



Statement of Catherine Crump, Staff Attorney

American Civil Liberties Union

On

The Geolocational Privacy and Surveillance Act

Before the House Judiciary Subcommittee on Crime, Terrorism, and

Homeland Security

May 17, 2012

Good morning Chairman Sensenbrenner, Ranking Member Scott and Members of the Subcommittee. Thank you for the opportunity to testify on behalf of the American Civil Liberties Union, its more than half a million members, countless additional activists and supporters, and fifty-three affiliate organizations nationwide.

The ACLU supports passage of H.R. 2168, the Geolocational Privacy and Surveillance Act. Requiring law enforcement agents to secure a warrant based upon probable cause before obtaining geolocational information would allow legitimate investigations to proceed, while ensuring that innocent Americans are protected from intrusions into their privacy. Passing the GPS Act would fulfill Congress's duty to ensure that the safeguards provided by the Fourth Amendment to the Constitution are respected, and it would allow Americans to preserve the privacy they have traditionally experienced, even as technology advances.

I. Introduction

GPS and cell site technology provide law enforcement agents with powerful and inexpensive methods of tracking individuals over an extensive period of time and an unlimited expanse of space as they traverse public and private areas. In many parts of the country, the police have been tracking people for days, weeks, or months at a time, without ever having to demonstrate to a magistrate that they have a good reason to believe that tracking will turn up evidence of wrongdoing. Today, individuals' movements can be subject to remote monitoring and permanent recording without any judicial oversight. Innocent Americans can never be confident that they are free from round-the-clock surveillance by law enforcement of their activities. As Justice Sonya Sotomayor recently wrote, "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."¹

Congress should pass the GPS Act to require law enforcement agents to secure a warrant based upon probable cause before obtaining geolocational information through GPS or cell site technology. The warrant and probable cause requirements, enshrined in the Fourth Amendment, ensure that an objective magistrate weighs the need to invade privacy when enforcing the law. Requiring a warrant would fulfill Congress's obligation to ensure that the Fourth Amendment's prohibition on unreasonable searches and seizures is respected. Americans' privacy rights are threatened by warrantless access to geolocational information, and history teaches that the executive cannot be counted upon to police itself. The need for the GPS Act is real and immediate, and we urge its passage.

¹ *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J concurring).

II. Current Technologies Allow for Detailed Tracking of Americans' Movements.

Recent technological developments make it possible to obtain geolocational information about the vast majority of Americans with great precision, in both real time and historically, regardless of whether they are tracked through their cell phones or their vehicles, or whether the police obtain GPS or cell site data.

A. Tracking Cell Phones

Over the past decade, cell phones have gone from a luxury good to an essential communications device. As of December 2011, there were more than 311.6 million wireless subscriber accounts in the United States—a number greater than the total U.S. population.² While cell phones are best known as devices used to make voice calls and send text messages, they are also capable of being used as covert tracking devices. As a result, cell phone technology has given law enforcement an unprecedented new surveillance tool. With compelled assistance from mobile phone carriers, the U.S. government now has the technical capability to covertly track any one of the nation's hundreds of millions of cell phone owners, for 24 hours a day, for as long as it likes.

Cell phones yield several types of information about their users' past and present location and movements: cell site location data, triangulation data, and Global Positioning System data. The most basic type of cell phone location information is "cell site" data or "cell site location information," which refer to the identity of the cell tower from which the phone is receiving the strongest signal and the sector of the tower facing the phone. This data is generated because whenever individuals have their cell phones on, the phones automatically scan for nearby cell towers that provide the best reception; approximately every seven seconds, the phones register their location information with the network.³ The carriers keep track of the registration information to identify the cell tower through which calls can be made and received. The towers also monitor the strength of the telephone's signal during the progress of the call to manage the hand-off of calls from one adjacent tower to another if the caller is moving during the call.⁴

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 has increased and the coverage area for each cell tower has shrunk, cell site location information has become more precise.

² CTIA, Wireless Quick Facts, *available at* <http://www.ctia.org/advocacy/research/index.cfm/aid/10323>.

³ *In re the Application of the United States for an Order Directing a Provider of Elec. Comm'n Serv. to Disclose Records to the Gov't*, 534 F. Supp. 2d 585, 589-90 (W.D. Pa. 2008) (Lenihan, M.J.), *rev'd on other grounds*, 620 F.3d 304 (3d Cir. 2010).

⁴ See Declaration of Henry Hodor at 7 n.6, *available at* http://www.aclu.org/pdfs/freespeech/cellfoia_release_4805_001_20091022.pdf

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 individual home or office.⁵ As consumers embrace data-hungry devices such as smartphones, the carriers have installed more towers, each with smaller coverage areas. Further improvement in precision can be expected given the explosive demand for wireless technology and its new services, to the point that “[t]he gap between the locational precision in today’s cellular call detail records and that of a GPS tracker is closing, especially as carriers incorporate the latest technologies into their networks.”⁶ As Professor Matt Blaze testified to Congress in June 2010, “[i]t is no longer valid to assume that the cell sector recorded by the network will give only an approximate indication of a user’s location.”⁷

In addition to cell site information, law enforcement agents can obtain location data at a high level of accuracy by requesting cell phone providers to engage in “triangulation,” which entails collecting and analyzing data of the precise time and angle at which the cell phone’s signal arrives at multiple cell towers. Current technology can pinpoint the location of the cell phone to an accuracy of within 50 meters or less anytime the phone is on, and the accuracy will improve with newer technology.⁸

Finally, a cell phone that has GPS receiver hardware built into it can determine its precise location by receiving signals from global positioning satellites. An increasing number of phones, particularly smartphones, contain such GPS chips, and over half of mobile subscribers are now smartphone users.⁹ Current GPS technology can pinpoint location when it is outdoors, typically achieving accuracy of within 10 meters.¹⁰ With “assisted GPS” technology, which combines GPS and triangulation, it is possible to obtain such accurate location information even when the cell phone is inside a home or a building.

Government requests for cell site location information are usually of two types: historical cell site data, which can be used to retrace previous movements, or prospective cell site data, which can be used to track the phone in real time. The availability of

⁵ *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. (2010) (statement of Professor Matt Blaze at 5), available at <http://judiciary.house.gov/hearings/pdf/Blaze100624.pdf>; Thomas Farely & Ken Schmidt, *Cellular Telephone Basics: Basic Theory and Operation* (2006), http://www.privateline.com/mt_cellbasics/iv_basic_theory_and_operation/

⁶ Statement of Professor Matt Blaze, *supra* n.5, at 13-14.

⁷ *Id.* at 13.

⁸ *Id.* at 10.

⁹ Keith Flagstaff, *Nielson: Majority of Mobile Subscribers Now Smartphone Owners*, Time Techland (May 7, 2012), <http://techland.time.com/2012/05/07/nielsen-majority-of-mobile-subscribers-now-smartphone-owners/>.

¹⁰ Statement of Professor Matt Blaze, *supra* n.5, at 5.

historical information and the length of time this information is stored depend on the policies of the cell phone company. According to an internal Department of Justice document, obtained by the ACLU through a public records act request, cell phone companies store their customers' historical location information for significant periods of time: Verizon stores the cell towers used by a mobile phone for "one rolling year"; T-Mobile keeps this information "officially 4-6 months, really a year or more"; Sprint and Nextel store this data for "18-24 months"; and AT&T/Cingular retains it "from July 2008."¹¹

B. Tracking Vehicles

Just as geolocation data can be gathered from cell phones, so, too, can it be gathered from vehicles. There are a number of ways this can be accomplished. As in the recent Supreme Court case *United States v. Jones*, the government can physically attach a GPS device to a car. In that case, law enforcement agents installed a GPS device on a vehicle and it remained there for 28 days. During this period, the GPS device allowed agents to track the location of the car at every moment. It had an antenna that received signals from satellites; the device used these signals to determine its latitude and longitude every ten seconds, accurately pinpointing its location to within 50-100 feet. Law enforcement agents connected that data to software that plotted the car's location and movements on a map. The software also created a comprehensive record of the car's locations.

However, law enforcement agents do not necessarily need to affix a GPS device to a car in order to track its movements. The increased prevalence of integrated car navigation systems may soon make even this minimal legwork unnecessary. *See, e.g., United States v. Coleman*, No. 07-20357, 2008 WL 495323, at *1 (E.D. Mich. Feb. 20, 2008) (discussing issuance of court order requiring car navigation company to disclose location data to law enforcement).

III. Tracking People's Location Can Invade Their Privacy Because It Reveals a Great Deal About Them.

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. *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.").

¹¹ U.S. Department of Justice, *Retention Periods of Major Cellular Service Providers*, available at <https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart>

In *United States v. Jones*, 132 S. Ct. 945, 954 (2012), 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 nonstop for 28 days. *Id.* at 954. 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. *Id.* at 953-64 (Sotomayor, J., concurring); *see also id.* at 964 (Alito, J., concurring). As Justice Alito explained, “[s]ociety’s expectation has been that law enforcement agents and others would not -- and indeed, in the main, simply could not -- secretly monitor and catalog every single movement of an individual’s car, for a very long period.” *Id.* at 964 (Alito, J., concurring).

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.” *Id.* at 955 (quoting *People v. Weaver*, 12 N.Y.3d 433, 442 (N.Y. 2009)). 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.” *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff’d sub nom. United States v. Jones*, 132 S. Ct. 945 (2012).

There have always been facets of American life that have been uniquely safeguarded from the intrusive interference and observation of government. Geolocational surveillance 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.” *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (quotations omitted).

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.

Jones, 132 S. Ct. at 956 (Sotomayor, J., concurring) (quotations omitted). Chief Judge Kozinski of the U.S. Court of Appeals for the Ninth Circuit has elaborated on this critical point:

I don't think that most people in the United States would agree with the panel that someone who leaves his car parked in his driveway outside the door of his home invites people to crawl under it and attach a device that will track the vehicle's every movement and transmit that information to total strangers. There is something creepy and un-American about such clandestine and underhanded behavior. To those of us who have lived under a totalitarian regime, there is an eerie feeling of déjà vu.

United States v. Pineda-Moreno, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissenting). *See also United States v. Cuevas-Perez*, 640 F.3d 272, 286 (7th Cir. 2011) (Wood, J., dissenting) (“The technological devices available for [monitoring a person’s movements] have rapidly attained a degree of accuracy that would have been unimaginable to an earlier generation. They make the system that George Orwell depicted in his famous novel, *1984*, seem clumsy and easily avoidable by comparison.”).

Furthermore, while the government routinely argues 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.” *In re Application of the U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827, 840 (S.D.Tex. 2010) (citation omitted). A contrary conclusion would eliminate privacy protections even in real-time data, because police officers would be free to use GPS devices to record vehicles’ travels so long as they waited some minutes before accessing those records, thereby rendering them “historical.”

IV. A Warrant and Probable Cause for Location Tracking is Vital to the Constitution and Innovation.

While the Supreme Court held in *Jones* that affixing a GPS monitor and then tracking a suspect’s whereabouts for weeks constitutes a “search” within the meaning of the Fourth Amendment, it did not address whether it is the sort of search that requires a judicial warrant supported by probable cause. It will likely take years for this question to reach the Supreme Court again. Congress should not stand by as law enforcement faces confusion over the rules for obtaining location information and Americans’ privacy rights are violated.

The warrant and probable cause requirements are essential components of the Fourth Amendment. The function of the warrant clause is to safeguard the rights of the innocent by preventing the state from conducting searches solely in its discretion:

Absent some grave emergency, the Fourth Amendment has interposed a magistrate between the citizen and the police. This was done not to shield

criminals nor to make the home a safe haven for illegal activities. It was done so that an objective mind might weigh the need to invade that privacy in order to enforce the law. The right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals. Power is a heady thing; and history shows that the police acting on their own cannot be trusted.

McDonald v. United States, 335 U.S. 451, 455 (1948).

The warrant and probable cause requirements are especially important here given the extraordinary intrusiveness of modern-day electronic surveillance. Without these requirements, the low cost of collecting and storing geolocational information would permit the police to continuously track any driver and cell phone user.

The warrant requirement imposes no great burden on the state. Under the GPS Act, obtaining warrants for geolocational information would be even less burdensome than obtaining them for telephone wiretaps, and the expectation of privacy implicated in placing calls on a public phone is no greater than the expectation that the state will not, absent a warrant, monitor a citizen's every movement continuously for months on end.

In addition congressional action to require a probable cause warrant for location tracking enjoys widespread support from companies and organizations from across the political spectrum including Amazon, the American Library Association, Americans for Tax Reform, AT&T, the Campaign for Liberty, Citizens Against Government Waste, the Competitive Enterprise Institute, the Center for Democracy and Technology, Consumer Action, eBay, Facebook, Freedom Works, Google, HP, IBM, the Information Technology & Innovation Foundation, Intel, the Liberty Coalition, the Newspaper Association of America, Salesforce.com, Tech America, Tech Freedom and Twitter.¹² This list demonstrates that many businesses agree that safeguarding location information is a necessity for American competitiveness and innovation.

V. There Is a Need to Act, and Congress Is the Appropriate Branch of Government to Act.

Congress cannot afford to wait any longer to enact a warrant and probable cause requirement for location tracking. Today Americans' privacy rights are being violated routinely by invasive location tracking, particularly cell phone tracking.

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 tracking cell phones.¹³ The ACLU received over

¹² A full list can be found here: <http://digitaldueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163>

¹³ ACLU, *Cell Phone Location Tracking Public Records Request*,

5,500 pages of documents from over 200 local law enforcement agencies. The responses show that while cell phone tracking is routine, few agencies consistently obtain judicial warrants. The overwhelming majority of the more than 200 law enforcement agencies that provided documents engaged in at least some cell phone tracking. Most law enforcement agencies explained that they track cell phones to investigate crimes. Some said they tracked cell phones only in emergencies, for example to locate a missing person. Only ten said they have never tracked cell phones.

Many law enforcement agencies track cell phones quite frequently. For example, based on invoices from cell phone companies, it appears that Raleigh, N.C. tracks hundreds of cell phones a year. The practice is so common that cell phone companies have manuals for police explaining what data the companies store, how much they charge police to access that data, and what officers need to do to get it.

Most law enforcement agencies do not obtain warrants to track cell phones, and the legal standards used vary widely. For example, police in Lincoln, Neb obtain GPS location data on telephones without demonstrating probable cause. Police in Wilson County, N.C. obtain historical cell tracking data where it is “relevant and material” to an ongoing investigation, a standard lower than probable cause. Yet some police departments do protect privacy by obtaining warrants based upon probable cause when tracking cell phones. For example, police in the County of Hawaii, Wichita, and Lexington, Ky. demonstrate probable cause and obtain a warrant when tracking cell phones. If these police departments can protect both public safety and privacy by meeting the warrant and probable cause requirements, then surely other agencies can as well.

Moreover, it is not just state and local law enforcement agencies that obtain geolocation data under inconsistent standards. The U.S. Attorney’s Offices appear to do so as well. The Department of Justice maintains that the government need not obtain a warrant and show probable cause to track people’s location, with only one exception: real-time GPS and triangulation data. Since at least 2007, DOJ has recommended that U.S. Attorneys obtain a warrant based on probable cause prior to engaging in these forms of cell phone tracking.¹⁴

However, not all U.S. Attorneys Offices obtain a warrant and show probable cause even in the limited circumstances in which DOJ recommends that they do so. Litigation by the ACLU and Electronic Frontier Foundation under the Freedom of Information Act revealed that U.S. Attorney’s Offices in the District of New Jersey and the Southern District of Florida have obtained even the most precise cell tracking

<http://www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-public-records-request>. Supporting documentation demonstrating the factual assertions throughout this section can be found at this webpage.

¹⁴ *Senate Judiciary 2011 ECPA Hearing*, at 7 (testimony of James A. Baker, Assoc. Deputy Attorney Gen., U.S. Dep’t of Justice). *available at* <http://1.usa.gov/IsojNy>.

information without obtaining a warrant and showing probable cause.¹⁵ Because the FOIA focused on only a small number of U.S. Attorney's Offices, it may well be that many other offices also do not follow DOJ's recommendation.

The records the ACLU has obtained from local, state, and federal law enforcement agencies conclusively demonstrate that warrantless geolocation tracking is not a merely a theoretical privacy risk. Americans' privacy rights are violated by warrantless cell phone tracking routinely.

Congress is in a good position to put an end to these violations. In his concurrence in *Jones*, Justice Alito wrote: "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."¹⁶ Moreover, when considering how to apply the Stored Communications Act to government requests to obtain historical cell site location information, the Third Circuit has stated that, "we are stymied by the failure of Congress to make its intention clear."¹⁷

Congress should act not just to protect privacy but also to safeguard law enforcement investigations. Given the changes in Fourth Amendment jurisprudence, law enforcement faces a very uncertain standard for proceeding with searches, operating in emergencies and securing information from telecommunications providers.

Point VI. The GPS Act Would Safeguard Americans' Privacy While Allowing Law Enforcement to Do its Job.

The ACLU supports passage of the GPS Act because it would ensure that law enforcement agents obtain a warrant for geolocation information, subject to certain reasonable exceptions.

The heart of Act is the requirement that "[a] governmental entity may intercept geolocation information or require the disclosure by a provider of a covered service of geolocation information only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure" § 2602(h)((2).

In turn, Federal Rule of Criminal Procedure 41 provides that "a warrant may be issued for any of the following: (1) evidence of a crime; (2) contraband, fruits of crime, or other items illegally possessed; (3) property designed for use, intended for use, or used in committing a crime; or (4) a person to be arrested or a person who is unlawfully restrained."

¹⁵ ACLU, *ACLU v. Department of Justice: ACLU Lawsuit To Uncover Records of Cell Phone Tracking*, Sept. 6, 2011, <http://www.aclu.org/free-speech/aclu-v-department-justice>

¹⁶ 132 S. Ct. at 964.

¹⁷ *In the Matter of the Application of the United States of American for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F.3d 304, 319 (3d Cir. 2010).

Thus, through its incorporation of the Rule 41 standard, the GPS Act strikes a reasonable—and constitutionally necessary—balance between privacy and law enforcement interests. Under this provision, for example, when law enforcement agents have a good reason to believe that tracking the location of a cell phone will turn up evidence of a crime, or that a cell phone was used during the commission of a crime, law enforcement agents will have little difficulty persuading magistrate judges to grant them permission to engage in location tracking.

Further, the GPS Act contains a limited number of exceptions, for:

- Emergency access when “it is reasonable to believe that the life or safety of the person is threatened”;
- Foreign intelligence surveillance covered by the Foreign Intelligence Surveillance Act of 1978;
- Law enforcement emergencies where there is not time to secure a warrant;
- To retrieve lost or stolen phones;
- To allow parents or guardians to monitor children; and
- When the user has consented.

The GPS Act could be strengthened through the inclusion of reporting requirements regarding law enforcement agencies’ collection of geolocation information. To be sure, law enforcement agencies may have a legitimate interest in keeping the details of specific investigations secret, but when it comes to aggregate statistical information about the use of specific surveillance techniques, the public interest is best served through disclosure.

Covert surveillance techniques are by their nature secret, which has important ramifications for the ability of both Congress and the public to engage in oversight. Robust reporting requirements play a valuable role in filling what would otherwise be a void of information regarding the activities of government. For example, each year the administrative office of the courts produces aggregate reports on the use of wiretap authorities by law enforcement agencies. Without revealing any sensitive investigative details, these reports give Congress and the public meaningful insight into the frequency with which the government uses this surveillance technique and the kinds of crimes that they are used to investigate.

Congress simply cannot perform effective oversight without data. For this reason, we urge the co-sponsors of the legislation to implement reporting requirements.

Conclusion

The ACLU agrees with Justice Alito that, in this time of rapid technological change, it is especially appropriate for Congress to step in and regulate the use of surveillance technology by government. The warrant and probable cause requirements strike the appropriate balance, ensuring that legitimate investigations can go forward

without eroding the privacy rights of innocent Americans. We urge the committee to support H.R. 2168 and report it favorably from the committee.