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
House Judiciary Committee
Constitution, Civil Rights, and Civil Liberties Subcommittee

June 24, 2010

Hearing on

ECPA Reform and the Revolution in Location Based Technologies and Services

ACLU
AMERICAN CIVIL LIBERTIES UNION

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

Chairman Nadler, Ranking Member Sensenbrenner, 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 continued focus on the need to modernize the Electronic Communications Privacy Act (ECPA) and ask the committee to reform ECPA to require a warrant based on probable cause for the use of location tracking information by law enforcement.

The danger posed by unregulated location tracking to American's privacy is real, immediate and universal. Because of the prevalence of mobile phones in modern society, almost every American is carrying a portable tracking device, one that can be used to reveal their current and past locations. These devices store their every move. 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. Because of the sensitivity and invasiveness of these records, law enforcement agents should always be required to obtain a 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 1990s[1] but more than a decade later we still have no uniform standard for when law enforcement can gain access to this information. While the Department of Justice has issued recommendations setting out when prosecutors should show probable cause, Freedom of Information Act requests (FOIAs) by the ACLU demonstrate that United States Attorney Offices are ignoring these recommendations at least in some cases. Worse, the government has effectively prevented 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 a practice that is inconsistent with our constitutional principles to become entrenched.

Congress is the only branch of government that is well-positioned to make sure that privacy is respected in the face of new mobile tracking technologies. The Executive has proven

[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).

itself unwilling to require a voluntary showing of probable cause. The courts are ill-equipped to do so because the government chooses not to appeal decisions, frustrating development of the law.

Congress must act. While some of the technical details are complicated, the principle is simple. Almost every American carries a portable tracking device. If Americans wish to continue to enjoy a robust right of privacy, Congress must update ECPA to compel the government to obtain a warrant and show probable cause before tracking cell phones.

Background

As of June 2009, there were an estimated total of 277 million cell phone service subscribers in the United States – about 90% of the overall population.[2] Whenever these subscribers have their cell phones on, the phones automatically scan for cell towers 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 200 meter to 30 kilometer (656 feet to 18 miles) radius from the tower.[6] This range is shrinking,

---

[2] As of June 2009, there were an estimated 276,610,580 wireless phone subscribers in the United States. *See* CTIA The Wireless Association, *CTIA's Semi-Annual Wireless Industry Survey* (2009) at 5, *available at* http://files.ctia.org/pdf/CTIA_Survey_Midyear_2009_Graphics.pdf (last viewed Nov. 14, 2009). The Central Intelligence Agency estimates that the United States population in July 2009 was 307,212,123. *See* Central Intelligence Agency, The World Factbook: United States, https://www.cia.gov/library/publications/the-world-factbook/geos/us.html (last viewed Nov. 18, 2009).

[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.).

[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.

as the number of active cellular towers is increasing by 11.5 % each year.[7] Some cell sites already cover only limited areas, such as tunnels, subways, and specific roadways.[8]

Beyond 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 in certain emergencies.[9] 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.[10] Under the Federal Communications Commission (FCC) guidelines this information must be accurate within 100 meters for 67% of the calls and within 300 meters for 95% of the calls by 2012.[11]

The second approach is to track the location of the cell phone using its GPS capabilities.[12] The FCC requires the GPS to be accurate within a minimum of 50 meters for 67% of calls and within 150 meters for 95% of calls by 2012.[13] This GPS is often much more accurate, frequently within a few meters.[14]

This tracking is likely to become even more accurate in the near future. As discussed above, the number of cell towers is increasing rapidly. [15] Furthermore, "[GPS] technology is rapidly improving so that any person or object . . . may be tracked with uncanny accuracy to virtually any interior or exterior location, at any time and regardless of atmospheric conditions."[16]

Current Legal Practices for Accessing Location Information

Layered on top of the variety of technologies which enable location tracking is a hodgepodge of statutes and legal precedents. Congress' failure to protect the privacy of location information through legislation combined with DOJ's aggressive assertion of entitlement to this same information has generated confusion and disagreement over the appropriate standard for accessing such information.

Department of Justice Standards

The Department of Justice asserts it should have access to enormous amounts of location information without having to obtain a warrant and show probable cause. Instead, DOJ argues

---

[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] Pub. L. No. 106-81, 113 Stat. 1286 (1999)
[10] *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.).
[11] 47 C.F.R. § 20.18(h)(1)(i).
[12] *See Who Knows Where You've Been?*, *supra*, at 308.
[13] 47 C.F.R. § 20.18(h)(1)(ii).
[14] Mario Aguilar, *GPS Power-Up: Get Ready for New Sense of Place*, Wired, April 19, 2010
[15] *See* CTIA, *supra*, at 9.
[16] *People v. Weaver*, 12 N.Y.3d 433, 441 (N.Y. 2009).

that the government can obtain most cell phone location information by demonstrating to a judge or magistrate that the information is relevant and material to an ongoing criminal investigation. According to 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[17]:

	Historical Records	Prospective Surveillance
Cell-site data	Relevant and material	Relevant and material
GPS, triangulation	N/A (because usually doesn't exist)	Probable cause

The DOJ 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 precise cell phone tracking.[18]

This policy position turns out to be more disturbing because some U.S. Attorney offices don't comply even with this very lax set of guidelines.[19] The ACLU's and EFF's FOIA litigation revealed that U.S. Attorney Offices in the District of New Jersey and the Southern District of Florida both obtain even the most precise cell tracking information without obtaining a warrant and showing probable cause.[20] 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 ignore 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 for even the most invasive forms of this surveillance. In the vast majority of judicial districts in this country, there are no decisions addressing cell phone tracking, yet there was cell phone tracking occurring in every district subject to the FOIA, even where there is no published opinion.[21] 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 of the country, most frequently under an unknown standard.

---

[17] Mark Eckenweiler, *Current Legal Issues In Phone Location*, slide 20, available at http://www.aclu.org/pdfs/freespeech/18cellfoia_release_CRM-200800622F_06012009.pdf.

[18] Email from Brian Klebba, *GPS or "E-911-data" Warrants*, November 17, 2009, available at http://www.aclu.org/pdfs/freespeech/cellfoia_dojrecommendation.pdf

[19] Letter from William G. Stewart II, to Catherine Crump, *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

[20] *Id.*

[21] http://www.aclu.org/free-speech/aclu-lawsuit-uncover-records-cell-phone-tracking

Procedures for Gathering Location Information

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. We acknowledge that law enforcement agents have legitimate interests in preventing the targets of government surveillance from learning that they are investigative subjects.

However, the orders granting or denying surveillance applications are often also filed under seal. These orders could be issued publicly, with any law enforcement sensitive information redacted, so the public is at least privy to the legal standards applied by the courts. Not only is this not standard practice, these orders and applications are routinely ordered sealed "until further order of the Court."[22] Because no one other than the court and the government know about these surveillance applications in most cases, and because the government has no motivation to move to unseal the orders, secrecy is the norm and disclosure is the exception.

This is an unfortunate break with the usual working of the judiciary, where a commitment to transparency is not only honored but also constitutionally required by the First Amendment.[23] One judge, the Honorable Stephen Smith, who is testifying before the committee, is a notable exception to the secrecy trend. He has issued a forward-thinking opinion putting an end to indefinite sealing of the surveillance orders he is called upon to issue.[24] Judge Smith's practice should be the norm.

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 render 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 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.[25] As long as the judicial system continues to proceed in a manner that favors one side over the other, it emphasizes the need for a full, open and fair debate about the propriety of warrantless cell phone tracking in Congress.

Reaction from the Judiciary

---

[22] *In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 891 (S.D. Tex. 2008) (Smith, J.)

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

[24] *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" is entitled to heightened public access rights)

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

From the limited published opinions available, it is apparent that courts do not always find in favor of the government position. In fact, the government frequently loses. The "strong majority" of district and magistrate judges have concluded in recently published opinions that the government lacks statutory authority to obtain prospective cell site location without a showing of probable cause.[26] In one of the few published decisions regarding government access to historical cell site location information, the Western District of Pennsylvania—with all magistrate judges signing the opinion—held that the government must obtain a warrant to access this information, in part because such applications raise constitutional concerns.[27] That decision, which was affirmed by the district court,[28] is now on appeal in the Third Circuit.

Until the action by the magistrate judges in Pennsylvania forced the government's hand – by making it impossible to get an order under a relevance standard in that district – a location tracking case had never been appealed to the appellate court in any circuit. In what seems to be the formal policy of the Department of Justice, adverse decisions on whether to grant cell tracking orders are not appealed from the magistrate and district court level – in spite of express requests from some magistrate and district court judges – in order to avoid binding precedent which might tie the government's hands in further cases.[29]

This highlights the lengths the government will go to maintain a relevance standard. A valuable law enforcement technique is being disallowed repeatedly and the government is taking no appellate action. Decisions by magistrate judges and district court judges are not binding precedent, even on other judges of the same district court.[30] 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 application 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.[31] Although the government initially filed a notice of appeal on the adverse ruling adverse, after the ACLU received permission to submit an amicus brief in the Second Circuit, the government sought and obtained multiple

---

[26] *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.); see W.D. Penn 2008 (Lenihan), 534 F. Supp. 2d at 600-01 (listing majority opinions holding that real-time cell site information cannot be obtained without a Rule 41 warrant)

[27] *Id.* at 616 (citing *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005)).

[28] *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. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008).

[29] *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.).

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

[31] Compare In re: Application of the United States of Americafor 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 Americafor 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.).

extension requests and then voluntarily dismissed its appeal.[32] Judges in the Eastern District of 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.[33]

The government is using secrecy, inconsistent rules, and procedural tactics to obtain invasive information with an inconsistent – but frequently very low – evidentiary standard. This is precisely the opposite of the uniformity and openness that are cornerstones of the rule of law in the United States.

Resulting Harms

These practices have trampled on the rights of Americans and led to misuse. 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."[34]

It is likely that these examples are the simply the tip of the iceberg. As noted above, much of this tracking is happening in secret and the parties involved typically don't have any incentive to draw attention to it. Law enforcement officials want to limit discussion of their investigatory techniques and telecommunications carriers are afraid of spooking their customers.

In addition to abuse, location tracking has led to the creation of an entire surveillance apparatus, much of it outside the public view. It has recently come to light 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."[35]

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

---

[32] In re application for a cell site order, Case No. 09-0807 (2d Cir. docketed Feb. 27, 2009).
[33] *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);
[34] Michael Isikoff, *The Snitch in Your Pocket*, Newsweek, Feb. 19, 2010.
[35] *Id*.

In the most recent example, the ACLU and EFF filed an amicus brief on June 18, 2010 in the case of *U.S. v. Soto*.[36] In this case the FBI sought and received tracking information without a warrant, not just for the criminal defendant, but for *about 180 other people*. Although the details remain unclear because the government's surveillance application is apparently under seal, it appears that the government took the dragnet approach of getting location information for a large number of innocent people to try to figure out who was involved in the crime.

This is even more troubling in light of the FBI policy on record retention. In an oversight hearing of the full House Judiciary Committee in May 2009, FBI Director Mueller addressed the issue:

> "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."[37]

So the collection of the movements and habits of innocent people 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 this committee last month:

> "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) [38]

This type of mass, generalized surveillance raises the prospect that the movements and habits of many innocent people are tracked and stored for decades.[39]

---

[36] 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.
[37] *Federal Bureau of Investigation: Hearing Before the H. Judiciary Comm.*, 111th Cong. 35-36 (2009) (statement of Robert Mueller, Director, FBI).
[38] *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).
[39] 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*

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, 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 standard: a warrant based on probable cause that respects the intent of the Founding Fathers and the Fourth Amendment.

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.