Written Statement of the
American Civil Liberties Union

Laura W. Murphy
Director
ACLU Washington Legislative Office

Christopher Calabrese
Legislative Counsel
ACLU Washington Legislative Office

Catherine Crump
Staff Attorney
ACLU Speech, Privacy and Technology Project

before the
Senate Judiciary Committee
Subcommittee on Privacy, Technology

May 10, 2011

Hearing on
Protecting Mobile Privacy: Your Smartphones, Tablets,

Cell Phones and Your Privacy

AMERICAN CIVIL LIBERTIES UNION

WASHINGTON LEGISLATIVE OFFICE
915 15th Street, NW Washington, D.C. 20005
(202) 544-1681 Fax (202) 546-0738

Chairman Franken, Ranking Member Coburn, and Members of the Committee:

The American Civil Liberties Union (ACLU) has more than half a million members, countless additional activists and supporters, and fifty-three affiliates nationwide. We are one of the nation's oldest and largest organizations advocating in support of individual rights in the courts and before the executive and legislative branches of government. In particular, throughout our history, we have been one of the nation's foremost protectors of individual privacy. We write today to applaud the committee for its focus on the privacy issues in mobile technologies and to describe the particular need for reform in the use of location tracking information by law enforcement.

While the increased use of smart phones raises a number of privacy issues it is imperative that the committee keep as a central focus law enforcement access to location information. Specifically that all such access should require a warrant issued by a court based on probable cause.

Unregulated location tracking poses a real, immediate, and universal danger to Americans' privacy. Because of the prevalence of mobile phones in modern society, every American is carrying a portable tracking device, one that can be used to reveal his or her current and past location. Whether it is a visit to a therapist or liquor store, church or gun range, many individuals' locations will be available either in real time or months later. Recent reports showing the extent to which Apple iPhones and smartphones running Google's Android operating system have been tracking and storing their users' location information were shocking to many and have created a public outcry. However we cannot focus on these two companies alone. Location tracking practices are widespread and fundamental to the provision of mobile communications services. Because of the sensitivity and invasiveness of location records, law enforcement agents should always be required to obtain a judicially-authorized warrant and show probable cause, no matter the technology employed or the age of the records.

Unfortunately, the government frequently obtains location tracking information without first obtaining a warrant and establishing probable cause. Law enforcement has obtained location information since at least the late 1990's[1] but more than a decade later we still have no uniform standard for when law enforcement can access to this information. While the Department of Justice (DOJ) has issued recommendations setting out when prosecutors should

[1] *See, e.g. United States v. Cell Site*, Case No. 99-00162 (S.D. Tex. Feb. 10, 1999); *United States v. Cell Site Info*, Case No. 00-02871 (S.D. Fl. May 28, 1999).

show probable cause, United States Attorneys are apparently free to ignore these recommendations, and some have chosen to do so. Worse the government seems to have engaged in a coordinated effort to prevent the creation of a uniform standard by refusing to seek appellate court decisions on the issue. This legal maneuvering has prevented public debate and allowed the entrenchment of a practice inconsistent with our constitutional principles.

Congress is the only branch of government that is well-positioned to ensure a respect for privacy in the face of new mobile tracking technologies. The Executive Branch has proven itself unwilling to show probable cause. The courts are not well-equipped to do so because the government chooses not to appeal lower court decisions, thereby frustrating development of the law. Accordingly, Congress must act. While some of the technical details are complicated, the principle is simple: almost every American is carrying a portable tracking device and if Americans are to continue enjoying a robust right of privacy, Congress should update the Electronic Communications Privacy Act (ECPA) to clarify that the government must obtain a warrant based on a showing of probable cause to track these devices.

Current Location Technology

As of December 2010, there were an estimated total of 302 million cell phone service subscribers in the United States.[2] Whenever these subscribers have their cell phones on, the phones automatically scan for the cell tower and the sector of that tower that provides the best reception and, approximately every seven seconds, the phones register their location information with the network.[3] The carriers keep track of the registration information in order 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, in order to manage the hand-off of calls from one adjacent tower to another if the caller is moving during the call.[4]

The cell phone technology yields several types of location information of interest to law enforcement officers. The most basic type of data is "cell site" data, or "cell site location information," which refers to the identity of the cell tower from which the phone is receiving the strongest signal at the time and the sector of the tower facing the phone.[5] This data is less accurate because it relies on simple proximity to a cell phone tower so it can be anywhere from a

---

[2] *See* CTIA The Wireless Association, *CTIA's Semi-Annual Wireless Industry Survey* (2010) at 5, *available at* http://files.ctia.org/pdf/CTIA_Survey_Year_End_2010_Graphics.pdf.

[3] *See 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*, 534 F. Supp. 2d 585, 589-90 (W.D. Pa. 2008) (Lenihan, M.J.), *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *appeal docketed*, No. 08-4227.

[4] *See* Decl. of Henry Hodor at 7 n.6, *available at* http://www.aclu.org/pdfs/freespeech/cellfoia_release_4805_001_20091022.pdf The Hodor Declaration offers a technical overview of how cell tracking is accomplished. The ACLU obtained it pursuant to an ongoing Freedom of Information Act lawsuit that it filed with the Electronic Frontier Foundation to access records related to the government's use of cell phone tracking. *See ACLU v. DOJ*, No. 08-1157 (D. D.C. filed July 1, 2008).

[5] *See, e.g., In the Matter of the Application of the United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Information*, 412 F. Supp. 2d 947, 948-49 (E.D. Wis. 2006) (Callahan, M.J.); *In the Matter of the Application of the United States of America for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking*, 441 F. Supp. 2d 816, 827 (S.D. Tex. 2006) (Smith, M.J.).

200 meter to 30 kilometer (656 feet to 18 miles) radius from the tower.[6] This range is shrinking, as the number of active cellular towers is increasing by 11.5 % each year.[7] Currently some cell sites only cover limited areas, such as tunnels, subways, and specific roadways.[8] 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."[9]

Beyond basic cell site location information, cellular service providers have the capacity and the obligation under the Wireless Communications and Public Safety Act of 1999 to create and disclose even more precise location information for E911 calls.[10] Cell phone providers generate this data in two ways. First, under the "network-based approach," the providers triangulate information regarding the strength of the signals from the cellular towers nearest to the phone.[11] Under Federal Communications Commission (FCC) guidelines, this information must be accurate within 100 meters for 67% of calls and within 300 meters for 95% of calls by 2012.[12]

The second approach is to track the location of the cell phone using its GPS capabilities.[13] The FCC requires the GPS to be accurate within 50 meters for 67% of calls and within 150 meters for 95% of calls by 2012.[14] This GPS is often much more accurate, frequently within a few meters.[15]

The recent reports of Google's and Apple's location tracking practices show the detail of information companies are capable of collecting. Security analyst Samy Kamkar found that an HTC Android phone collected location information every few seconds and transmitted the data to Google at least several times an hour.[16] In addition to the location, the phone was transmitting the name, location and signal strength of nearby Wi-Fi networks and a unique phone identifier. Apple says it "intermittently" collects location data, including Wi-Fi networks and transmits that data to itself every 12 hours. It was impossible to disable the tracking file on iPhone even when disabling location services. [17]

---

[6] But sometimes, depending on topography or other impediments to transmission, a phone receives the strongest signal from a cellular tower other than the one that is closest to it. Hodor Decl., *supra*, at 7-8.
[7] *See* CTIA, *supra*, at 9.
[8] *See* Thomas Farley and Ken Schmidt, *Cellular Telephone Basics: Basic Theory and Operation*, http://www.privateline.com/mt_cellbasics/iv_basic_theory_and_operation/ (last accessed Dec. 21, 2009).
[9] Hearing on ECPA 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 13-14), http://judiciary.house.gov/hearings/pdf/Blaze100624.pdf (hereinafter, "Blaze testimony").
[10] Pub. L. No. 106-81, 113 Stat. 1286 (1999)
[11] *See* Note, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 Harv. J. L. & Tech. 307, 308-10 (2004); *See, e.g.*, *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 749-51 (S.D. Tex. 2005) (Smith, M.J.).
[12] 47 C.F.R. § 20.18(h)(1)(i).
[13] *See Who Knows Where You've Been?*, *supra*, at 308.
[14] 47 C.F.R. § 20.18(h)(1)(ii).
[15] Mario Aguilar, *GPS Power-Up: Get Ready for New Sense of Place*, Wired, April 19, 2010
[16] Valetino-Devries, Jennifer, *IPhone Stored Location in Test Even if Disabled*, Wall Street Journal, April 25, 2011
[17] *Id.*

In addition some of the most popular "apps" are selling users' personal information including GPS location to third parties. Earlier this year the popular online radio service Pandora, received a subpoena from a federal grand jury investigating whether they were sharing information about their users with advertisers and other third parties. Last month the Wall Street Journal reported that 47 apps transmitted the phone's location in some way.[18]

This tracking is likely to become even more accurate in the near future. As discussed above, the number of cell towers is increasing rapidly. [19] Furthermore, "[GPS] technology is rapidly improving so that any person or object . . . maybe tracked with uncanny accuracy to virtually any interior or exterior location, at any time and regardless of atmospheric conditions."[20]

Current Legal Practices for Accessing Location Information

Unfortunately, it remains unclear under what circumstances federal prosecutors obtain a warrant and show probable cause to access cell phone location information, and under what circumstances courts have held that this is the legal minimum showing and process required under the law. Although DOJ has issued guidelines for prosecutors that require probable cause in some circumstances, these are not consistently followed. Because the vast majority of judicial decisions on point are sealed, and those limited number that are public are in conflict, the state of the law is unclear. Federal prosecutors generally decline to appeal adverse rulings to circuit courts. Clarity is unlikely anytime soon unless Congress acts.

Department of Justice Standards

The Department of Justice asserts it should have access to most kinds of location information without having to obtain a warrant and show probable cause. Instead, DOJ argues that the government should be able to obtain most cell phone location information by demonstrating to a judge or magistrate only that the information is relevant and material to an ongoing criminal investigation. According to testimony before this committee and a document obtained by the ACLU and the Electronic Frontier Foundation (EFF) through a FOIA request, it is DOJ's policy to obtain mobile location information under the following standards:[21]

	Historical Records	**Real-time Surveillance**
Cell-site data	Relevant and material	Relevant and material

[18] Efrati, Thurm, and Searcey, *Mobile-App Makers Face U.S. Privacy Investigation*, Wall Street Journal, April 5, 2011

[19] *See* CTIA, *supra*, at 9.

[20] *People v. Weaver*, 12 N.Y.3d 433, 441 (N.Y. 2009).

[21] Mark Eckenweiler, *Current Legal Issues In Phone Location*, slide 20, *available at* http://www.aclu.org/pdfs/freespeech/18cellfoia_release_CRM-200800622F_06012009.pdf and U.S. Congress, Hearing of the Senate Judiciary Committee, The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age, Written Statement of Associate Deputy Attorney General James A. Baker, April 6, 2011.

GPS, triangulation	N/A (because usually doesn't exist)	Probable cause

According to internal DOJ documents, the Department 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 around the country obtain a warrant based on probable cause prior to engaging in these forms of cell phone tracking.[22]

In testimony before this Committee, DOJ has amplified that position by saying: "When prosecutors seek to obtain prospective E-911 Phase II geolocation data (such as that derived from GPS or multilateration) from a wireless carrier, the Criminal Division of the Justice Department **recommends** the use of a warrant based on probable cause" (emphasis added).[23] Focusing attention on the word 'recommends' is critical because 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.[24] The ACLU's and EFF's FOIA litigation revealed that U.S. Attorneys' offices in the District of New Jersey and the Southern District of Florida have obtained even the most precise cell tracking information without obtaining a warrant and showing probable cause.[25] Because the FOIA focused on only a small number of U.S. Attorneys' offices around the country, it may well be that many other offices also do not follow DOJ's recommendation.

In fact, this practice may be widespread. There are no published legal opinions on the lawfulness of warrantless cell phone tracking in either the District of New Jersey or the Southern District of Florida, and yet the FOIA litigation proved conclusively that cell phone tracking occurs in those districts and indeed that federal prosecutors do not feel obligated to show probable cause even where DOJ recommends it. In the vast majority of judicial districts in this country, there are no decisions addressing cell phone tracking, yet cell phone tracking was occurring in every district subject to the FOIA, even where there is no published opinion setting out the circumstances in which the practice is permissible.[26] Given that cell phone tracking is now a decades-old law enforcement technique that has proven useful, we must assume authorities use it in all or essentially all parts of the country, most frequently under an unknown standard.

Procedures for Gathering Location Information

[22] Email from Brian Klebba, *GPS or "E-911-data" Warrants*, November 17, 2009, *available at* http://www.aclu.org/pdfs/freespeech/cellfoia_dojrecommendation.pdf.
[23] U.S. Congress, Hearing of the Senate Judiciary Committee, The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age, Written Statement of Associate Deputy Attorney General James A. Baker, April 6, 2011.
[24] Letter from William G. Stewart II, to ACLU, *Mobile Phone Tracking (Items 3-5)/DNJ*, Dec. 31, 2008, *available at* http://www.aclu.org/pdfs/freespeech/cellfoia_released_074132_12312008.pdf; Letter from William G. Stewart II to Catherine Crump, *Mobile Phone Tracking(Items 3-5)FLS*, Dec. 31, 2008, *available at* http://www.aclu.org/pdfs/freespeech/cellfoia_released_074135_12312008.pdf.
[25] *Id.*
[26] http://www.aclu.org/free-speech/aclu-lawsuit-uncover-records-cell-phone-tracking

The reason there is so little information available arises in part from the unique procedural posture in which cell phone tracking applications reach courts. For legitimate reasons, applications to track cell phones are often filed under seal. Law enforcement agents sometimes need to prevent the targets of government surveillance from learning that they are investigative subjects.

However, the orders granting or denying surveillance applications also are often also filed under seal, routinely with the notation "until further order of the Court."[27] Because there is no end date on sealing, and no one other than the government and court know the contents of the order, in most cases there is no one with both the motivation and the knowledge to move to unseal them. Public access to the courts would be better served were judges to require that redacted copies of both the applications and orders be filed publicly. This would allow the public to know the legal standards applied by the courts.

This is an unfortunate break with the usual working of the judiciary, where a commitment to transparency is not only embodied in the common law right of access but also constitutionally required by the First Amendment.[28] Some magistrate judges such as the Honorable Stephen Wm. Smith, who has testified before Congress on the issue, are notable exceptions to this trend. Judge Smith has issued an opinion putting an end to indefinite sealing of the surveillance orders he is called upon to issue.[29]

Ex parte adjudication of cell phone tracking applications also contributes to the dearth of published legal opinions on the subject. Ex parte proceedings – when the government presents its arguments in favor of surveillance without presentation of any opposing argument – will favor unpublished decisions because there is no motivation for the only party present, the government, to ask the court to issue a public decision. The ACLU and others have tried to remedy the situation by offering to submit amicus briefs to present the pro-privacy viewpoint. Unfortunately, because many applications for surveillance are so time-sensitive that they must be acted on immediately, some judges have taken the position that there is unlikely to be a practical way to permit amicus participation.[30]

Reaction from the Judiciary

From the few published opinions available, it is apparent that courts do not always find in favor of the government position that it need not obtain a warrant based on probable cause for some forms of cell phone tracking. In fact, the government frequently loses. A "strong majority" of district and magistrate judges have concluded in recently published opinions that the government lacks statutory authority to obtain real-time cell site location without a showing of

---

[27] *In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 878 (S.D. Tex. 2008) (Smith, J.)

[28] *Press-Enterprise Co. v. Superior Court of California*, 478 U.S. 1, 8 (1986)

[29] *In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 891 (S.D. Tex. 2008) (Smith, J.) (holding that "documents authored or generated by the court itself" are entitled to heightened public access rights)

[30] *See, e.g.*, Letter from Hon. David Martin and Hon. Lincoln Almond to ACLU, *Cell phone tracking*, Mar. 12, 2010 (on file with author).

probable cause.[31] Because the government has never followed through on an appeal of an adverse decision addressing real-time tracking, no circuit court has had the opportunity to review these holdings.

The government did appeal an adverse decision addressing historical information. In a decision joined by all of the magistrate judges in the Western District of Pennsylvania, a magistrate judge there held that government requests for court orders requiring mobile carriers to disclose their customers' location information must be based upon probable cause.[32] After the decision was summarily affirmed by the district court, the government appealed to the Third Circuit. In a decision issued this month, the circuit concluded that judges have "the option to require a warrant showing probable cause," although it cautioned that "it is an option to be used sparingly."[33]

Until the action by the magistrate judges in the Western District of Pennsylvania forced the government's hand – by making it impossible to get an order under the "relevant and material" standard in that district –a location tracking case had never been appealed to the appellate court in any circuit. By not appealing, federal prosecutors avoid binding precedent which might tie the government's hands in further cases.[34] Decisions by magistrate judges and district court judges are not binding precedent, even on other judges of the same district court.[35] So long as there are at least some judges in a district who believe that warrantless cell phone tracking is permissible, the government will be able to get its applications approved at least some of the time.

This is exactly the situation in the Southern District of New York, where one district court judge has approved warrantless real-time cell phone tracking in the absence of probable cause and another has held that probable cause is required.[36] Although the government initially filed a notice of appeal with regard to the adverse ruling, after the ACLU received permission to submit an amicus brief in the Second Circuit, the government sought and obtained multiple extension requests and then voluntarily dismissed its appeal.[37] Judges in the Eastern District of

---

[31] *In re Applications of the United States of America for Orders Pursuant to Title 18, United States Code, Section 2703(d)*, 509 F. Supp. 2d 76, 78 (D. Mass. 2007) (Stearns, D.J.).

[32] *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*, 534 F.Supp.2d 585, 585-86 (W.D. Pa. 2008).

[33] *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*, No. 08-4227, ___F.3d ___ (3d Cir. Sept. 7, 2010).

[34] *In the Matter of the Application of the United States of America for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking*, 441 F. Supp. 2d 816, 827-28 (S.D. Tex. 2006) (Smith, M.J.).

[35] *Federal Trade Commission v. Tariff*, 584 F.3d 1088, 1092 (D.C. Cir. 2009).

[36] *Compare In re: Application of the United States of America for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone*, 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (Kaplan, D.J.) *with In the Matter of an Application of the United States of America for an Order Authorizing the Use of a Pen Register With Caller Identification Device Cell Site Location Authority on a Cellular Telephone*, 2009 WL 159187 (S.D.N.Y. 2009) (McMahon, D.J.).

[37] *In re application for a cell site order*, Case No. 09-0807 (2d Cir. docketed Feb. 27, 2009).

New York also split on the question, and only prosecutors and the courts know how this issue is handled in the majority of the country where there are no published opinions.[38]

The state of the law regarding cell phone tracking is characterized by secrecy and contradictory rulings. This is precisely the opposite of the uniformity and openness that are cornerstones of the rule of law in the United States.

Resulting Harms

In addition to frustration and lack of transparency, this low legal standard has already led to misuse by law enforcement. A recent *Newsweek* article highlighted the problem:

> Some abuse has already occurred at the local level, according to telecom lawyer Gidari. One of his clients, he says, was aghast a few years ago when an agitated Alabama sheriff called the company's employees. After shouting that his daughter had been kidnapped, the sheriff demanded they ping her cell phone every few minutes to identify her location. In fact, there was no kidnapping: the daughter had been out on the town all night. A potentially more sinister request came from some Michigan cops who, purportedly concerned about a possible "riot," pressed another telecom for information on all the cell phones that were congregating in an area where a labor-union protest was expected.[39]

It is likely that these examples are the simply the tip of the iceberg. As described extensively above, much of this tracking is happening in secret and for the most part the parties involved don't have any incentive to draw attention to it: law enforcement wants to limit discussion of their investigatory techniques and telecommunications carriers are afraid of spooking their customers.

In addition to abuse, location tracking has also led to the creation of an entire surveillance apparatus, much of it outside the public view. It came to light last year that:

> Sprint Nextel has even set up a dedicated Web site so that law-enforcement agents can access the records from their desks—a fact divulged by the company's "manager of electronic surveillance" at a private Washington security conference last October. "The tool has just really caught on fire with law enforcement," said the Sprint executive, according to a tape made by a privacy activist who sneaked into the event.[40]

This allows detailed disclosure of an individual's movements to law enforcement with a click of a mouse.

---

[38] *Compare* 396 F. Supp. 2d 294 (E.D.N.Y. 2005) (Orenstein, M.J.) (probable cause for prospective tracking) *and* 2009 WL 1530195 (E.D.N.Y. 2009) (Pollak, M.J.), (probable cause for prospective tracking, reversed by Judge Garaufis) *with* 2009 WL 1594003 (E.D.N.Y. 2009) (Garaufis, D.J.) (no probable cause necessary for prospective tracking).

[39] Michael Isikoff, *The Snitch in Your Pocket*, Newsweek, Feb. 19, 2010.

[40] *Id*.

In the most recent example, the ACLU and EFF filed an amicus brief last year in the case of *U.S. v. Soto*.[41] The FBI sought and received tracking information without a warrant, not just for the criminal defendant, but for *about 180 other people*. Because the government's surveillance application is apparently under seal, the details remain unclear. But it appears that the government took the dragnet approach of getting location information for a large number of innocent people in order to figure out the very small number of people who were involved in the underlying crime.

This is even more troubling in light of the FBI policy on record retention. This exchange is from FBI Director Robert Mueller's appearance before an oversight hearing of the House Judiciary Committee in May 2009:

> Mr. NADLER. You keep for 20 years information about innocent people, private information that you have collected in the course of an investigation in which it turns out they had nothing to do with.
> Mr. MUELLER. We may well undertake an—an allegation may come in as to the involvement of a person in a mortgage fraud scheme. We go and investigate, find that that person is innocent, the allegation is false, we keep those records, yes.[42]

So the collection of the movements and habits of innocent people – regardless that it has no bearing on a criminal investigation - will remain part of an FBI profile for 20 years.

The mass tracking in *Soto* is not an isolated incident of overreaching by the FBI. It is just one manifestation of the "communities of interest" approach the government has adopted to tracking down criminals. According to Albert Gidari's testimony before the House Judiciary Committee last year:

> The following issues are faced by service providers every day in response to government demands for acquisition and use of location Information:
>
> …
>
> d. Target v. Associates (hub and spokes). Regardless of the legal standard applicable to the target phone, what standard applies to obtain the location information for all those with whom the target communicates? **It is common in hybrid orders for the government to seek the location of the community of interest – that is, the location of persons with whom the target communicates** (emphasis added). [43]

[41] Brief of Amici Curiae in Support of Motion To Suppress, *United States v. Soto*, Case No. 09-cr-200 (D. Conn. June 18, 2010), *available at* http://www.aclu.org/files/assets/2010-6-18-USvSoto-AmiciBrief.pdf.
[42] *Federal Bureau of Investigation: Hearing Before the H. Judiciary Comm.*, 111th Cong. 35-36 (2009) (statement of Robert Mueller, Director, FBI).
[43] *Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights and Civil Liberties*, 111th Cong. (2010) (statement of Albert Gidari, Partner, Perkins Coie LLP).

This type of mass, generalized surveillance raises the prospect that the movements and habits of many innocent people are tracked and stored for decades.[44]

Conclusion

It has been, and continues to be, the practice of the government to obtain very private and sensitive information based on a very low legal standard – relevance and materiality – and, at least in the case of the FBI, to store it for decades. The government has gone to great lengths to preserve this authority, even to the extent of giving up the power in particular cases, in order to continue to submit secret motions in jurisdictions around the country.

The information in question reveals individual movements for months or years and potentially reveals personal information across a broad range of subjects from medical information (visits to a therapist or an abortion clinic) to First Amendment protected activity (attendance at a church or political protest) to personal habits (visits to a gun range or bar).

There is a compelling need for Congress to act in this case. It must amend ECPA in order to move from a confusion of legal standards that serve the American public very poorly to a uniform probable cause standard which respects the intent of the Founding Fathers and the Fourth Amendment.

[44] It may be that the problem is actually *worse* than described here. In a report on the misuse of exigent letters the Department of Justice Inspector General describes widespread requests for community of interest information. Apparently it was part of "boilerplate" request language for at least some National Security Letters. *A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records*, Inspector General, Department of Justice, January 2010 at 56. Further according to an Office of Legal Counsel opinion there may be some telephone records that the FBI can access without any process under ECPA. *Id*. at 264.