



Statement of Catherine Crump, Staff Attorney

American Civil Liberties Union

On

The Electronic Communications Privacy Act (ECPA), Part 2: Geolocation
Privacy and Surveillance

Before the House Judiciary Subcommittee on Crime, Terrorism, and
Homeland Security

April 25, 2013

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.

Over the past week and a half, our nation has been gripped by the horrific events in Boston. Today our thoughts remain with the victims of this tragedy, with their families and with the diverse spectators and athletes that comprise the Boston Marathon community. Although details of the investigation are still unfolding, it is apparent that electronic surveillance played an important role in locating and tracking the suspected perpetrators. This is as it should be. No one denies that electronic surveillance such as access to mobile phone location data is a valuable law enforcement tool—and indeed, in horrific and rare events such as the Boston Marathon bombings, an essential one. That is why the ACLU has supported and continues to support an exemption in the law, permitting the immediate disclosure of location data to law enforcement agencies in such life and death situations.

However, in routine investigations, law enforcement agencies such as local police and the FBI should secure a warrant based upon probable cause to obtain mobile phone location data. The ACLU supports the Geolocation Privacy and Surveillance Act because the framework it establishes allows law enforcement to access the tools they need, while providing an independent check and balance through a review by a judge which will ensure that innocent Americans do not have their privacy violated.

I. Introduction

Mobile phone technology provides law enforcement agents with an invasive yet inexpensive method of tracking individuals over extended periods of time and unlimited expanses of space as they traverse public and private areas. It also makes it possible for law enforcement agents to identify all individuals located in a specific area—a valuable tool, but one that by necessity reveals the location of vast numbers of innocent Americans. In many parts of the country, the police have been obtaining mobile phone location data for days, weeks, or months at a time, without ever having to demonstrate to an independent judge that they have a good reason to believe that tracking will turn up evidence of wrongdoing.

Congress should reform our electronic privacy laws to require law enforcement agents to secure a warrant based upon probable cause to obtain mobile phone location data. The warrant and probable cause requirements ensure that an objective magistrate determines that there is a good reason to believe that a search will turn up evidence of wrongdoing before mobile phone location data is disclosed. The application of this standard as a routine matter, coupled with immediate disclosure of location data to law enforcement agencies in true emergencies, would ensure that legitimate law enforcement investigations can proceed and that Americans will not suffer undue invasions of their privacy.

II. Mobile Phone Technology Enables Invasive Tracking of Americans' Movements.

Today mobile phone technology makes it possible to obtain location data about the vast majority of Americans with great precision, in both real time and historically. As of June 2012, there were 321.7 million wireless subscriber accounts in the United States—a number greater than the total U.S. population.¹ Mobile phone technology has given law enforcement an unprecedented new surveillance tool. With assistance from mobile phone carriers, the government now has the technical capability to covertly track any one of the nation's hundreds of millions of mobile phone owners, for 24 hours a day, for as long as it likes. Through so-called "tower dumps," it can also identify all of the individuals whose mobile phones used a particular tower—allowing law enforcement agents to infer who was present at a location days, weeks or months after the fact.

A. Types of mobile phone location data available to law enforcement agents

Mobile phones yield several types of information about their users' past and present locations and movements: cell site location data, triangulation data, and Global Positioning System data. The most basic type of mobile 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 connected and the sector of the tower facing the phone. This data is generated because whenever individuals have their mobile phones on, the phones automatically and frequently scan for nearby cell towers that provide the best reception. 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.²

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. As Professor Matt Blaze has testified, 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.³ Customers with poor cell phone coverage in their homes can request that their

¹ CTIA, *Wireless Quick Facts*,
<http://www.ctia.org/advocacy/research/index.cfm/aid/10323>.

² See Decl. of Henry Hodor at 7 n.6, *available at*
http://www.aclu.org/pdfs/freespeech/cellfoia_release_4805_001_20091022.pdf.

³ *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 & Ken

carrier provide them a “femtocell,” a small cellular base station, which can cover just one home.⁴ As consumers embrace data-hungry devices such as smartphones, the carriers have installed more towers, each with smaller coverage areas in order to cope with the demand for data.

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.”⁵ In the words of Professor Blaze, “[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.”⁶

In addition to cell site information, law enforcement agents can obtain location data at a high level of accuracy by requesting mobile phone carriers to engage in “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. Current technology can pinpoint the location of a mobile phone to an accuracy of within 50 meters or less anytime the phone is on, and the accuracy will improve with newer technology.⁷

Finally, a mobile phone that has GPS receiver hardware built into it can determine its precise location by receiving signals from global positioning satellites. Current GPS technology can pinpoint location when it is outdoors, typically achieving accuracy of within 10 meters.⁸

B. Types of government requests for mobile phone data

Law enforcement agents can request two categories of cell site location information: historical cell site data, which can be used to retrace previous movements, or prospective cell site data, which can be used to track mobile phones in real time. The availability of historical information and the length of time this information is stored depend on the policies of the mobile phone carrier. According to an internal Department of Justice document, obtained by the ACLU through a public records act request, mobile phone carriers 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”;

Schmidt, *Cellular Telephone Basics: Basic Theory and Operation*, Private Line (Jan. 1, 2006), http://www.privateline.com/mt_cellbasics/iv_basic_theory_and_operation/.

⁴ Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 Berkeley Tech. L.J. 117, 132 (2012).

⁵ Statement of Professor Matt Blaze, *supra* note 3, at 13-14.

⁶ *Id.* at 13.

⁷ *Id.* at 10.

⁸ *Id.* at 5.

Sprint and Nextel store this data for “18-24 months”; and AT&T/Cingular retains it “from July 2008.”⁹

Law enforcement agencies can obtain data regarding the movements of one or more persons over time, or they can obtain data regarding all of the people whose phones were using a particular tower at a particular time. This latter method of obtaining cell site location information is often referred to as a “tower dump.” Because tower dumps obtain the information of everyone whose phone was using a particular cell phone tower, by their nature they sweep in vast quantities of data about innocent people who will never know that their location data was shared with the government.

Mobile carriers have established automated systems to provide location and other customer data to law enforcement agents. For example, Sprint created a website, which was used to transmit 8 million “pings” of location data in a year.¹⁰ Sprint charges \$30 a month per target for use of its L-Site program to track location.¹¹ Location surveillance is one of the cheapest and easiest, yet most invasive forms of government surveillance.

III. Current Law is Unclear and Inadequately Protective of Privacy.

There is confusion among courts, law enforcement agents and members of the public regarding what legal standard law enforcement agents must meet to obtain mobile phone location data. 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 mobile phone location data. In fact, one federal appellate court struggling to apply the law to a government request for historical cell site location information stated that it was “stymied by the failure of Congress to make its intention clear.”¹²

The ACLU has documented the resulting patchwork of varied and conflicting legal standards. 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.¹³

⁹ 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>.

¹⁰ Pell & Soghoian, *supra* note 4, at 121.

¹¹ Helen A.S. Popkin, *Carriers Charge Cops for Cellphone Information*, NBCNews.com, <http://www.nbcnews.com/technology/technolog/carriers-charge-cops-cellphone-information-656559>.

¹² *In re Application of U.S. for an Order Directing a Provider of Elec. Comm’n Serv. to Disclose Records to Gov’t*, 620 F.3d 304, 319 (3d Cir. 2010).

¹³ Supporting documentation demonstrating the factual assertions throughout this section can be found at ACLU, *Cell Phone Location Tracking Public Records Request* (Mar. 25, 2013), <http://www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-public-records-request>.

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 obtain even GPS data without a warrant based upon probable cause. Police in Wilson County, North Carolina obtain historical cell site location information by proffering only that the data is “relevant and material” to an ongoing investigation. Yet some police departments, including police in the County of Hawaii, Wichita, and Lexington, Kentucky, do secure warrants based upon probable cause to obtain mobile phone location data. 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 mobile phone location data under inconsistent standards. The U.S. Attorney’s Offices appear to do so as well. The Department of Justice recommends that law enforcement agents obtain a warrant based upon probable cause to precise access real-time location data.¹⁴ However, not all U.S. Attorneys Offices comply with this recommendation. 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 the Department of Justice classifies as precise mobile phone location data without obtaining a warrant and showing probable cause.¹⁵

Unfortunately, today the federal government’s policies, procedures and practices for obtaining mobile phone location data are more opaque than ever. In what has been labeled as the most consequential Fourth Amendment decision in a decade, 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.¹⁶ *Jones*, however, left unresolved whether such GPS tracking is the sort of search that requires a warrant based on probable cause. Moreover, the Court did not discuss how its holding would apply to surveillance performed with other technologies such as mobile phone tracking. While FBI General Counsel Andrew Weissmann has explained that the Department of Justice has issued two guidance memoranda setting out its view of how *Jones* affects the constitutionality of various forms of location tracking, neither has been made public despite an ACLU request for them under the Freedom of Information Act. The ACLU has filed suit in federal court to force the release of these memoranda.

¹⁴ *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 <http://1.usa.gov/IsojNy>.

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. 945, 949 (2012)

IV. 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.¹⁷ In *United States v. Jones*,¹⁸ 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.¹⁹ 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.²⁰ 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."²¹

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."²² 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."²³

There have always been facets of American life that 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

¹⁷ 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.").

¹⁸ 132 S. Ct. 945, 954 (2012)

¹⁹ *Id.* at 954.

²⁰ *Id.* at 953-64 (Sotomayor, J., concurring); see also *id.* at 964 (Alito, J., concurring).

²¹ *Id.* at 964 (Alito, J., concurring).

²² *Id.* at 955 (quoting *People v. Weaver*, 12 N.Y.3d 433, 442 (N.Y. 2009)).

²³ *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).

unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse.”²⁴ 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.²⁵

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.²⁶

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*.²⁷

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

²⁴ *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (quotations omitted).

²⁵ See *In re Application of the United States of America for Historical Cell Site Data*, 747 F. Supp. 2d 827, 840 (S.D. Tex. 2010) (“[Cell site location information] will also inevitably be more intrusive [than vehicle GPS tracking], because the phone can be monitored indoors where the expectation of privacy is greatest.”); 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).

²⁶ *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (quotations omitted).

²⁷ *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.”).

person]’s life the government seeks to obtain is no less intimate simply because it has already been painted.”²⁸ It is hard to see how daily requests for historical location differ from continuous real-time tracking.

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 an abortion clinic, a church or at an AA meeting can reveal information that is highly sensitive. 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.”²⁹ 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 mobile phone location data.

V. Congress Should Act to Protect Americans’ Privacy by Imposing a Warrant and Probable Cause Requirement for Mobile Phone Location Data.

Congress is in a good position to protect Americans’ privacy. In his concurrence in *Jones*, Justice Alito wrote: “In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.”³⁰ Given that it will likely take years before the Supreme Court once again considers the constitutionality of location tracking, Congress should not stand by as the privacy of Americans is invaded due to confusion over the rules.

The warrant and probable cause requirements play important roles in safeguarding Americans’ privacy. 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.³¹

²⁸ *In re Application of the U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827, 840 (S.D.Tex. 2010) (citation omitted).

²⁹ *United States v. Karo*, 468 U.S. 705, 707 (1984).

³⁰ 132 S. Ct. at 964.

³¹ *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.

The warrant requirement imposes no unreasonable burden on the law enforcement agents – they obtain these regularly and routinely for searches of homes, vehicles and email accounts. Warrants are a clear and familiar standard, requested by law enforcement and issued by judges for hundreds of years. Moreover, under the GPS Act, obtaining warrants for geolocational information would be even less burdensome than the process law enforcement agencies have followed for decades to obtain telephone wiretaps.

VI. Specific Issues

While privacy advocates and law enforcement agents may disagree about many aspects of law enforcement access to mobile phone location data, it is helpful to start out by identifying points of common ground. The Department of Justice already recommends that its agents obtain a warrant based upon probable cause to engage in precise forms of real-time mobile tracking.³² This is identical to the standard advocated by the ACLU and others pushing for reform, and it is the standard that would be mandated by the GPS Act.

There is disagreement regarding what standard law enforcement should meet to engage in less precise forms of real-time tracking such as cell site location information, but this is an increasingly illusory divide. As Professor Blaze has explained, today cell site location information can be very precise and can place people inside constitutionally protected spaces such as a home. Cell site location information will only get more precise over time. Unless Congress wishes to revisit this issue every few years in order to evaluate the accuracy of current location tracking technology, the standard for all types of real-time location tracking should be the same. That is the only standard that will have any hope of standing the test of time.

There is also disagreement regarding what the standard should be for *historical* location data. Because, as discussed above, people have just as strong a privacy interest in where they have been in the past as they do in where they will go in the future, law enforcement agents should also have to obtain a warrant based upon probable cause to access historical mobile phone location data.

Another area of contention is how to handle law enforcement requests for “tower dump” data. These requests have unique features, in particular the way in which they sweep in the location data about vast numbers of innocent individuals. It is important that law enforcement agencies implement strict minimization and notice requirements so that after the investigation is over, the individuals are told that their data was obtained by

³² See *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 <http://1.usa.gov/Is0jNy>.

law enforcement. Also, law enforcement agencies should not indefinitely retain data on innocent people.

Finally, the ACLU believes that “emergency” must not become a catch-all phrase that allows police to skirt appropriate standards. While obviously legitimate emergencies must be handled quickly, in every case they should be followed by an explanation filed with the court that describes the circumstance of the emergency and certifies that the facts surrounding it are true to the best of the officers’ knowledge.

VII. The ACLU Endorses the GPS Act.

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”³³ 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.”

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.

³³ § 2602(h)(2).

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 nationwide. 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.

Last year, Congress received some data regarding cell phone surveillance after Congressmen Barton and Markey wrote letters to the wireless carriers. Of the four largest carriers, three provided statistics in their responses (T-Mobile declined), revealing that they received 1.3 million requests from law enforcement agencies each year. However, only one company, Sprint Nextel, provided specific data about the location requests it receives.

Congress cannot perform effective oversight of these invasive surveillance powers with data from only one of the four major wireless carriers. Furthermore, as the disclosures were in response to a specific request by two members of Congress, the wireless carriers are not obligated to provide updated data this year.

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.