re* Application of the United States for Historical Cell Site Data, No. 11-20884 (5th Cir. July 30, 2013); United States v. Davis, 785 F.3d 498 (11th Cir. 2015); United States v. Graham, 796 F.3d 332, 360 (4th Cir. 2015) (rehearing en banc granted); *In re* Application of U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to Gov't, 620 F.3d 304 (3d Cir. 2010); United States v.Carpenter, Nos. 14-1572 & 14-1805 (6th Cir.); *In re* Application for Telephone Information Needed for a Criminal Investigation, U.S. Dist. 2015 WL 4594558 (N.D. Cal. 2015).

[51] Tracey v. State, 152 So.3d 504 (Fla. 2014); United States v. Skinner, 690 F.3d 772 (6th Cir. 2012).

[52] *See* United States v. Espudo, 954 F. Supp. 2d 1029, 1035 (S.D. Cal. 2013) (collecting cases).

[53] *Riley*, *supra* note 6 at 2491.

The Geolocation Surveillance and Privacy Act, however, could be strengthened by:

- Including clear rules on the use of Stingrays, and other devices that collect location and other information. These rules should require a warrant to use a Stingray; require timely purging of non-target information; specify the information that must be included in any warrant application; and require prosecutors to notify individuals in cases where information obtained or derived from a Stingray is used;
- Eliminating exceptions that permit the collection of location information without a warrant under provisions of the Foreign Intelligence Surveillance Act, which have been abused to permit bulk collection; and
- Requiring law enforcement agencies' to report statistics on their collection of location information, to facilitate effective oversight.

As Congress considers location-tracking legislation, however, we cannot afford to let the DOJ sit idle. We urge this committee to insist that DOJ take steps to protect the rights of Americans by promptly adopting a policy requiring a warrant to collect real-time and historical location information. Such a policy would reflect Americans' reasonable expectation of privacy; the finding by a majority of the Supreme Court that long-term GPS monitoring infringes on reasonable privacy expectations; and the limits the Fourth Amendment places on government access to Americans' private information.

In addition, the committee should demand that DOJ disclose information on how it is interpreting the *Jones* decision, and publicly release its policies surrounding law enforcement collection of location information. To date, the DOJ has refused to release this information to the public or members of Congress, citing concerns that disclosures could reveal sensitive law enforcement methods. Such concerns, however, are unfounded. Just last year, the DOJ was able to publicly release guidance on the use of Stingrays, without compromising law enforcement activities. Similarly, on an issue of this paramount importance, the DOJ must respond to demands from the public and Congress for greater transparency.

VI. Conclusion

The ACLU agrees with Justice Alito that, in this time of rapid technological change, Congress has an important role to play in regulating the use of surveillance technology by government. Thus, we urge Congress to pass legislation, and in the interim, for the committee to urge DOJ to adopt policy requiring a probable cause warrant to collect historical and real-time location information, disclose information on how it is interpreting *Jones,* and to publically release its policies on law enforcement collection of location information. Such an approach safeguards Americans' privacy interests, while preserving the ability of law enforcement to appropriately access the information necessary to perform their duties.

Published on *American Civil Liberties Union* (https://www.aclu.org)

Neema Singh Guliani [1]

Title / Position:

ACLU Legislative Counsel

Neema Singh Guliani is a legislative counsel with the American Civil Liberties Union Washington Legislative Office, focusing on surveillance, privacy, and national security issues. Prior to joining the ACLU, she worked in the Chief of Staff's Office at DHS, concentrating on national security and civil rights issues. She has also worked as an adjudicator in the Office of the Assistant Secretary for Civil Rights in the Department of Agriculture and was an investigative counsel with House Oversight and Government Reform Committee, where she conducted investigations related to the BP oil spill, contractors in Iraq and Afghanistan, and the Recovery Act. Neema is a graduate of Brown University where she earned a BA in International Relations with a focus on global security and received her JD from Harvard Law School in 2008.

Contact Information:

Source URL: https://www.aclu.org/bio/neema-singh-guliani

Links
[1] https://www.aclu.org/bio/neema-singh-guliani