ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA) (PART II): GEOLOCATION PRIVACY AND SURVEILLANCE

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, HOMELAND SECURITY, AND INVESTIGATIONS

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

APRIL 25, 2013

Serial No. 113–34

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE

80–542 PDF WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

BOB GOODLATTE, Virginia, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
STEVE CHABOT, Ohio
SPENCER BACHUS, Alabama
DARRELL E. ISSA, California
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
MARK AMODEI, Nevada
RAÚL LABRADOR, Idaho
BLAKE FARENTHOLD, Texas
GEORGE HOLDING, North Carolina
DOUG COLLINS, Georgia
RON DeSANTIS, Florida
[Vacant]

JOHN CONYERS, JR., Michigan
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
JUDY CHU, California
TED DEUTCH, Florida
LUIS V. GUTIERREZ, Illinois
KAREN BASS, California
CEDRIC RICHMOND, Louisiana
SUZAN DelBENE, Washington
JOE GARCIA, Florida
HAKEEM JEFFRIES, New York

SHELLEY HUSBAND, *Chief of Staff & General Counsel*
PERRY APELBAUM, *Minority Staff Director & Chief Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, HOMELAND SECURITY, AND INVESTIGATIONS

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*
LOUIE GOHMERT, Texas, *Vice-Chairman*

HOWARD COBLE, North Carolina
SPENCER BACHUS, Alabama
J. RANDY FORBES, Virginia
TRENT FRANKS, Arizona
JASON CHAFFETZ, Utah
TREY GOWDY, South Carolina
RAÚL LABRADOR, Idaho

ROBERT C. "BOBBY" SCOTT, Virginia
PEDRO R. PIERLUISI, Puerto Rico
JUDY CHU, California
LUIS V. GUTIERREZ, Illinois
KAREN BASS, California
CEDRIC RICHMOND, Louisiana

CAROLINE LYNCH, *Chief Counsel*
BOBBY VASSAR, *Minority Counsel*

CONTENTS

APRIL 25, 2013

ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA) (PART II): GEOLOCATION PRIVACY AND SURVEILLANCE

THURSDAY, APRIL 25, 2013

HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON CRIME, TERRORISM, HOMELAND SECURITY, AND INVESTIGATIONS

COMMITTEE ON THE JUDICIARY

Washington, DC.

The Subcommittee met, pursuant to call, at 10 a.m., in room 2141, Rayburn House Office Building, the Honorable F. James Sensenbrenner, Jr. (Chairman of the Subcommittee) presiding.

Present: Representatives Sensenbrenner, Goodlatte, Scott, Conyers, Chu, and Richmond.

Staff Present: Anthony Angeli, Majority Counsel; and Joe Graupensperger, Minority Counsel.

Mr. SENSENBRENNER. The Subcommittee will come to order. Without objection, the Chair will be authorized to declare recesses during votes today.

This hearing is the second in a series on the Electronic Communications Privacy Act, otherwise known as ECPA. Today, we will examine the issue of geolocation and its use by law enforcement in criminal investigations.

While this hearing was planned before the attack in Boston, those tragic events highlight the importance of the topic. The stakes are high. As in any ECPA reform, Congress needs to strike the right balance to protect privacy rights without undermining law enforcement.

The term "geolocation" is often used broadly and in a variety of contexts. Geolocation refers to the method of assessing the location of an electronic device—typically a cell phone, but sometimes a vehicle—with or without a tracker or a computer.

Geolocation is often related with the acquisition of cell tower information to determine the general location of a cell phone. Thus, frequently, geolocation is related to the use of global positioning systems, or GPS.

The results from its use often vary. Depending upon the type of cell phone being tracked or the provider on whose network it operates, the information about a phone's location can vary from a city block to specific latitude and longitude coordinates.

The primary objective of this hearing is to examine whether the electronic acquisition of a device's geographical location is covered by the Fourth Amendment and, if so, what level of legal process should be required before accessing such information. The hearing will also examine how law enforcement makes use of this information and its importance in their response to criminal and national security threats.

ECPA has not kept pace with the assortment of new communication devices and other technologies that are now widely available in today's marketplace. This is particularly true with geolocation technology. As GPS technology has become cheaper, more widely available, and used more frequently in our daily lives, the legal authorities and restrictions that are or should be in place to govern when and where such information is accessed and used have become less clear.

No one doubts that geolocation information is useful, especially to law enforcement officers and agents. The larger question is how do we balance the needs of law enforcement with the expectations of privacy of those they are charged with protecting?

In *U.S. v. Jones*, the Supreme Court proposed that new intrusions on privacy may spur the enactment of legislation to protect against these intrusions, as had occurred in the case of wiretapping many years ago. The court asserted that Congress should enact a comprehensive statute regulating the use of GPS tracking technology for law enforcement purposes.

Since all geolocation capabilities are not created equal, our task in enacting comprehensive legislation is more complex. Unfortunately, *Jones* was limited to the installation of a GPS tracker on a suspect's vehicle and gives us limited guidance.

I am dismayed to point out that the Department of Justice declined to testify at today's hearing. I was tempted to have an empty chair for their witness, should they change their mind at the last minute. There is not an empty chair at the witness table, but the chair notes that there are plenty of empty chairs in the room, should they decide to appear.

As the Nation's most frequent user of ECPA for geolocation purposes, the department is in a unique position to educate the Members of this Subcommittee on the status of Federal law and the department's current practices when seeking court orders for geolocation information. While DOJ has briefed Committee staff on ECPA and geolocation, the Obama administration has refused our request to testify in public because it lacks a clear policy position on how best to reform ECPA.

This is unacceptable, and I don't want to spend a lot of time working on something that is workable when, all of a sudden, out of the blue there will be a statement of Administration policy that will threaten a veto over hours of work and input from everybody except the Department of Justice. We must, unfortunately, move forward in their absence.

I welcome our witnesses who are with us today and look forward to their testimony and now recognize the gentleman from Virginia, Mr. Scott, the Ranking Member.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. Chairman, today we meet to discuss issues related to geolocation, privacy, and surveillance and the need to clarify the standards of Government access to certain types of personal location information.

Technology affords us greater conveniences, but advances in technology present new challenges to our privacy rights. Much more information is generated about us, and we are presented with questions about how it is stored and by whom it may be accessed.

The Supreme Court 1967 decision *Katz v. United States* continues to direct our privacy jurisprudence. In that case, a man's calls from a public pay phone booth were recorded by a device attached to the outside of the booth by the FBI. The court ruled that this eavesdropping was a search under the Fourth Amendment because it violated a man's "reasonable expectation of privacy."

Now that standard should continue to guide us today. When we go somewhere in public, we know that we may be seen by others, and even if we do not want others to know where we are, the visual recognition by others is a risk we take. What we do not expect is that our carrying of a personal communication device, such as a cell phone, will be used by Government to track and record our every move.

This is particularly the case as cell site location information has become, in many cases, as accurate as GPS because of the growing number of cell sites and the use of microcells that cover extremely small areas. We have laws that make a combination between privacy rights and sometimes urgent need of law enforcement to investigate crimes, and that is why Congress drafted Federal statutes to restrict Government access to the content of electronic communications but provides a less stringent standard for accessing noncontent records reflecting just that a communication took place, but not the content of the communication.

The Electronic Communications Privacy Act, which was enacted in 1986, was forward looking in some ways but did not contemplate every possible technological advance. Because the statute did not foresee the current state of location technology, the law does not provide clear guidance as to what steps the Government must take in order to obtain location data from devices like cell phones and navigation systems in cars.

While we should have exceptions for emergency situations and situations where the need to locate a missing person—where there may be a need to locate a missing person, we need legislation to address the lack of clarity in the law by generally requiring the Government to show something, possibly probable cause, to get a warrant in order to obtain historical and prospective data location about our citizens.

Given our expectation of privacy, this should be the starting point for our discussion of the issue today.

I yield back the balance of my time.

Mr. SENSENBRENNER. I thank the Ranking Member.

The Chair now recognizes the most recent Chairman emeritus of the Committee, the gentleman from Michigan, Mr. Conyers, for his opening remarks.

Mr. CONYERS. Thank you, Chairman Sensenbrenner and Ranking Member Scott.

I will put my statement in the record and indicate my support and co-sponsorship of H.R. 1312 and warmly welcome the witnesses that are joining us here today.

This question of cell phones and tracking locations are right smack up against the privacy considerations, and this discussion and this legislation will be very important in that direction.

And so, I am happy to join all of you at this hearing, and I return the balance of my time.

[The prepared statement of Mr. Conyers follows:]

Prepared Statement of the Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary

Today we consider a critical issue of personal privacy: whether the government should have to show probable cause and get a warrant in order to obtain from wireless devices information about where someone has been or is going. **This is particularly important because the ACLU has reported the widespread use of cell phone tracking by law enforcement agencies and revealed that the legal standards used to engage in tracking vary widely.**

I want to make several points about this issue and what we must do.

First, government tracking of everywhere we go is contrary to our reasonable expectation of privacy. Today, almost all of us carry cell phones or other electronic devices, but we do so in order to communicate with each other, not to be tracked by the government. Geolocation tracking, whether information about where we have been or where we are going, strikes at the heart of personal privacy interests.

The pattern of our movements reveals much about ourselves. When individuals are tracked in this way, the government is able to generate a profile of a person's public movements that includes details about a person's familial, political, professional, religious, and other intimate associations.

Next, we must recognize that the Supreme Court's decision last year in *U.S. v Jones* reinforces the fact that the question of location privacy in the hands of Congress. In *Jones,* the court ruled that placing a GPS tracking device on a car constitutes a search under the Fourth Amendment.

While the Court was not presented with the question of whether a warrant should be required or under what standard a court order should be issued, the case highlights the need for us to address the full range of location tracking issues.

In his concurring opinion, Justice Alito noted that the availability of location tracking devices, including cell phones, raises important questions about our expectations of privacy. He noted that Congress has not adequately addressed these issues and that "in circumstances involving dramatic technological change, the best solution to privacy concerns may well be legislative."

Finally, I propose that we enact legislation to address uncertainty in the law and provide the appropriate standard. Current law does not adequately address this issue and we need to enact H.R. 1312, the "Geolocation Privacy and Surveillance Act."

I am a cosponsor this bill, introduced by Congressman Jason Chaffetz to require the government to obtain a warrant based on probable cause to compel cell phone companies to disclose the location information of their customers.

As the New York Times reported, "lawyers and law enforcement officials agree[] that there [is] uncertainty over what information the police are entitled to get legally from cell phone companies, what standards of evidence they must meet, and when courts must get involved."

Protecting the privacy of this information is up to Congress, and given the reasonable expectations of privacy we have about our location information, the appropriate standard is probable cause. That is why I support enactment of H.R. 1312.

Thank you.

Mr. SENSENBRENNER. I thank the distinguished Chairman emeritus.

By tradition, we swear witnesses in at the beginning of each hearing. So will the witnesses please rise, raise your right hand?

[Witnesses sworn.]

Mr. SENSENBRENNER. Let the record show that each of the witnesses answered in the affirmative, and the Chair will now introduce the witnesses.

Mr. Mark Eckenwiler is senior counsel of the firm Perkins Coie. His focus is in electronic privacy law, civil and criminal liability for online conduct, computer intrusions, and service provider interactions with law enforcement. Mr. Eckenwiler previously served with the Department of Justice as a primary authority on Federal electronic surveillance law, including the Wiretap Act, the pen register/trap and trace statute, the Electronic Communications Privacy Act of 1986, and CALEA.

Most recently, he was the Associate Director for Technology with the Office of Enforcement Operations in the Justice Department's Criminal Division, where he oversaw all Federal applications for Internet communications surveillance orders.

He received his bachelor's of arts degree from Harvard, his master of arts from Boston University, and his law degree from NYU School of Law.

Mr. Peter Modaferri has been a detective with the Rockland County District Attorney's Office for over 40 years and the last 25 years as chief of detectives. Since 1990, Mr. Modaferri has chaired the Investigative Operations Committee for the International Association of Chiefs of Police. He is a member of the Criminal Intelligence Coordinating Council and served as a regional expert for the Office of National Drug Control Policy Technology Transfer Program and consulted with the Foreign Terrorism Tracking Task Force, which was established in 2001.

Mr. Modaferri is a graduate of the FBI National Academy, holds a B.A. from Siena College, and a master of arts in criminal justice, and has concluded the coursework in the doctoral program at the City University of New York. In 1992, he was awarded a Fulbright Fellowship for graduate study in the United Kingdom.

Ms. Catherine Crump currently serves as a staff attorney for the American Civil Liberties Union Speech, Privacy, and Technology Project. She is currently litigating constitutional challenges to cell phone tracking by law enforcement and is seeking information related to the Justice Department interpretation of how *United States v. Jones* applies to its location tracking activity.

If you find that out, please let us know because, apparently, they don't want to tell us directly.

She has directed nationwide requests for public records regarding law enforcement's use of cell phone information and license plate readers. She received her bachelor of arts from Stanford University and her law degree from Stanford Law School.

Mr. Matthew Blaze is Associate Professor of Computer and Information Science at the University of Pennsylvania. Mr. Blaze's research focuses on cryptography, mass applications, trust management, human scale security, secure systems design, networking, and distributed computing. His focus is in security technology with bearing on public policy issues, including cryptology policy, wiretapping, and surveillance.

He received his bachelor of science degree from City University of New York, Hunter College; his master of science degree from Columbia; and his master's of art and Ph.D. from Princeton.

Each of the witnesses' written statements will be entered into the record in its entirety, and I ask that each summarize his or her testimony in 5 minutes. We have the lights there. The yellow light means you should speed up, and the red light means you should stop.

Mr. Eckenwiler?

TESTIMONY OF MARK ECKENWILER, SENIOR COUNSEL, PERKINS COIE LLP

Mr. ECKENWILER. Chairman Sensenbrenner, Ranking Member Scott, Mr. Chairman Emeritus, and distinguished Members of the Subcommittee, thank you for your invitation to testify this morning on the important topic of cell phone location privacy.

My name is Mark Eckenwiler, and I should state at the outset that my comments today reflect only my personal views. I will, of course, be drawing on my 16 years of experience working on a daily basis with the Electronic Communications Privacy Act, or ECPA. I am not speaking today on behalf of the Justice Department or my current employer or any individual client.

My testimony today focuses on both the types of location data that law enforcement seeks from wireless providers and the legal rules that restrict such disclosures. I have three main points.

First, not all location data is the same. It can be generated in a variety of ways, and one type of location data, cell site location information, is less precise than others. Second, in general, existing law provides a carefully calibrated set of meaningful protections for wireless user location data. The sky is not falling. And third, the current framework does, however, have some gaps and inconsistencies that I think would benefit from careful study by this Committee.

Now I mentioned that there are different types of location data. Cell site information is generated in the ordinary course of business whenever a user sends or receives a phone call or a text message. It does not provide pinpoint location information for a phone. Rather, these records indicate which cell tower handled a particular communication.

Because tower spacing varies widely across a range of locations from rural to suburban to urban settings, so does the area covered by each tower. And as a result, cell site location information may place a phone on a given city block, or it may only indicate a very large area of several square miles in which a phone was apparently located at the time of a communication.

Contrast this with precise location information. This separate class of data, which includes but is not limited to GPS, is different not only in its level of precision and, thus, its privacy invasiveness, but also how it is obtained. One significant difference is that precise location information may be generated even when the phone is not in active use, sending or receiving a communication.

Existing law treats these two types of information, cell site and precise location information, very differently. Under ECPA, law enforcement can obtain stored cell site records—that is, for some pe-

riod in the past—only by applying to a court for a so-called 2703(d) order.

Now the standard for issuance of this, specific and articulable facts, is an important safeguard, and indeed, the executive director of the Electronic Frontier Foundation testified before a joint House/Senate committee this standard affords "a high degree of protection."

The rules governing prospective collection of cell site information—that is, real-time collection—are a subject of profound disagreement among the Federal courts. Some of them apply this same 2703(d) standard in granting so-called "hybrid orders." Others see a gap in the statute and have required a warrant because there's no other available mechanism.

Because precise location information, by contrast, is not collected by wireless carriers in the ordinary course, it is not typically available as a stored record for past periods. For ongoing surveillance, ECPA provides no clear statutory mechanism, and as a result, the practice at the Federal level has been to seek a search warrant under Criminal Rule 41, based upon a showing of probable cause.

Finally, as set out in more detail in my written statement, the current legal framework is not perfect. There are a number of issues that merit this Committee's attention, and I would be pleased to discuss those in greater detail during the Q&A.

In summary, Mr. Chairman, existing law, especially ECPA, recognizes the important privacy interests at stake by putting meaningful legal barriers between law enforcement and users' location data. In doing so, current law takes the approach of careful calibration of legal standards rather than one size fits all.

Thank you for the opportunity to appear this morning. I look forward to your questions.

[The prepared statement of Mr. Eckenwiler follows:]

Before the

Committee on the Judiciary

Subcommittee on Crime, Terrorism,
Homeland Security, and Investigations

United States House of Representatives

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

Geolocation Privacy and Surveillance

April 25, 2013

Statement of

Mark Eckenwiler
Senior Counsel
Perkins Coie LLP

I. INTRODUCTION

Chairman Sensenbrenner, Ranking Member Scott, and distinguished members of the Subcommittee, thank you for convening this hearing. It is an honor to appear before you today to discuss the important legal and technical issues raised by law enforcement access to wireless user location data.

Let me say at the outset that these comments reflect my personal views. I am not speaking for or on behalf of any client or group of clients, nor for my former colleagues at the Department of Justice. Instead, I offer my personal observations, drawn from over 16 years of working with the Electronic Communications Privacy Act (ECPA) while with the Justice Department and, more recently, in the course of representing service providers in private practice.

II. TYPES OF LOCATION DATA AVAILABLE FROM WIRELESS CARRIERS

To understand the issues surrounding law enforcement access to carrier-held location data, it is essential to start with the technology, not the law. Law enforcement typically seeks two distinct types of location data from wireless carriers: cell-site location information and precision location data.

A. Cell-Site Location Information (CSLI). As you know, cellular providers rely upon a network of antennas to provide service across large coverage areas. Whenever a user places or receives a voice call (or sends or receives a text message), the radio portion of that communication is transmitted between the customer's handset and a nearby tower. If the user moves in the course of a voice call—such as when traveling on the highway—the call may be seamlessly "handed off" to one or more other towers in sequence as the handset moves through different coverage areas.

Spacing between towers is determined primarily by the amount of network activity (and thus by the number of users) in a given area. In sparsely populated regions, cell towers are widely spaced, with each typically serving a coverage area several miles in radius. In suburban areas with moderate population density, carriers place towers closer together, with each having a service radius of a mile or less. Antennas in center cities are clustered even more tightly, with cell towers in the most densely populated areas (such as midtown Manhattan) spaced every 200 meters or less.

In suburban and urban areas, the coverage area for a given cell tower is typically subdivided into multiple sectors (or tower "faces"). In these cases, there are typically three 120-degree sectors, each with its own antenna. (To visualize this configuration, imagine a clock face divided into thirds from 10 to 2, 2 to 6, and 6 to 10. Each "pie slice" represents the coverage area for a given antenna.) Towers in sparsely populated areas, by contrast, normally have a single omnidirectional antenna.

Whenever a user places or receives a voice call (or sends or receives a text message), the network handling that communication—which may be the customer's home network, or another network with which the customer's carrier has a roaming agreement—creates a record of the first cell tower that handles the call or text message. If the tower coverage area is divided into multiple sectors, the stored cell-site location information (CSLI) record also indicates which

particular antenna handled the communication. Most, but not all, carriers also record the last tower (and, where applicable, sector) handling a voice call. Because text messages are short, and thus are transmitted almost instantaneously, they pass through only a single antenna.

The degree to which CSLI reveals the location of a user's phone varies for several reasons. First, these records do not provide grid coordinates for the phone itself; rather, they indicate which nearby antenna transmitted a communication associated with that handset. Because tower spacing varies enormously, the radius of corresponding tower coverage does as well, and therefore the projected area from where a call was placed will likewise vary.

In heavily populated urban areas, CSLI can—subject to the further limitations discussed below—place a handset in an area of approximately 1,000 square meters. In suburban areas with towers spaced further apart, CSLI may suggest an area of a square mile or more. Tower data from rural areas, by contrast, provides only very broad location data often covering dozens of square miles or more.

Other factors also contribute to the general imprecision of CSLI. For example, the boundaries between the sectors of an individual cell tower, as well as the boundaries between areas served by different towers, are neither precise nor fixed. Records showing communications activity alternating between two adjacent coverage areas may indicate handset movement back and forth between the areas, or may instead result from the activity of a non-moving user in an area of overlapping coverage.

More importantly, a particular communication is not always handled by the closest tower. Both natural terrain features (*e.g.*, hills and valleys) and man-made structures interfere with line-of-sight radio transmission. Weather conditions, including precipitation or even humidity level, also may affect signal propagation.

At times, the carrier antenna closest to the user's handset may even be entirely unavailable. This can result from local, temporary equipment or network outages, or simply from network congestion. For example, when highway traffic backs up at a toll plaza or accident scene, the nearest tower's capacity may be saturated by unusually high activity levels. In these circumstances, the next user trying to make a call may only be able connect to a more distant, less burdened tower; the resulting CSLI record will indicate usage of the latter, creating the misleading impression that the handset was closer to that tower than to any other.

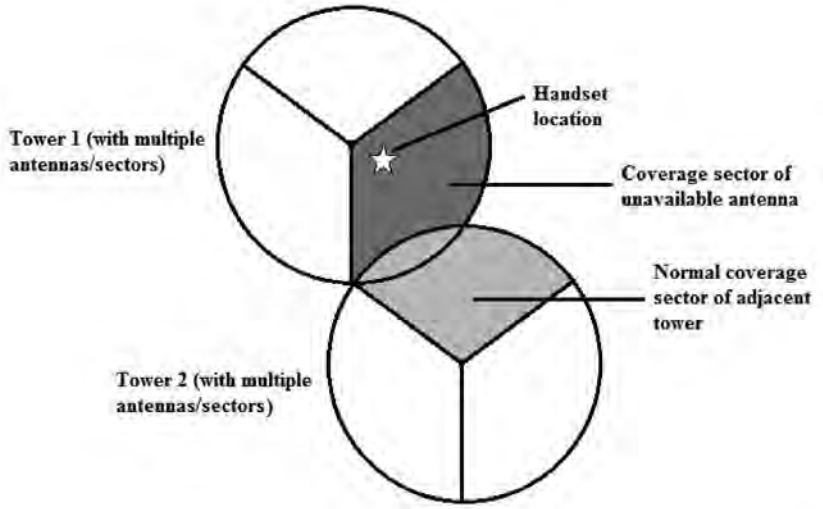


Figure 1

In Figure 1 above, the star represents a hypothetical handset location; the dark area represents the normal, but temporarily unavailable, coverage area for the closest antenna on Tower 1; and the light gray area depicts the normal coverage area for an adjacent tower's sector. Activity handled by Tower 2 would create a record associating the handset with the light gray area, even though the phone was outside that sector and closer to Tower 1.

Some commentators assert that the increasing use of "microcells" with smaller coverage areas renders CSLI functionally equivalent to GPS or other more precise location technologies. These claims are misleading. User-owned microcells – such as those purchased and installed by home customers – do not expand the network of towers available to the general population. Rather, these microcells are usable only by their owners, and therefore cannot provide service to, let alone identify the location of, the millions of other cell phone users.

B. Laws Restricting Disclosure of CSLI to Government Agencies: The Electronic Communications Privacy Act (ECPA) is the main federal statute regulating communications privacy. ECPA draws numerous distinctions between

- real-time (prospective) collection and access to historical records;
- communications content and non-content records; and
- transactional non-content records and more limited subscriber records.

Depending on the type of information sought and the manner in which it is to be collected, ECPA requires varying forms of compulsory process. These range from subpoenas—issued by a

prosecutor (or, in some cases, an investigative agency) on the comparatively low standard of relevance—up through various types of increasingly demanding court orders—with wiretap orders (based on probable cause and other special requirements) at the other end of the spectrum.

1. Access to Stored CSLI

As originally enacted in 1986, ECPA allowed the government to obtain any stored non-content record about a communications provider's customer using a grand jury, trial, or administrative subpoena. As part of the 1994 Communications Assistance for Law Enforcement Act (CALEA), however, Congress amended ECPA to divide non-content records into two categories.

The first of these categories, often referred to informally as "basic subscriber information," remains available in response to a subpoena.[1] These records—explicitly enumerated in an exhaustive list of six categories—include the customer's name, address, account identifier, length of service, and method of payment. Except for "local and long distance telephone connection records, or records of session times and durations," however, this category does not include records about specific user activity.

Instead, when law enforcement seeks to compel a service provider to disclose other stored non-content records, it must apply for a unique type of court order that was created in the 1994 amendment to ECPA.[2] To obtain this so-called "2703(d) order" (named for the section of the statute where it resides), the government must

> offer[] specific and articulable facts showing that there are reasonable grounds to believe that … the records or other information sought, are relevant and material to an ongoing criminal investigation.

As explained in the report from this Committee, "[t]he intent of raising the standard for access to transactional data is to guard against 'fishing expeditions' by law enforcement."[3] Advocating strongly in favor of this raised standard during an August 11, 1994 joint House-Senate committee hearing on the legislation,[4] the Executive Director of the Electronic Frontier Foundation described the proposal as follows:

> Chief among these new protections is an enhanced protection for transactional records from indiscriminate law enforcement access.

---

[1] *See* 18 U.S.C. § 2703(c)(2).

[2] *See* § 2703(d).

[3] H. Rep. No. 827, 103d Cong., 2d Sess., at 31 (Oct. 4, 1994).

[4] *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services, 1994: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary*, 103d Cong., 2d Sess. 160-61 (1994) (prepared statement of Jerry J. Berman, Executive Director, Electronic Frontier Foundation).

> ... Provisions in the bill recognize that this transactional information created by new digital communications systems is extremely sensitive and deserves a high degree of protection from casual law enforcement access which is currently possible without any independent judicial supervision. ...
>
> In order to gain access to transactional records ... law enforcement will have to prove to a court, by the showing of "specific and articulable facts" that the records requested are relevant to an ongoing criminal investigation. This means that the government may not request volumes of transactional records merely to see what it can find through traffic analysis. Rather, law enforcement will have to prove to a court that it has reason to believe that it will find specific information relevant to an ongoing criminal investigation in the records it requested. ...
>
> Court order protection will make it much more difficult for law enforcement to go on "fishing expeditions" through online transactional records, hoping to find evidence of a crime by accident. ...
>
> The most important change that these new provisions offer is that law enforcement will: (a) have to convince a judge that there is reason to look at a particular set of records, and; (b) have to expend the time and energy necessary to have a United States Attorney or District Attorney actually present a case before a court.

An overwhelming majority of courts, including the federal Third Circuit Court of Appeals, has found that historical "CSLI from cell phone calls is obtainable under a § 2703(d) order."[5] Although a handful of lower courts have held that section 2703(d) does not apply to stored CSLI, this view has failed to win broader acceptance.[6] Many of these same lower court judges have also argued that historical CSLI is protected by the Fourth Amendment, and that a warrant is therefore necessary to compel such third-party records. Here, too, this represents a minority position; so far as I am aware, no federal court has ever granted a motion to suppress CSLI on these or any other grounds, despite attempts by numerous criminal defendants.[7]

---

[5] *In re Application*, 620 F.3d 304, 313 (3d Cir. 2010).

[6] Courts adopting this minority view point to the exclusion of "any communication from a tracking device (as defined in section 3117 of this title)" from ECPA's definition, at 18 U.S.C. § 2510(12)(C), of "electronic communication." (As noted by the Third Circuit, this view fails to distinguish between a communication itself – such as a phone call – and data *about* the communication, such as CSLI.) The minority view has the perverse consequence of excluding CSLI entirely from ECPA's protections, meaning that the government could compel CSLI using lesser compulsory process such as a subpoena.

[7] *See, e.g., United States v. Graham*, 846 F. Supp. 2d 384 (D. Md. 2012) (finding no Fourth Amendment interest); *see also United States v. Jones*, 2012 WL 6443136 at *5 & n.9 (D.D.C. Dec. 14, 2012) (collecting cases).

2. Prospective Collection of CSLI

CSLI acquired in real time is qualitatively the same (and thus its value is subject to the same practical limitations) as historical CSLI. The rules governing real-time government acquisition of CSLI from wireless carriers are, however, much less clear.

The pen register statute permits the government to obtain a court order authorizing ongoing collection of non-content "dialing, routing, addressing, or signaling information,"[8] information that would normally include CSLI. However, CALEA states that

> with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127), such call-identifying information [delivered by a carrier to the government] shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number) ....[9]

This restriction creates a gap in the statutory framework: although it declares which type of process may not be used (*i.e.*, a bare pen register order), it does not prescribe the types of court orders that may be used. (Moreover, the other major federal statute governing real-time surveillance—the far more demanding Wiretap Act—does not apply because it regulates only the collection of communications contents.[10])

In an effort to fill this gap, prosecutors began to apply for court orders under the combined authority of the pen register statute and section 2703(d) (which, as discussed above, requires a higher showing) on the grounds that such orders are not "solely pursuant" to pen register authority. Beginning in 2005, however, lower court judges started to reject these so-called "hybrid" orders. While some of these courts based their objections on obvious misunderstandings of the technology and kinds of data involved,[11] others reasoned that section 2703(d)—located in the Stored Communications Act,[12] and lacking provisions that address duration and other aspects of real-time surveillance—could not be used to collect information prospectively. These courts concluded that the government needs to use a search warrant, not

---

[8] 18 U.S.C. § 3127(3).

[9] 47 U.S.C. § 1002(a)(2).

[10] *See* 18 U.S.C. §§ 2510(4) (defining "intercept" to mean "the aural or other acquisition of the contents" of a protected communication) & 2510(8) (defining "contents" to mean "any information concerning the substance, purport, or meaning of [a] communication").

[11] The most obvious example of this phenomenon is *In re Application*, 402 F. Supp. 2d 597 (D. Md. 2005), in which the court confuses CSLI with GPS data. *See id.* at 599.

[12] Chapter 121 of Title 18 is entitled "Stored Wire and Electronic Communications and Transactional Records Access."

because the Fourth Amendment requires it, but rather because a search warrant is the only available mechanism.[13]

Courts remain sharply divided on this question, with practices varying from district to district (and, in some cases, from one judge to another within a single federal district). Even courts endorsing the hybrid theory have called upon Congress to resolve the issue.[14]

C. Precision Location Information (PLI). Beginning in 1997, the FCC adopted regulations requiring cellular carriers to be able to locate wireless 911 callers. Phase I of this rulemaking—known as Enhanced 911 or simply E-911—required carriers to be able to deliver a 911 caller's cell-site and sector information (*i.e.*, CSLI) to the "public safety answering point" (*i.e.*, the 911 call center). Because of the inherent limits on the precision of CSLI, E-911 Phase II (in effect today) requires carriers to be able to deliver more precise location information.

In imposing these obligations, the FCC permitted carriers to choose either of two different methodologies for complying:

1. **Handset-based location technology** relying on special hardware or software in the mobile phone itself. U.S. carriers opting for such a "handset solution" have chosen to use Global Positioning System (GPS) technology, in which the phone calculates its position based on signals received from overhead GPS satellites.

2. **Network-based location technology** in which the work of calculating a phone's position occurs not on the handset, but rather in the carrier's network. This "network solution" typically involves measuring the time required for a test signal to travel between the handset and detection devices on cell towers in the vicinity. Using the known locations of those towers and the different timing information, software in the carrier's network is able to calculate a position for the phone. (This process, technically known as "multilateration," is often referred to informally as "triangulation.")

Generally speaking, the regulations require such E-911 Phase II location information to be accurate to within 50-300 meters.[15]

Contrary to popular belief, carriers do not collect these types of precise location information (PLI) on consumer-level users in the ordinary course of business.[16] As a result, historical PLI from these technologies is not available to law enforcement.

---

[13] Typical of this line of cases is *In re Application*, 497 F. Supp. 2d 301 (D.P.R. 2007).

[14] *See In re Application*, 632 F. Supp. 2d 202, 211 (E.D.N.Y. 2008) ("District courts across the country are divided on an issue that requires balancing the Government's investigatory needs with citizens' right to privacy. Absent clarity from Congress, this division and inconsistency in outcomes will continue because the issue is one about which reasonable judges can, and obviously do, disagree."); *In re Application*, 460 F. Supp. 2d 448, 450 (S.D.N.Y. 2006).

[15] The applicable regulation (47 C.F.R. § 20.18(h)) lays out a complex set of criteria, including several deadlines for compliance across increased geographic areas. In general, handset-solution phone location data must be more precise than network-solution data.

However, law enforcement may nevertheless seek PLI on a prospective basis. Because ECPA itself provides no clear mechanism for compelling this type of information, it is common for prosecutors to obtain a search warrant under Federal Rule 41 or a state equivalent. In doing so, some prosecutors rely on the explicit "tracking device" provisions of Rule 41, while others rely upon the Rule's well-established history of use as a general means of conducting ongoing evidence collection.[17] These may appear either in the form of stand-alone warrants, or as supplemental authority incorporated into a wiretap order.[18]

III. ISSUES DESERVING CONGRESSIONAL ATTENTION

As suggested above, there are several areas in which the current legal framework is not entirely satisfactory. These include the following:

1. Hybrid orders. Easily the source of greatest controversy, the government's use of hybrid orders—*i.e.*, court orders combining the authority of the pen register statute and the "specific and articulable facts" test of section 2703(d) —has led to a sharp divide among lower federal courts. Greater clarity in this area would be an enormous benefit to the service provider community; providers have a substantial interest in knowing with certainty the boundaries of what is lawful, in protecting their customers' privacy, and in avoiding potential civil liability.

2. "Tower dumps". Instead of seeking historical CSLI for the identified phone of a specific target, prosecutors sometimes use a section 2703(d) order to seek all records associated with calls handled by a given tower for a specified interval of time (usually corresponding to the date and time of an unsolved crime). These so-called "tower dumps" can be essential to identifying suspects in certain kinds of crimes such as bank robberies,[19] but almost invariably involve disclosure of large numbers of user records. The volume of information varies enormously according to time of day, the size of the

---

[16] Many carriers do, however, offer so-called "fleet management" services to business customers at additional cost. In some cases, these services—intended for locating a company's delivery drivers, construction site supervisors, and the like—permit not only real-time monitoring but also review of historical PLI.

[17] Prior to the 2006 addition of tracking device provisions, prosecutors used Rule 41 to obtain warrants when needed to authorize the use of such devices. This practice flowed directly from the Supreme Court's directive in *United States v. Karo*, 468 U.S. 705, 718 (1984), to seek a warrant for certain tracking device uses. Prior to the 1986 enactment of the pen register statute, the Supreme Court likewise read Rule 41 as "sufficiently flexible" for use in authorizing prospective surveillance of dialed telephone numbers. *United States v. New York Telephone Co.*, 434 U.S. 159, 169 (1977). And the federal circuits are unanimous in relying on Rule 41 as authority for issuance of surreptitious video surveillance warrants, even though the Rule contains no explicit provisions contemplating this use. *See, e.g., United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992) (*en banc*); *United States v. Cuevas-Sanchez*, 821 F.2d 248, 252 (5th Cir. 1987).

[18] *See, e.g., United States v. Ortega-Estrada*, 2008 WL 4716949 at *14 (N.D. Ga. Oct. 22, 2008).

[19] *See, e.g.,* Criminal Complaint, *United States v. Capito* (D. Ariz. Mar. 12, 2010) (describing, at pp. 12-15, the use of tower dump data to identify the phones used by suspects at four separate armed bank robberies), available at http://tinyurl.com/towerdump.

requested time frame, and the type of area (rural, suburban, or urban) at issue, but can reveal thousands or even tens of thousands of records.[20]

Given the potential for disclosure of such customer information, the Committee may wish to consider the desirability of additional statutory protections such as limits on the number of records or the length of the time window requested, or protocols for sealing or destroying voluminous non-pertinent records.

3. Warrants or orders to surveil unidentified phones contacting a target phone. Prosecutors at the state level sometimes apply for warrants or court orders that authorize monitoring the location not only of a named target phone (as to which they must establish probable cause), but also of any other phone that contacts (or is contacted by) the target phone during the authorized period of surveillance. This is a troubling practice: it allows for location monitoring of an undetermined number of phones not identified in the warrant, and on the questionable assumption that even a single contact with the target phone constitutes evidence of criminal activity.

   In light of the potential for significant, unjustified privacy invasions—for example, from misdialed numbers or calls from family members or others uninvolved in criminal activity—the Committee should carefully consider whether additional safeguards are required to limit or prohibit these types of orders.

4. Legal framework for real-time PLI monitoring. More generally, the Committee may wish to examine the adequacy of the current, somewhat ad hoc use of Rule 41 to authorize real-time law enforcement access to PLI. Specific areas for potential review include the following:

   a. *Whether the "tracking device" provisions are adequate for use in this area.* Rule 41 requires that a "tracking device" warrant be issued in the district where the device is "install[ed]."[21] Although this poses no problems in the case of the physical tracking devices clearly contemplated by the Rule's drafters, it is a potentially serious obstacle in situations where (1) the court believes the tracking device provisions strictly apply to cell phone location and (2) the applicant cannot attest that the phone is within the district at the time of application. Indeed, since the objective of such applications is to learn the location of the target phone through court-authorized electronic surveillance, this requirement generally creates a Catch-22.

   b. *Burden on service providers, and compensation therefor.* Rule 41 does not impose any explicit limit on how often law enforcement may request PLI in the course of executing a prospective warrant. In many instances, manual intervention by carrier personnel is necessary, often on nights and weekends, making frequent

[20] According to the *Capito* complaint, "[i]nvestigators used the four most rural [bank robbery] locations in order to minimize the amount of extraneous telephone data that would likely be obtained ...." *Id.* at 13.

[21] Fed. R. Crim. P. 41(b)(4).

requests extremely burdensome. Moreover, Rule 41 contains no provisions for compensating carriers for their often substantial compliance costs.

c. *Emergency requests*. Both the Wiretap Act and the pen register statute include express language allowing law enforcement to conduct surveillance in emergencies without first obtaining court authorization.[22] Each of these statutes requires the government to apply to a court for retroactive authorization within 48 hours. By contrast, Rule 41 contains no such emergency compulsion provision.

IV. CONCLUSION

ECPA and its companion statutes currently provide significant privacy protection for wireless customers' location data. However, at least one gap in the statute has provoked widespread disagreement among federal judges, and other practical and procedural difficulties have emerged over time. Because these problem areas have a direct impact on user privacy, on service providers' compliance practices, and on our Nation's law enforcement efforts, the Committee deserves great credit for recognizing the need to re-examine the existing legal authorities and consider potential solutions.

Thank you for this opportunity to testify. I look forward to your questions.

[22] *See* 18 U.S.C. §§ 2518(7) (wiretap emergency authority) & 3125 (pen register).

Mr. SENSENBRENNER. Thank you.
Mr. Modaferri? Could you please press the voice button?

TESTIMONY OF PETER A. MODAFERRI,
INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

Mr. MODAFERRI. Good morning, Chairman Sensenbrenner, Ranking Member Scott, and Members of the Subcommittee.

Thank you for this opportunity to discuss the role that geolocation information plays as evidence in criminal investigations and its importance in law enforcement's effort to seek justice and public safety in the 21st century.

It is from the vantage point of being a detective for 40 years and currently chief of detectives and longtime chairman of the IACP's Police Investigative Operations Committee that I have seen a great deal of—a great and growing value of geolocation information to criminal investigations. Two issues have arisen over the past 10 years, which have increased this value significantly—globalization and wrongful convictions.

When this information is obtained in early stages of investigation, it provides fundamental building blocks on which successful cases may rest. Requiring probable cause in the initial stage of investigation to obtain certain types of geolocation information would make it significantly more difficult to solve crimes.

Investigative issues of time, technology, and process must be addressed in a way that allows us to proceed from the initial stages of an investigation, where little is known and nothing can be assumed, to a point where investigators establish probable cause.

The classic questions presented in investigations—who, what, where, when, why, and how—can be answered with geolocation evidence. To learn facts and make valid assumptions, investigators use available geolocation evidence as a filter to help corroborate or refute statements and conclusions at any time during investigation, to confirm or dismiss alibi statements or claims of witnesses, and to act as—for stored times and places, it can be the only witness at a crime scene.

Geolocation information gives us more than the ability to solve crime. It can prevent wrongful arrest by revealing the suspect was not at the scene of the crime. Mistaken identifications are a leading cause of wrongful convictions.

It can provide us with accurate time and place evidence that can confirm or refute identifications, confessions, and inaccurate testimony. Justice and public safety in the 21st century is a new ballgame. Today's criminal investigators are more mobile than ever. That makes law enforcement access to geolocation information all the more important.

Law enforcement must take advantage of geolocation information and location-based information just as the private sector does. Smartphones, mobile devices, GPS, and preinstalled technology like OnStar are available with more location technology evolving at a rapid pace.

Technologies generate—also generate historical data and business records from which location information can be derived. E-ZPass, credit card, and debit transactions are examples.

If we do not have standards of access in place to ensure we can get location evidence early in a case, then law enforcement will miss out on the productivity impact of advancing technology. That affects our ability to do our jobs the best we possibly can.

An example that demonstrates this type of importance of geolocation information was a bank robbery case in the Rockland County area. In the area around Rockland County, there were seven bank robberies. We had no success in identifying the perpetrators of those crimes until a witness came forward. She was a victim of one of the crimes, and she was at a gas station and saw a person who she believed was one of the robbers. And she was able to take a photograph of that person's car, and it had dealer license plates on it.

Using a subpoena, the detectives were able to get a possible identity on the person who purchased that car. Police then focused on the—with the subpoena on the basis of subscriber information and phone numbers. That was followed by a so-ordered subpoena, which produced historical cell site locations. Then a trap and trace pen register surveillance with location authorization was established.

Utilizing probable cause, we then attached a GPS device. The result was an arrest of the suspects immediately after their next robbery, while they were holding the proceeds of the crime.

At the beginning of the case, standard identification procedures were of little value, and there were no suspects in the case. A witness opened a criminal investigation. To build the case, subpoenas for stored cell phone call detailed records with location information were issued once we had that lead.

The subpoenas produced suspects and locations that were essential to reach probable cause. Throughout the investigation, location information revealed and confirmed the activities of the true perpetrators. Not only did it help identify the right people, it resolved a misidentification and prevented a wrongful arrest.

To conclude, Mr. Chairman, geolocation information has become an essential building material in the construction of many criminal investigations. It could be the concrete that cements eyewitness identification, the criminal, and the crime scene together.

To gather and integrate this information in the initial stages of an investigation, we must have reasonable balance between the standards of access required to obtain location evidence and the need of the investigation to proceed. Just as important, law enforcement must be able to receive these facts in a rapid and complete response from the holder of the information record.

Requiring probable cause to get basic limited information about a person's historical location could make it significantly more difficult for us in law enforcement to solve crimes and seek justice.

Thank you.

[The prepared statement of Mr. Modaferri follows:]

Statement of Peter A. Modafferi

Before the
Committee on the Judiciary
Subcommittee on Crime, Terrorism, Homeland Security and Investigations
United States House of Representatives
2141 Rayburn House Office Building
Washington, D.C. 20515

HEARING ON THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA) PART 2: GEOLOCATION PRIVACY AND SURVEILLANCE

April 25, 2013

Peter A. Modafferi
Chief of Detectives
Rockland County, N.Y. District Attorneys Office
County Court House
1 South Main Street
New City, N.Y. 10956

Introduction

Good Morning Chairman Sensenbrenner, Ranking Member Scott, and distinguished members of the subcommittee. Thank you for this opportunity to speak to you this morning to discuss geolocation information, the role that information plays as evidence in criminal investigations, and its importance in law enforcement's effort to seek justice and public safety in the 21st century.

My name is Peter A. Modafferi and I am the Chief of Detectives of the Rockland County, New York District Attorney's Office. I also Chair the Police Investigative Operations Committee of the International Association of Chiefs of Police and I have worked on a number of boards, working groups and committees concerned with issues related to criminal investigations.

I have been a detective for 41 years. For many years I conducted investigations into all types of criminal activity and I now lead, direct and coordinate these investigations. Today I wish to share with you what I have learned about investigations both from my experiences in Rockland County and from the exposure to the field which I have gained through various committees and working groups.

It is from this vantage point that I have seen the great potential that lies in law enforcement's utilization of the innovations in geolocation information. Utilizing this information in the early stages of an investigation often provides fundamental building blocks on which cases may rest. Requiring probable cause in the initial stage of an investigation to gain access to geolocation information would make it significantly more difficult to solve crimes.

It is my observation that, today, there is a digital evidence aspect to nearly every crime scene. Increasingly, those scenes are filled with digital evidence and, inevitably, to fully benefit from that evidence we must gather geolocation information. Some of this valuable evidence that is crucial in generating leads and ruling out suspects is in jeopardy if we are held to a probable cause standard to access every aspect of geolocation data.

There are issues of time, technology and process that must be addressed in such a manner that will allow us to proceed with an investigation from its initial stages, where little is known and nothing can be assumed, to a point where we go in the direction of establishing probable cause. From this point, we will hopefully proceed to an arrest that will withstand the rigors of due process and the judicial system and lead with 100% accuracy to a conviction beyond a reasonable doubt.

My Perspective

Crime is and always will be one of the most serious issues confronted by civilization.

Today's communications systems, worldwide information services, massive participation in social media services and multi-national economic partnerships have dramatically impacted our society. It is to this "globalized" environment that law enforcement must adapt, culturally and technologically in order to address crime.

The Investigative Process

Why is geolocation information valuable to law enforcement?

In the initial stages of an investigation, law enforcement seeks to quickly develop leads and theories that incorporate answers to classic questions presented: Who, What, Where, When, Why and How. Geolocation evidence can inform the answer to each question. The unique value of geolocation information is found in its two components – an accurate location and an accurate time the location was determined.

When investigators start working a case, little may be known and nothing should be assumed. To know pertinent facts and make valid assumptions, investigators use available geolocation evidence as a filter. This process allows investigators to winnow out and prioritize leads from the unorganized mass of related and unrelated information that surrounds a crime and a crime scene.

This process is the beginning of the effort to assemble an offering of probable cause to believe that a certain person or persons committed the crime, and that particular evidence will be found in specific locations.

Through the lens of geolocation evidence, investigators press to correctly determine an answer to Who, When and Where - what witnesses, victims, knowledgeable persons and perpetrators – were in the vicinity of the crime at about the time it occurred.

How is geolocation evidence used in an investigation?

In addition to providing clarity by answering some or all of the initial questions presented, the time and place components of geolocation information can be of use to corroborate or refute statements and conclusions offered at any time during the investigation.

Geolocation information can be used to confirm or dismiss alibi statements that are offered to show that a subject was not present at the time and place the crime occurred, or to confirm or dismiss the claim of a witness or another knowledgeable person who was present at a certain time or place.

A location-enabled digital device can be a "witness" to a crime. In fact, in cases where a human witness does not exist or is not discovered, the stored contents of the device may

be the only initial "witness" available to investigators. In this case, the geolocation information components of time and place are of upmost importance.

Justice and Public Safety in the 21st Century

Evidence is the basic foundation for addressing crime and criminals. The investigative process is how we secure the evidence we need to protect society and attain justice and public safety in the 21st century. Today we are part of a digital world and in that world digital evidence abounds.

Geolocation evidence is essential to obtain in the early stages of investigations when probable cause has not been established. Requiring probable cause to get basic, limited information about a person's historical location would make it significantly more difficult to solve crimes and seek justice for victims.

We do not have the luxury of setting the pace at a crime scene or in conducting an investigation. If we are constrained by a process that slows our progress in pursuing justice by extending the timeline of an investigation, the digital evidence at a crime scene may well go unexplored, evidence not be seized and analyzed, and our investigation will not meet our needs or the expectations of victims or civilized society as a whole.

The court room and judicial process are the safety net for a free and just society. That wrongful convictions have occurred is tragic and everything must be done to avoid them in the future. The process starts at the crime scene or with knowledge that a crime may have been committed and proceeds ahead. In the end, the basic fact is that you cannot have a wrongful conviction without a wrongful arrest. A wrongful arrest is the result of an inadequate investigation.

We have found that wrongful arrests occur because what we thought was proof wasn't always concrete, and what we thought was science was not always definitive. Some of our investigations, based on flawed conclusions, were neither necessarily accurate nor conclusive.

Geolocation information offers tremendous factual data that can be used to remedy these failures. Geolocation information can confirm or refute identifications, confessions and inaccurate testimony.

Added to the issues raised through the examination of wrongful convictions is globalization. The "usual suspects" are not just from the "old neighborhood" anymore. Globalization has, in the words of Thomas Friedman "unleashed the energies of hundreds of millions of people"[1]. Unfortunately some of those people and their energies result in

[1] The World is Flat, Thomas Friedman, Farrar, Straus & Giroux, April 2005

crime. Criminal activity and the location of criminals is not restricted by the limits and boundaries of an earlier era. Many of those boundaries have evaporated. The only boundaries that now limit globalization are governmental, which for criminals are easy obstacles to overcome.

To learn from this and better ourselves we must take full advantage of all that is available in today's world. Processes, guidelines and standards must be developed that will allow law enforcement to gain from technological evolution and attain what Friedman refers to as "productivity impact." Utilizing all that can be found at a crime scene or directly from a device recovered through a crime scene will not simply result in an increase in arrests but also an increase in accuracy and effectiveness, which will lead to justice and public safety in the 21st century.

An investigation is a process. It starts with the basics of who, what, when and where which may lead to a suspect, facts, evidence and probable cause to believe a suspect committed the crime. Utilizing geolocation information will offer substantial facts which will assist in obtaining a conviction beyond a reasonable doubt.

Law enforcement in the 21st century must combine new technologies with new ways of doing business to maximize investigative potential, create productivity "breakthroughs" and bring criminals to justice. "Productivity impact" in law enforcement investigations can be achieved in part through effective use of geolocation information.

A recent investigation into a series of bank robberies in the tri state area around New York City offers a significant example of how geolocation information can help solve a case and avoid a possible wrongful conviction.

Two brothers, residents of New York City, had robbed seven banks in the suburbs outside of the city. Utilizing standard investigative methods, detectives developed a suspect. Bank employees however were not able to identify the individual because he wore a mask. As the investigation progressed, a teller from one of the banks that were robbed believed she had seen the defendant at a gas station and photographed the vehicle he was driving. However, none of the employees at the banks could identify the individual from the gas station as the robber.

Utilizing a range of legal process from a subpoena to a court order, detectives obtained basic geolocation information, which eventually led to development of probable cause and the placing of a GPS system on the vehicle. Once probable cause was established the suspect's location was monitored by tracking his cell phone.

The geolocation information obtained without a warrant at the beginning of the investigation when probable cause was not determined led to the arrest of two individuals immediately after a bank robbery. At the time of arrest they had the proceeds of the robbery in their possession.

As it turned out the original suspect was not the individual who entered the banks during the robberies. He was a cousin. If not for the teller seeing one of the brothers and photographing the vehicle he has just purchased (it had dealer license plates at that time) the actual robbers would not have been traced. Though similar in appearance, the man at the gas station was the person who entered the bank not the person the police were focusing on.

The right persons were arrested due to the effective use of geoloaction information at the early stages of the investigation when probable cause was not evident. Standard identification procedures were of no value.

Following The Digital Footprint

The essentials to ensure the effectiveness of law enforcement lie in establishing a basic foundation from which we can pursue investigations. Investigations don't start with probable cause; they *lead us* to probable cause. Through investigations we discover facts. From these facts we start to build our case, which will hopefully lead to building probable cause and a fact-filled evidentiary case that leads to guilt beyond a reasonable doubt.

What is a "digital footprint" and how can investigators benefit from it? The science and technology behind geolocation has opened a new world filled with data that can corroborate or refute human observations. Geolocation information is part of a person's "digital footprint."

Evidence garnered through geolocation information can be established through of all types of equipment and records. Phones, mobile devices, trackers, and preinstalled (OnStar) technology are available today with more specific technology evolving at a rapid pace. Also from this technology comes the historical data and business records from which location information can be derived – EZ Pass, Credit Card / Debit Transactions, etc.

To establish probable cause we need a reasonable, manageable balance between legal process and investigative responsiveness.

As an example, an anonymous tip was offered to the Rockland County Drug Task Force. The tip included the name of an individual and a phone number connected to that individual. The caller stated that this person was operating a clandestine laboratory manufacturing illegal drugs.

The person offering the information stated that the principals involved in this criminal conspiracy had met recently at the location of the laboratory. The caller also stated an approximate date and time of that meeting. As is often the case, the initial information available to the investigators could not be confirmed and the person offering the information wished to remain anonymous.

The first step in the investigation was to subpoena basic subscriber information and limited call detail records. These subpoenas were issued in an effort to further identify the user of the given phone number and to display incoming and outgoing calls to and from associate numbers. This was done in an attempt to propose that certain associate phone numbers pointed to other members of the group and to discern a communications pattern between the conspirators. Any other associate numbers were ignored.

The boundaries of the information sought were confined to the proposed date/time window suggested by the caller.

Once a group of apparently related associate phone calls was established at the date and time proposed, historical geolocation information associated with the interacting phone numbers was obtained. This stored historical geolocation information is created and retained by the service provider during the operation of the cellular phone system. The boundary of this information was limited to the narrowed date/time in hopes that it might suggest a possible location of the meeting and the laboratory.

The use of this geolocation information led to the possible location of the lab and this information combined with standard police surveillance procedures led to a search warrant for the lab based on probable cause. We would not have been able to establish probable cause without the geolocation information provided in response to the initial subpoenas.

The technologies and records that can lead to geolocation of a criminal or exoneration of an innocent party varies between situations where geolocation is already "turned on" and recorded, and geolocation that results form a real time effort to obtain geolocation information. We can subpoena previously obtained records data or, following proper legal process, we can "turn on" appropriate technology.

Conclusion

Very little, if any, construction begins with out a foundation. Geolocation information is an essential building block in "the construction" of a criminal investigation. Often it will prove to be the concrete that cements eyewitness identification and the crime scene together. Geolocation puts us in an area where evidence and possibly a criminal or fugitive can be found.

To gather up and cement these building blocks together in the initial stages of an investigation we must determine a reasonable, manageable balance between legal process and investigative responsiveness. (Note, an emergency situation initiates a different, more expeditious process). In a criminal investigation, or a public safety/security event, access to geolocational information and records is an essential requirement to the determination of true facts. Likewise, it is essential to receive these facts in a rapid and complete response from the holder of that information or record.

I have not attempted to address the science and techniques used to derive geolocation information because I am not a technologist. What I have addressed in my testimony are the needs, the logistics and the processes that relate to the use of technology that helps law enforcement make accurate, effective and efficient decisions in the course of an investigation. Requiring probable cause to get basic, limited information about a person's historical location would make it significantly more difficult to solve crimes and seek justice.

Thank you for your time and the opportunity to address this issue.

Mr. SENSENBRENNER. Thank you.
Ms. Crump?

TESTIMONY OF CATHERINE CRUMP, STAFF ATTORNEY, AMERICAN CIVIL LIBERTIES UNION (ACLU)

Ms. CRUMP. Good morning, Chairman Sensenbrenner, Ranking Member Scott, Chairman Emeritus, and Members of the Subcommittee.

Thank you for the opportunity to testify on behalf of the American Civil Liberties Union.

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 that tragedy and with their families.

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. That is as it should be. No one denies that electronic surveillance can be an important tool for law enforcement and, indeed, in horrific and rare events, such as what transpired in Boston, an essential one.

That is why the ACLU has always supported an exemption in the law permitting immediate disclosure of location data in aid to agencies in such life and death situations. However, in routine investigations, law enforcement agencies, such as the 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 agents to access the tools they need while providing an independent check and balance through review by a judge, which will ensure that innocent Americans do not have their privacy violated.

Mobile phone location 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 both public and private areas. It also makes it possible for law enforcement agents to identify all individuals located in a particular location, a valuable tool, but one that, by necessity, can reveal the location of thousands or even tens of thousands of innocent Americans.

In many parts of the country, the police have been tracking mobile phones for days, weeks, or even months at a time without ever having to demonstrate to an independent judge that they have a good reason to believe the tracking will turn up evidence of wrongdoing.

Mobile phone location data implicates strong privacy interest because tracking people's movements makes it possible to learn a great deal of personal and private information about them. As Justice Alito explained, society's expectation has been that law enforcement agents would not and, indeed, in the main could not track people's movements over a long period of time in their car, an observation which applies with even greater force to the cell phones people carry with them all the time.

The warrant and probable cause requirements are essential components of the Fourth Amendment. The probable cause require-

ment is not high. Law enforcement merely has to have a good reason to believe that a search will turn up evidence of wrongdoing.

It is useful to identify points of agreement between law enforcement interests and those civil society organizations concerned about privacy. First, the Department of Justice already recommends that its agents obtain a warrant based upon probable cause to secure real-time precision location information, the very standard that the ACLU supports.

Also, local law enforcement agencies, such as the County of Hawaii, Wichita, and Lexington, Kentucky, already secure warrants across the board. Thus, merely codifying a longstanding Department of Justice policy would help protect Americans' privacy.

Second, we agree with Mr. Eckenwiler, as he stated in his written testimony, that the so-called cell tower dumps, the acquisition of location data of all individuals at a particular location, pose especially grave privacy concerns because they could sweep up the locations of thousands of innocent Americans. Like Mr. Eckenwiler, we believe the Committee should consider additional statutory protection, such as limits on the number of records or the length of time window requested or protocols for sealing or destroying the documents obtained.

We also agree with numerous law enforcement representatives that the current legal standards in force are unclear. However, we part ways over the applicable legal standard because the warrant and probable cause requirement should apply across the board to cell phone location data.

These requirements are especially important today, given the tremendous and rapid technological development over the past 10 years that make it easier than ever to track Americans' every movement. The ACLU supports passage of the GPS Act because it would ensure that law enforcement agents obtain a warrant based upon probable cause to access mobile phone location data subject to appropriate exceptions.

Thank you.

[The prepared statement of Ms. Crump follows:]

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. Commc'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 cite 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/lsojNy.

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.

Mr. SENSENBRENNER. Thank you.
Mr. Blaze?

TESTIMONY OF MATTHEW BLAZE, PROFESSOR, UNIVERSITY OF PENNSYLVANIA

Mr. BLAZE. First of all, thank you. Thank you, Chairman Sensenbrenner and Members of the Subcommittee, for the opportunity to testify here today.

The focus of my remarks will be on the technology of mobile location tracking and the trends that we can expect mobile location technologies to follow as these devices become a more ubiquitous and critical part of our daily lives into the future.

I think the most important thing for the Committee to consider in drafting legislation regulating the use of location information from mobile devices is that this is a very rapidly moving area of technology, enjoying continued and explosive growth. And that will continue for the foreseeable future and beyond.

I'd like to talk for just a few moments about how cellular mobile devices operate. Of course, as you know, cellular telephones and cellular data devices, such as tablet computers, operate not with a wired connection, but rather with a radio connection.

The radio connection is provided by a service provider that operates a network of base stations throughout its geographic coverage area. These base stations are alternatively called cell sites or cellular base stations or sometimes towers or sector antennas. The terms are approximately equivalent for our purposes here.

Unfortunately, the capacity of any given base station is limited by two fundamental factors. The first and today less important one is the radio range over which they can operate. A cellular telephone under ideal conditions in a clear radio spectrum may be able to operate with a base station as far as a mile or two from the cellular handset.

But the more important limitation is the spectrum capacity of the frequency bands that are used by the mobile service providers. Each base station has a limited number of calls that it can process, a limited number of data services that it can handle simultaneously from different customers.

So as cellular and mobile technology has grown and become so important, as we all get different mobile devices and use them more often for more things, with higher bandwidth broadband connections, service providers have had no choice but to reduce the geographic area over which each base station operates so that smaller cell towers, smaller antennas cover a smaller number of users who can take advantage of the services that they've provided.

And this trend has over the last 15 years been continuously in the direction of higher and higher density. We have provided more spectrum to mobile service providers, but the amount of spectrum is ultimately limited not by regulation, but by physics, and so really the only direction in which growth can happen at the explosive pace that it's occurring is by making the base stations serve a smaller and smaller geographic area.

One of the trends is the use of small cell sites that cover very small geographic areas, such as an individual home or an individual office. These are sometimes called microcells or picocells or

femtocells. Various service providers offer them. These may cover an area as small as this hearing room or our homes.

Because of this increased density and because of this increased amount of usage, it's become more difficult to meaningfully distinguish between cell site location and other geolocation technologies, such as vehicle-based GPS and precise location technologies that are used for E911 services, particularly if we consider how revealing this information is about our daily lives.

Unlike vehicle-based GPS surveillance, we carry our cellular telephones with us everywhere we go. We have them on at all times. We take advantage of data services that cause them to send and receive data without us being aware that it's occurring in many cases. And we can use them indoors and in private spaces, unlike GPS devices, which generally work only outdoors with a view to the satellite.

And then, finally, the precision with which these can be located is increasing as the density improves, and that trend is going to continue because service providers have no choice but to improve density if they want to provide more services——

Mr. SENSENBRENNER. The gentleman's time is expired.

Mr. BLAZE. Oh, I'm sorry. My light wasn't working.

[The prepared statement of Mr. Blaze follows:]

House Committee on the Judiciary

Subcommittee on Crime, Terrorism, and Homeland Security

Hearing on ECPA, Part 2: Geolocation Privacy and Surveillance

Written Testimony of

Professor Matt Blaze

April 25, 2012

1. Introduction and Background

Thank you for the opportunity to provide some background about location technology in current and emerging wireless networking. I hope my remarks will be helpful in understanding how location information is calculated and the direction that this important and yet rather complex technology is taking. I offer this statement today on my own behalf and do not represent any other party or organization.

As I will discuss below, geolocation is an area that is enjoying a period of rapid technological innovation and competition among different technologies. Many assumptions that might have been true several years ago, such as that GPS satellites always provide higher precision location information than the cellular network does, are no longer universally true today. For any legislation that seeks to regulate the use or disclosure of location tracking technology to

remain meaningful in the years to come, it is critical that it avoid defining terms in ways that are likely to become obsolete soon after it becomes law.

In sum, my primary messages to policy makers considering how best to legislate in the area of location tracking are:

- The accuracy and precision with which a cellular telephone handset can be located by network-based (non-GPS) techniques depends on a range of factors, but has been steadily improving as technology has advanced and as new infrastructure is deployed in cellular networks. Under some circumstances, the latest generation of this technology permits the network to calculate users' locations with a precision that approaches that of GPS.
- A mobile user, in the course of his or her daily movements, will periodically connect to cell towers serving large and small geographic sectors. Even if the network only records cell tower data, the precision of that data will vary widely for any given customer over the course of a given day, from the relatively less precise to the relatively very precise, and neither the user nor the carrier will be able to predict whether the next data location collected will be relatively more or less precise. For a typical user, over time, some of that data will inevitably reveal locational precision approaching that of GPS.
- Network-based geolocation can often be *more* revealing than GPS tracking, because new and emerging cell location techniques can work

> indoors and in places not typically accessible to GPS receivers, and the increasingly high resolution that that cell site tracking can achieve in densely populated areas -- and the ability to provide this data even when the handset is indoors -- can paint an even richer picture of an individual's movements than GPS.

I am currently an associate professor of computer and information science at the University of Pennsylvania in Philadelphia, where I serve as director of the Distributed Computing Laboratory and conduct research on computer security, cryptography, network communication, and surveillance technology. Prior to joining the faculty at Penn, I was for 12 years a member of the research staff at AT&T Labs (previously known as AT&T Bell Labs) in New Jersey. I have a PhD in computer science from Princeton University, a Masters degree from Columbia, and I completed my undergraduate studies at the City University of New York.

A focus of my research is on the properties and capabilities of surveillance technology (both lawful and illicit) in the context of modern digital systems and communications networks. This research aims to strengthen our critical infrastructure against criminals and other unauthorized eavesdroppers and to help ensure that authorized surveillance systems work as intended in the rapidly changing environments in which they must reliably collect evidence and investigative intelligence. Sometimes, this work has led to surprising observations about real-world surveillance systems. For example, in 1994, I

discovered weaknesses in the NSA's "Clipper" key escrow encryption system that led to that system's abandonment before it was widely deployed. More recently, my graduate students and I found previously undiscovered vulnerabilities in analog telephone wiretaps used by law enforcement, and we identified ways for law enforcement agencies to harden their CALEA intercept systems against a variety of surveillance countermeasures.

There is perhaps no more ubiquitous symbol of our highly connected society than the cellular telephone. Over the course of only a few short decades, mobile communication devices have evolved from being little more than an expensive curiosity for the wealthy into a basic necessity for most Americans, transforming the way we communicate with one another, do business, and obtain and manage the increasing volume of information that is available to us. According to recent estimates, there are today more than 331 million active wireless subscriber accounts in the United States. Many households now forgo traditional "landline" telephone service, opting instead for cellular phones carried by each family member. Wireless carriers have strained to keep up with the explosive demand for cellular service, in many areas deploying new infrastructure (most visibly cellular antenna towers) as quickly as they can find places to put it.

As difficult as it may be to imagine modern life without the cell phone, it is sometimes easy to forget how rapidly the technology has come about and how quickly new research ideas in wireless communication can advance into

products and services that we take for granted. Over the last 25 years the mobile telephone has transformed from an analog voice-only service (originally available in only a few markets) into a high-bandwidth, always-on Internet access portal. "Smartphones", such as the latest iPhones and Android devices, act not just as voice telephones, but as personal digital organizers, music players, cameras, email readers, and personal computers, in a package that fits in our pocket. We now carry our phones with us wherever we go, and we expect them to have service wherever we happen to be.

Many of the most important and innovative new applications and services that run on mobile devices take advantage of the ability to quickly and automatically detect the user's location to provide location-specific information and advice. At the same time, cellular providers calculate where phones in their networks are located (and how they move) to manage various network functions and to plan where new infrastructure is required.

2. Wireless Location Technologies

Unlike conventional wireline telephones, cellular telephones and cellular data devices use radio to communicate between the users' handsets and the telephone network. Cellular service providers maintain networks of radio base stations (also called "cell sites") spread throughout their geographic coverage areas. Each base station is responsible for making connections between the regular telephone network and nearby cellular phones when they make or receive calls. Cell phone handsets periodically (and automatically) identify themselves to the nearest base station (that with the strongest radio signal) as they move about the coverage area. If a phone moves away from the base station with which it started a call and nearer to a different base station, the call is "handed off" between base stations without interruption. This process of "registration" between a phone and the nearest cellular base stations happens automatically whenever a cellular handset is turned on; no intervention by the user is required. The effect is that phones will generally work any time they are within radio range of at least one base station, which allows users to use their phone at any location in their provider's geographic coverage area.

There are two different technical approaches that can be used for calculating the location of a cell phone. In the first approach, the user's phone calculates its own location using special GPS satellite receiver hardware built in to the handset. In the second approach, the cellular system infrastructure calculates

the location of the phones that are active in the network, using the normal cellular radio interfaces and without explicit assistance from the users' handsets.

2.1 Handset-based GPS

For smartphone applications that run on the user's handset, the most prominent location technology is GPS. In GPS location, a user's phone contains special hardware that receives signals from a constellation of global position satellites. This allows a phone handset to calculate its latitude and longitude whenever it is in range of the satellites. GPS technology can achieve very high spatial resolution (typically within ten meters). In the latest phone models that incorporate GPS chipset hardware, GPS location features are integrated into applications for mapping, street directions, and to obtain information about local services and merchants.

Whether or not the calculated GPS location of a handset is sent to the network (or any other third party) depends on the application software that the phone is running. Some applications, as a matter of course, may periodically transmit their location to external services. For example, a mapping application might send its current GPS-calculated location to a network-based service in order to discover, say, the locations of nearby businesses that might be of interest to the user. Network-based services that make use of a phone's GPS location

might be offered by the cellular carrier or by a third party, internet-based entity.

Unfortunately, GPS, for all its promise, has a number of fundamental limitations. It relies on special hardware in the phone (particularly a GPS receiver chip) that is currently included only in the latest handset models and that generally is enabled for location tracking only when the phone user is explicitly using it to run a location-based application on the phone. Perhaps most importantly, GPS works reliably only outdoors, when the handset is in "view" of several GPS satellites in the sky above.

2.2 Network-based location

GPS is only one technology for cell location, and while it is the most visible to the end user, GPS is neither the most pervasive nor the most generally applicable cellular phone location system, especially in the surveillance context. More ubiquitously available are techniques that (unlike GPS) do not depend on satellites or special hardware in the handset, but rather on radio signal data collected and analyzed at the cellular providers' towers and base stations. These "network-based" location techniques can give the position of virtually every handset active in the network at any time, regardless of whether the mobile devices are equipped with GPS chips and without the explicit knowledge or active cooperation of the phone users.

The accuracy and precision with which a handset can be located by network-based (non-GPS) techniques depends on a range of factors, but has been steadily improving as technology has advanced and as new infrastructure is deployed in cellular networks. Under some circumstances, the latest generation of this technology permits the network to calculate users' locations with a precision that approaches that of GPS.

Network-based location techniques work by exploiting the cellular radio infrastructure that communicates between the network and the users' phones. All cellular systems have an extensive network of base stations ("towers") spread throughout their areas of service such that a cell phone in any locations in the coverage area is within radio range of at least one base station. This arrangement essentially divides the carrier's coverage area into a mosaic of local "sectors", each served by an antenna at a local cellular base station. Network-based location enables a cellular provider to identify the sector in which a user's phone is located, and, in some cases, to further pinpoint their location within a sector.

2.2.1 Sector identification

At a minimum, cellular providers record the identity of the particular base station (or sector) with which a cellular phone was communicating every time it makes or receives a call and whenever it moves from one sector to another. How precisely this information by itself allows a phone to be located depends

on the size of the sector; phones in smaller sectors can be located with better accuracy than those in larger sectors.

Historically, in the first cellular systems, base stations were generally placed as far apart from one another as possible while still providing adequate radio coverage across the area terrain (effectively making the sector areas they cover as large as technically possible). In early cellular systems, a base station might have covered an area several miles or more in diameter (and in sparsely populated, rural areas, this may still be true today). But as cellular phones have become more popular and as users expect their devices to do more and to work in more locations, the size of the "typical" cell sector has been steadily shrinking.

The reason for this trend toward smaller cell sectors is the explosive growth in the demand for wireless technology. A sector base station can handle only a limited number of simultaneous call connections given the amount of radio spectrum "bandwidth" allocated to the wireless carrier. As the density of cellular users grows in a given area, the only way for a carrier to accommodate more customers is to divide the coverage area into smaller and smaller sectors, each served by their own base stations and antennas. New services such as 3G and LTE/4G Internet create additional pressure on the available spectrum bandwidth, usually requiring, again, that the area covered by each sector be made smaller and smaller. At the same time, users increasingly rely on their mobile devices to work wherever they happen to be, indoors and out, on the

street, in offices and residences, even in basements and elevators. The only way to make service more reliable in more places under varying radio conditions is to add base stations that cover "dead spots". Adding base stations to eliminate dead spots further reduces the area of a typical sector's coverage.

As a result of these pressures, the number of cellular base stations has been growing steadily, with a corresponding decrease in the geographic area served by each. According to a recent Cellular Telecommunications Industry Association (CTIA) study, the number of cellular base stations in the United States tripled over the most recent ten year period. Indeed, this trend has been accelerating rapidly, with the deployment of the latest generation of smaller and smaller-scale cellular base stations (called, variously, "microcells", "picocells" and "femtocells"). These small cells are designed to serve very small areas, such as particular floors of buildings or even individual homes and offices. By some estimates, the number of these small-scale cellular base stations equaled or outstripped the number of conventional cells in the US in 2010, and their deployment continues to grow at a very fast rate.

The effect of this trend toward smaller cell sectors is that knowing the identity of the base station (or sector ID) that handled a call is tantamount to knowing a phone's location to within a relatively small geographic area. In relatively unpopulated areas with open terrain, a sector might cover an area miles in diameter. But In urban areas and other environments that use microcells, a

sector's coverage area can be quite small indeed, sometimes effectively identifying individual floors and rooms within buildings.

2.2.2 Enhanced location with time- and angle- of arrival

The decreasing size of cell sectors is not the only factor making cellular network-based location more accurate. New technology allows cellular network providers to locate not just the sector in which the users' wireless device is located, but its position *within* the sector. By correlating the precise time and angle at which a given device's signal arrives at multiple sector base stations, new technology now makes it practical for a network operator to pinpoint a phone's latitude and longitude at a level of accuracy that can approach that of GPS.

A variety of "off-the-shelf" products and system upgrades have recently become available to cellular providers that use enhanced time- and/or angle-of arrival calculations to collect precise location information about users' devices as they move around the network. Current commercially available versions of this technology can pinpoint a phone's location to an accuracy of within 50 meters or less under many circumstances, and emerging versions of the technology can increase accuracy even beyond that. This is accomplished without requiring any new or special hardware (such as GPS chips) to be installed on the end-users' phones. Accurate locations can be tracked with this technology even when no calls are being made or received, as long as the

user's phone is turned on and is within a coverage area. (Whether locations are routinely tracked and recorded at times other than when calls are made or received depends on the policy of the particular carrier).

Although these enhanced location technologies are not yet universally available in every network, wireless carriers are deploying them because they provide information that is extremely valuable in managing their networks and businesses. By tracking more precisely where mobile devices are located within sectors (and their patterns of movement), a carrier can better identify where new infrastructure might be required, where old infrastructure might be redundant, and how and where their customers use different service offerings.

While each carrier has its own data collection and retention practices, carriers typically create "call detail records" that can include the most accurate location information available to them. Historically, before more advanced location techniques were available, carrier call detail records typically have included only the cell sector or base station identifier that handled the call. As discussed in the previous section, the base station or sector identifier now carries with it far more locational precision than it once did.

As even more precise location information becomes available, cellular records increasingly (now and in the future) can effectively include what amounts to the customer's latitude and longitude along with the sector IDs traditionally used in cellular carrier databases. Some carriers will also store this location information not just when calls are made or received, but also about "idle"

phones as they move about the network. Creating and maintaining detailed records about the locations of phones as they move from place to place makes good engineering sense, and we should expect the trend toward more, and more precise, location data collection to continue as part of the natural progression of commercial wireless technology. Once the infrastructure to collect it is installed, the marginal cost of collecting and storing high-resolution location data about every customer is relatively small. Such information will be collected because it is extraordinarily valuable for network management, for marketing, and for developing new services.

3. Cell Phone Location and Law Enforcement Surveillance

As noted above, even on networks that do not employ time-of-arrival or angle-of-arrival location enhancements, the base station or sector location now identifies the location of a surveillance target with increasing specificity as cellular sectors become smaller and smaller and as microcells, picocells, and femtocells are being deployed to provide denser coverage. In legacy systems or in rural areas, a sector ID might currently specify only a radius of several miles, while in a dense urban environment with microcells, it could identify an individual floor or even a room within a building. How precisely the sector ID locates a target depends on the layout of the particular carrier's network and where in the network the target is located, but the industry trend is moving inexorably toward sectors that cover smaller and smaller areas.

Most carriers' systems use a variety of large and small sector configurations that vary based on the different terrain and densities they must cover. A mobile user, in the course of his or her daily movements, will periodically move in and out of large and small sectors. Even if the network only records cell tower data, the precision of that data will vary widely for any given customer over the course of a given day, from the relatively less precise to the relatively very precise, and neither the user nor the carrier will be able to predict whether the next data location collected will be relatively more or less precise. For a typical user, over time, some of that data will inevitably reveal locational precision approaching that of GPS.

As cellular carriers roll out better location technologies in the course of their business, the location information sent to law enforcement (as transmitted from the carrier's call database in (near) real time in response to a wiretap order) is, inherently, becoming more and more precise. As sectors become smaller, the locational information they reveal becomes more intrinsically precise. And as networks improve, sector data is increasingly being linked to or supplanted by even more accurately calculated position information about each customer's handset.

In the past, when cell sectors were widely spaced and before the availability of the enhanced network-based location technologies now being deployed by wireless carriers, it may have been technically sound to distinguish between location based on the cellular network (at presumably low accuracy) and that based on GPS (at higher accuracy). Today, however, this distinction is increasingly obsolete, and as cellular networking technology evolves, it is becoming effectively meaningless. As microcell technology and enhanced location techniques become more widely deployed in cellular networks, the information revealed by the cell sector identifier pinpoints, under many circumstances, a user's location to a degree once possible only with dedicated GPS tracking devices. It 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. The gap between the location 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.

Because the precision provided by cellular network-based location techniques approaches that of GPS-based tracking technology, cellular location tracking has significant advantages for law enforcement surveillance operations over traditional GPS trackers. New and emerging cell location techniques can work indoors and in places not typically accessible to GPS receivers. Cellular location information is routinely and automatically calculated by the network, without triggering any suspicious or alerting behavior on the handset that might be noticed by the subject. And the "tracking device" is no longer a hidden box that must be surreptitiously installed and that might be discovered, but a benign object that is deliberately carried by the target: his or her own telephone, computer, or tablet.

These characteristics -- ubiquitous and continuous availability, lack of alerting, and high precision -- make network-based cellular tracking an extremely attractive and powerful tool for law enforcement surveillance. The increasingly high resolution that that cell site tracking can achieve in densely populated areas -- and the ability to provide this data even when the handset is indoors -- can paint an even richer picture of an individual's movements than can vehicle-based GPS devices.

Mr. SENSENBRENNER. That light isn't working. So sorry about that.

Mr. BLAZE. Thank you, Mr. Chairman.

Mr. SENSENBRENNER. Okay. The Chair will enforce the 5-minute rule during the question time and first recognizes the Chair of the full Committee, the gentleman from Virginia, Mr. Goodlatte.

Mr. GOODLATTE. Thank you, Chairman Sensenbrenner, and thank you for holding this hearing.

I regret that I wasn't able to be here at the outset. So I am going to use my question time to offer my observations about geolocation issues, and I will start by saying that the Electronic Communications Privacy Act, or ECPA, provides a myriad of protections. Keep in mind that it was enacted well before our everyday use of cell phones and the Internet, yet ECPA sets forth the rules that prevent unauthorized Government access to certain electronic records.

Even when it became law in 1986, ECPA, perhaps unintentionally, set the standards for the court-authorized disclosure of geolocation information. A suspect's location is often only a piece of the puzzle for law enforcement, but sometimes that piece is a matter of life or death.

In 2001, enhanced or E911 was deployed in the U.S. to associate a location with the origin of a phone call. Geolocation is critical in cases of child abductions, lost hikers, and missing Alzheimer's patients where every minute counts.

In many other investigations, geolocation is a vital building block in order to prevent or curtail a crime. Many criminals use false identities to impede law enforcement so they may complete their crimes and commit more. In every case, the identity of the criminal is essential for the investigation to move forward. The geolocation of dangerous fugitives is crucial, particularly after they are convicted of crimes like rape and murder.

Today, many civil liberty concerns center on the abundance of new technological devices and a lag in the law keeping pace with this new technology. For instance, the law is well settled when it comes to police entering a home to arrest someone or conduct a search. However, complexities arise when, by the use of cell phones, we are permitting communication providers to record our location to route a phone call.

We also allow them to record our location in order to advertize to us or send us instant coupons on our cell phones when we subscribe to a certain app. Cellular providers often use cell tower data, but also use GPS technology and our public Wi-Fi connections to determine where we are.

In updating our Federal surveillance laws, Congress must weigh our privacy interests with the needs of law enforcement without stifling commerce and innovation. Last week, the Department of Justice briefed Judiciary staff on its current practices in seeking geolocation data. I was encouraged to learn that the department seeks a court order for every type of geolocation information it acquires.

At a minimum, the department obtains what is called a 2703(d) Federal court order when it seeks historical cell site data on a particular cell phone. This cell site data only provides very general location information, which can vary widely.

On the other side of the spectrum, the Department of Justice obtains a search warrant from a Federal judge when it seeks very accurate real-time location information based on GPS satellite technology. Such search warrants are based on probable cause, the same standard specified in the Fourth Amendment to our Constitution.

While these practices are encouraging, current DOJ practices do not carry the same weight as Federal statutes. The privacy interests we have in our cell phones are being protected today through a patchwork of Federal laws. Our task is to reexamine current laws and give clarity to individuals, corporations, innovators, and law enforcement.

I look forward to working with my colleagues to examine geolocation privacy and surveillance. Our efforts must protect individual liberties by providing clear guidelines for when and how geolocation information can be accessed and used.

And I thank Chairman Sensenbrenner and yield back.

Mr. SENSENBRENNER. I thank the full Committee Chair.

The Chair recognizes the Ranking Member, Mr. Scott of Virginia.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. Modaferri, you indicated—you talked about a crime where somebody committed seven robberies. Was any attempt made to get historic data at those locations to see if one person had been in all seven sites at the particular times?

Mr. MODAFERRI. You mean a general subpoena for anybody in that area? No.

Mr. SCOTT. Well, if you had—if you got a document—if you got a tower dump from the seven different sites and cross-referenced and found that only one person had been at all seven sites at the same time, is that—would that have been possible information to get?

Mr. MODAFERRI. Not logically because all 7 robberies, the robberies were between 3 and 6 months apart in different locations in a tri-State area.

Mr. SCOTT. How long is the tower information kept?

Mr. MODAFERRI. That I don't know.

Mr. SCOTT. Anybody know how long tower information is kept?

Mr. ECKENWILER. Ranking Member Scott, it varies according to provider. Some keep that information for a few months. Some keep it for up to a year or two.

Mr. SCOTT. And so, if it was one of the services that kept it for a year or two, then you could have gotten information from the seven different locations. Is that true?

Mr. ECKENWILER. If there were, in fact, network events that would be represented. Certainly when the records are available, the Government can compel them. Whether or not there would be a commonality across all seven of those locations is dependent not just on whether the phone was present, but whether there was an active communication like the sending or receipt of a text message or a phone call.

Mr. SCOTT. The information that you are near a site is not recorded?

Mr. ECKENWILER. When the Government obtains a tower dump that you referred to, what is produced is only a set of affirmative

network activities, like the receipt of a call. A phone call is answered. A phone call is placed. It does not reflect the presence of all phones that are simply on but not in active communication at that time.

Mr. SCOTT. Is that because the information is not available or because it wasn't—you can't get it?

Mr. ECKENWILER. It's not the practice of the carriers to log that. There is not a real technical reason to retain information at that level of granularity.

Mr. SCOTT. How expensive is it to the either law enforcement, if they pay for it, or the provider to provide a tower dump?

Mr. ECKENWILER. I'd say a tower dump is fairly burdensome for the providers to disclose to law enforcement. And in practice, what often happens is law enforcement will obtain an order for a certain set of information, and there is often a negotiation, as there is in other cases—grand jury subpoenas and administrative subpoenas—to see if the scope of the request cannot be narrowed.

Mr. SCOTT. Ms. Crump, we were talking about probable cause before you get all of this information. Probable cause is usually that a crime has been committed and the—what would be the standard after the crime has been committed to try to catch people?

Ms. CRUMP. Are you contemplating the fugitive-type situation?

Mr. SCOTT. Yes.

Ms. CRUMP. I think that the civil liberties groups that support a probable cause requirement believe that in general the standard should be probable cause that a crime has been committed but also agree that it is important that fugitives be apprehended and don't have an objection to cell phone location data being used in that circumstance.

So a standard, for example, that there was an arrest warrant out for someone and that location information was useful to effectuate that arrest warrant is not something that anyone would object to.

Mr. SCOTT. There is an expectation that the Government isn't following you everywhere you go. How would you deal with emergency situations?

Ms. CRUMP. We support an exception such as that in place in the GPS Act. Earlier, Mr. Goodlatte set out a number of examples of emergency situations—a child abduction, a lost hiker, and situations like that. I think everyone agrees that in those types of circumstances, it is important that law enforcement be able to act immediately and that if there's not enough time to secure a warrant, that they should be able to proceed on an emergency basis and go ahead and locate someone.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. SENSENBRENNER. Thank you.

The junior Chairman emeritus of the Committee, the gentleman from Michigan, Mr. Conyers?

Mr. CONYERS. Well, I thank the senior Chairman emeritus for recognizing me.

This is an unusual hearing in that I can't remember ACLU ever quoting Justice Alito before, nor can I remember all of the emeritus being on the same bill of a Republican Member of the Committee, and the general agreement actually among the four witnesses. The

only difference of view that I have been able to note is the difference between a probable cause standard and a 2703(d).

And I was wondering do you firmly hold to that, to the 2703(d) order, Mr. Eckenwiler? Or are you prepared to reluctantly go along with the probable cause standard that is in the bill?

Mr. ECKENWILER. Mr. Conyers, I think, as Mr. Modaferri pointed out, one of the difficulties with adopting a probable cause standard for that less precise class of location data, cell site information, has significant potential to impair law enforcement investigations.

Think of this as the building block of—it's one of the building blocks for an investigation. In some cases, it may be used in conjunction with bank records. It may be used in conjunction with telephone toll records. There are various pieces that go into an investigation, especially at those earliest stages when probable cause has not yet been developed.

And so, I think there would be significant costs to law enforcement if an across-the-board probable cause standard were to be adopted. But I would also refer you to the language I quoted earlier from Jerry Berman, the executive director of EFF, testifying before joint House/Senate Judiciary Committee hearing.

Pointing out that the 2703(d) standard is, in fact, meaningful, Mr. Berman pointed out in his testimony court order protection will make it much more difficult for law enforcement to go on fishing expeditions. And he pointed out in that same testimony that law enforcement would have to meet this particular showing, this need to establish access to these records based on specific and articulable facts.

So law enforcement has to tell a story. It's not like certain other kinds of compulsory process, a grand jury subpoena, which merely issues from the prosecutor. It's not like a pen register order to monitor the noncontent activity on, say, a telephone line, the numbers dialed out or in. Those kinds of orders, under the existing statute, simply require a certification to a judge, who has no discretion.

2703 is different. A factual showing has to be made to the court, which the court may then weigh and, based upon that weighing of the showing, may grant or deny the application.

Mr. CONYERS. Professor Blaze, I know you have a slightly different view?

Mr. BLAZE. So I think this is one of the areas where Mr. Eckenwiler and I disagree. The gap between these different technologies is narrowing, I think, sufficiently that we can't really make meaningful distinctions between how revealing they are.

So if we understand GPS location technology to be revealing enough to warrant one standard, I don't see any technological basis to understand cell site location as being sufficiently less precise or less revealing to merit a different standard.

The gap is narrowing in how precise they are, and in some cases, cell site location can reveal location information when vehicle-based GPS would be unable to, such as when the target is indoors.

Mr. CONYERS. Well, I guess the probable cause standard based on the Fourth Amendment is more compelling. But you know, when you read these off the top, Chairman Sensenbrenner, you could probably use either one to accomplish your goal.

And I thank you for the time.

Mr. SENSENBRENNER. I thank the gentleman from Michigan.

The gentleman from Louisiana, Mr. Richmond?

Mr. RICHMOND. Thank you, Mr. Chairman.

Let me see, my first question, and I guess I will direct this question to Ms. Crump. Do cell phone users ever find out that their geolocation information has been divulged?

Ms. CRUMP. Thank you for the question.

That highlights one of the key problems with this form of tracking. On occasion, cell phone users do learn that they are tracked. But in order for that to happen, in general, they have to be prosecuted, and then that evidence has to be used in the case-in-chief.

That means that whenever someone is tracked and they are innocent or the Government chooses not to disclose that information, individuals never learn they were subject to that technique. That has had the effect of meaning that for a long time, the Government's policies and procedures for engaging in cell phone tracking have been shrouded in secrecy.

And we believe that it's important that individuals who are subject to this form of surveillance receive notice, at least after the fact when the investigation is closed, because that will increase the public's awareness and information about how the Government is balancing civil liberties and law enforcement interests.

Mr. RICHMOND. Now is that—is your position pretty consistent with what they do with wiretaps?

Ms. CRUMP. Yes, that's true.

Mr. RICHMOND. So after a wiretap, they do disclose to the person that they were subject to a wiretap?

Ms. CRUMP. Yes. That's the case.

Mr. RICHMOND. Do they also disclose that to the person who may have been on the phone with someone on a wiretap that they were—that their call was intercepted or that you all don't do that? Do you know that, Mr. Eckenwiler?

Ms. CRUMP. The answer—oh.

Mr. ECKENWILER. Yes. The—in general, the requirement under Section 2518 of Title 18 requires that notice be given. Often the court may direct the scope of the disclosure, but it is not simply limited to the person who is named in the wiretap order.

So, in direct response to your question, yes, other communicants with whom that person has, say, spoken on the phone would also typically receive notice.

Mr. RICHMOND. Is there a timeframe on that notice or——

Mr. ECKENWILER. The statute, Title III, the Wiretap Act currently says that the—what's called the inventory must be given within 90 days after the termination of the wiretap, although the delay of notice may be extended for good cause shown to the issuing court.

Mr. RICHMOND. And I don't know if we discussed it, but I will go back to you, Ms. Crump. What standard do you think should be applied to the one-time ping or the real-time looking at where a person is once?

Ms. CRUMP. Our view is that a one-time real-time tracking ping should also require probable cause. The reason for that is you do not know, generally speaking, when you conduct that ping whether someone is going to be in a, for instance, a private place where

they have a reasonable expectation of privacy. And the better rule is a probable cause requirement across the board.

Mr. RICHMOND. We have mentioned a couple of times about reasonable expectation of privacy, and I guess as technology evolves, at some point, do you think there is going to be a discussion that if you have your cell phone with you, you probably don't have a reasonable expectation of privacy?

Ms. CRUMP. No. I don't think people should have to give up their privacy rights simply because today's modern era essentially requires people to have a cell phone in order to participate. It has traditionally been the case that individuals have been able to move around public and private places without being subject to the continuous monitoring and permanent recording of their movements.

I think that's an important freedom and that it shouldn't be sacrificed just because we now have cell phones.

Mr. RICHMOND. Well, you mentioned the recording of their movements, and I guess that one is probably a lot easier than the real-time where you are. And I wouldn't want anyone recording my movements, but do I have a reasonable expectation of privacy that if I was in the audience, no one would know I was here?

I mean, as it evolves, the question is how realistic it becomes and how reasonable that expectation is? And that is why I pose it because at some point, I think that question will become very relative to all of the conversations that we have in terms of our privacy.

Mr. Eckenwiler, did you want to add to that?

Mr. ECKENWILER. It's certainly true, Congressman Richmond, that there are different kinds of location data, many of which are overtly public. People who post on social media and choose to turn on their location disclosure feature, I think it would be abundantly clear that there is no expectation of privacy that attaches to that kind of location information.

Mr. RICHMOND. I thank you, and I yield back, Mr. Chairman.

Mr. SENSENBRENNER. I thank you.

The gentlewoman from California, Ms. Chu?

Ms. CHU. Thank you, Mr. Chair.

For the panel, I would like to ask this question. We trust law enforcement to use their own discretion in deciding whom to physically follow around for extended periods of time. Why can't law enforcement be trusted to exercise their discretion when engaging in similar tracking using GPS systems or cell phones?

Isn't using electronic tracking just more efficient, or is there something fundamentally different about electronic tracking? Ms. Crump?

Ms. CRUMP. Thank you for the question.

There is something fundamentally different about electronic tracking. Physical tracking is by necessity limited by officer resources. And because that form of tracking requires the expenditure of tremendous resources, that itself acts on a check against abusive forms of that tracking.

In contrast, electronic tracking is wholly concealed. Individuals don't know it's happening, but it can also be done in a very resource-efficient way, which means that legal protections against it are all the more important.

Ms. CHU. Mr. Blaze?

Mr. BLAZE. If I might just add to that? And the electronic tracking, unlike physical surveillance, follows us wherever we go, particularly cell phone-based electronic tracking.

It follows us indoors into private spaces, in places where physical surveillance would be unable to track somebody, at least undetectably. So there is a technological distinction as well.

Ms. CHU. Thank you.

Mr. ECKENWILER. Thank you for the question, Congresswoman Chu.

I agree that a probable cause standard is appropriate for real-time GPS or other precise location data. Let me give you a couple of reasons.

One is that it is not event based. Cell site information is derived from specific overt user activity, a call, the sending of a text message. And so, that's generated in the network. The network has to know about that.

The network can't not know about it anymore than I can dial a phone number without telling the phone company what number I want to call. It just is an innate part of the transaction. But the acquisition of precise location information may be done, as I indicated in my opening remarks, even when there is not an active communication in progress on the device.

What's also I think significant here, even before anybody had cell phones, the Supreme Court indicated in a case in the early 1980's with respect to physical tracking devices that when a tracking device actually reveals the presence of something within a protected area that's not otherwise observable by the police, that that can implicate a reasonable expectation of privacy. That's the Karo case, K-a-r-o.

Now there's an important distinction here, and that is between whether the item is merely in a protected area or whether the information about it reveals that it's there. So it's not just enough that something is in some area at the time that location data like cell site is acquired. But if the information is so precise as to place it inside a particular home, which is what happened with the physical GPS tracker in Karo, then, yes, indeed. If you apply that same logic to cell phone GPS, it would follow that there's an expectation of privacy.

Ms. CHU. Yes, in fact, I wanted to follow up by saying that the majority opinion in *Jones* found that a search occurred because law enforcement had committed a trespass by fixing this GPS tracking device to a private vehicle without a valid warrant. Does that means there is less of a concern when location tracking is done without fixing a device, such as using cell phone location data?

Ms. Crump?

Ms. CRUMP. No, I don't think there's any less of an expectation of privacy. The one opinion did focus on trespass, but five other justices focused on the nature of the intrusion of being tracked. To be sure, that case involved attachment of a GPS device, but I don't think, practically speaking, whether the technological method is attachment of a GPS device or a cell phone makes any difference.

Although I'm always glad when there's agreement between the Department of Justice and the ACLU on a question, however we get there, I do think the distinction between whether the location

data is generated by the network or an act of intrusion into the phone is overly formalistic, and the more common sense approach is to focus on the privacy intrusion and what people's expectations are.

Mr. SENSENBRENNER. The gentlewoman's time has expired.

And the Chair yields himself 5 minutes to wrap up.

Last year, the court handed down the *Jones* decision, and about the only thing the justices could agree upon was that there was a search that occurred. And then they were all over the map under what circumstances, a judicial review, and I don't want to talk about what type of specific review would be or what kind of warrant or 2703 device would be.

But I would like to each ask of the witnesses whether they think it would be wise for Congress to try to set some markers on what needs to be done in advance, if anything, with various types of use of GPS equipment, or the topic of our first hearing on ECPA, largely to prevent a court decision from coming down years from now which might reopen or place in jeopardy cases that already had been filed.

And I would like to ask each of the four witnesses to answer that question. Meaning do we need a bill, and what should the bill contain?

Mr. ECKENWILER. Thank you, Mr. Chairman.

Just so I understand the question, is this directed to physical GPS, or do you still have in mind phone GPS?

Mr. SENSENBRENNER. Both.

Mr. ECKENWILER. As to physical GPS, such as that that was at issue in the *Jones* case, it seems to me the Supreme Court has laid down a pretty clear marker, and there is already—at least in Federal Rule 41, there has been since 2006 a set of procedures for applying for and obtaining a warrant to install and use a physical tracking device. So it's not clear to me that there's a particular need for this Committee to act in that area.

Mr. Chairman, you mentioned prior cases, cases that may have been investigated or charged prior to a particular court decision. What's interesting is that in the roughly 14 months, 15 months since *Jones* came down, that issue has come up across the country in various courts. And generally speaking, *Jones* has not resulted in the suppression of evidence for pre-*Jones* law enforcement conduct. The short answer is there's a good faith exception.

And then to respond briefly to your question about phone location information, I would simply reiterate what I said earlier. I think that would come at significant expense to important law enforcement equities. As to cell site location information, I don't think that it would be inappropriate at all to clarify, and in fact, I've mentioned in my list of areas for the Committee's further inquiry the potential need to amend Rule 41 for prospective GPS acquisition on phones.

Mr. SENSENBRENNER. Mr. Modaferri?

Mr. MODAFERRI. Thank you.

I would say that from my perspective as a detective, we do need clarification. We do need an act to clarify what Mr. Eckenwiler's—the points that Mr. Eckenwiler made because we are acting some-

what in the dark in certain areas. And as technology evolves, we need a law that can address things as it changes.

But I wouldn't—I'm not a lawyer so I won't get into the details of Mr. Eckenwiler.

Mr. SENSENBRENNER. Ms. Crump?

Ms. CRUMP. The short answer to your question is, yes, it is essential that Congress act. It took many years for the court to even reach the *Jones* decision. GPS tracking had been going on for a long time, and it only partially answered the question. And it's important that this body step in and clarify the law so that everyone understands what their rights are.

Second, I think law enforcement and civil liberties organizations such as the ACLU at the least agree that the current system is unclear and in a state of chaos with judges applying different standards to identical forms of tracking in different States and that it's important that the law be uniform.

Mr. SENSENBRENNER. Mr. Blaze?

Mr. BLAZE. Thank you.

I'm also not an attorney. So I will answer from the technical perspective. Any legislation that attempts to distinguish between the revealing and intrusiveness of vehicular GPS, precise cellular geolocation, and cell site geolocation will be doomed to become increasingly meaningless as those technologies converge in their precision.

Mr. SENSENBRENNER. That concludes this hearing.

Without objection, all Members will have 5 legislative days to submit additional written questions for the witnesses and additional materials for the record.

The gentleman from Virginia?

Mr. SCOTT. Mr. Chairman, I ask unanimous consent that a law review article by Stephanie Pell, published in the Berkeley Technology Law Journal, be entered in the record.*

Mr. SENSENBRENNER. Without objection.

And without objection, the hearing is adjourned.

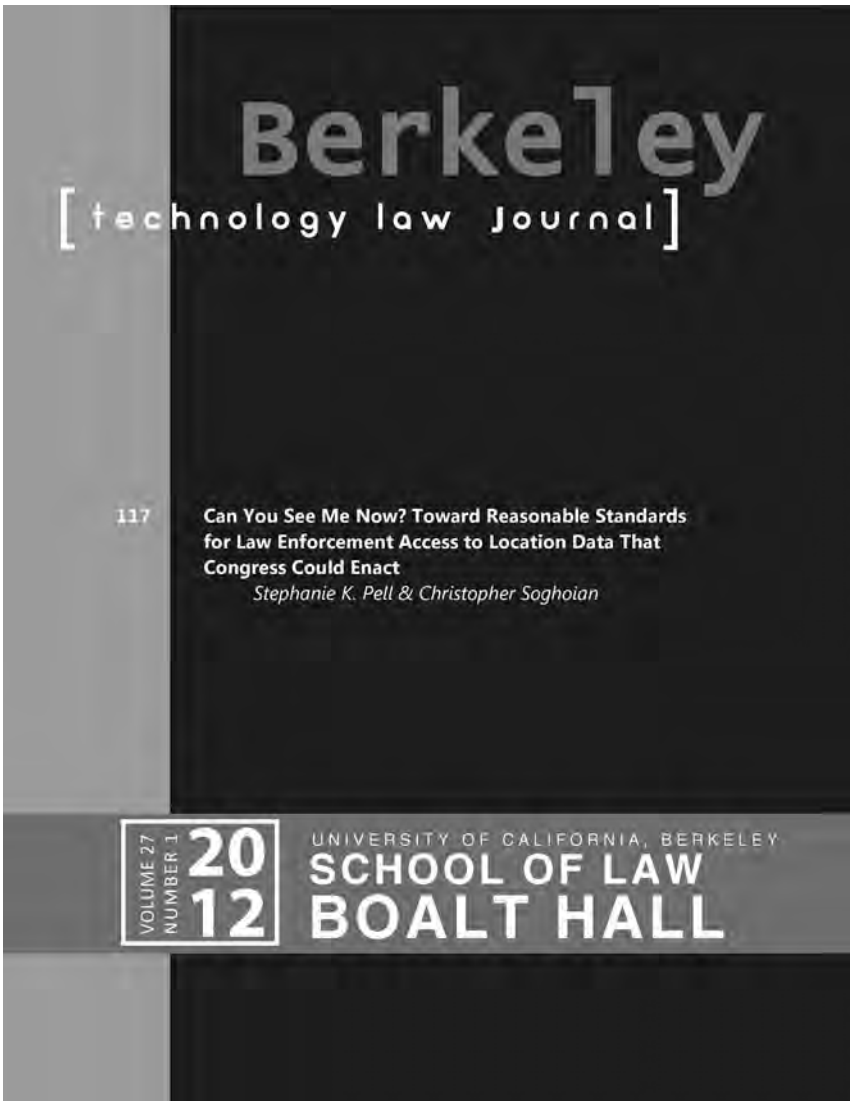
[Whereupon, at 11:06 a.m., the Subcommittee was adjourned.]

*See Appendix.

APPENDIX

Material Submitted for the Hearing Record

Material submitted by the Honorable Robert C. "Bobby" Scott, a Representative in Congress from the State of Virginia, and Ranking Member, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations



CAN YOU SEE ME NOW?: TOWARD REASONABLE STANDARDS FOR LAW ENFORCEMENT ACCESS TO LOCATION DATA THAT CONGRESS COULD ENACT

Stephanie K. Pell[†] *& Christopher Soghoian*[††]

ABSTRACT

The use of location information by law enforcement agencies is common and becoming more so as technological improvements enable collection of more accurate and precise location data. The legal mystery surrounding the proper law enforcement access standard for prospective location data remains unsolved. This mystery, along with conflicting rulings over the appropriate law enforcement access standards for both prospective and historical location data, has created a messy, inconsistent legal landscape where even judges in the same district may require law enforcement to meet different standards to compel location data. As courts struggle with these intertwined technology, privacy, and legal issues, some judges are expressing concern over the scope of the harms, from specific and personal to general and social, presented by unfettered government collection and use of location data and how to respond to those harms. Judges have sought to communicate the scope and gravity of these concerns through direct references to Orwell's dystopia in *1984*, as well as suggestive allusions to the "panoptic effect" observed by Jeremy Bentham and his later interpreters, such as Michel Foucault. Some have gone on to suggest that privacy issues raised by law enforcement access to location data might be addressed more effectively by the legislature.

This Article proposes a legislative model for law enforcement access standards and downstream privacy protections for location information. This proposal attempts to (1) articulate clear rules for courts to apply and law enforcement agents and industry to follow; and (2) strike a reasonable balance among the interests of law enforcement, privacy, and industry with the ultimate goal of improving the position of all concerned when measured against the current state of the law.

---

† Principal, SKP Strategies, LLC; former Counsel to the House Judiciary Committee; former Senior Counsel to the Deputy Attorney General, U.S. Department of Justice; former Counsel to the Assistant Attorney General, National Security Division, U.S. Department of Justice; and former Assistant U.S. Attorney, Southern District of Florida. Email: stephanie@stephaniepell.net

†† Graduate Fellow, Center for Applied Cybersecurity Research; Ph.D. Candidate, School of Informatics and Computing, Indiana University. Email: chris@soghoian.net.

The authors would like to thank Derek Bambauer, Catherine Crump, Susan Freiwald, Jim Green, Albert Gidari, Markus Jakobsson, Paul Ohm, Christopher Slobogin, and Magistrate Judge Stephen Wm. Smith for their feedback and assistance. The authors would also like to thank the attendees of the Privacy Law Scholars Conference, where this Article was presented in the summer of 2011.

TABLE OF CONTENTS

I. INTRODUCTION

Over several months in 2008, a gang of five men, described as the "Scarecrow Bandits" in media reports, committed or attempted twenty-one violent "takeover-style" bank robberies in the Dallas area.[1] FBI agents investigating the case contacted cellular telephone companies and obtained phone number logs to determine which telephones had been near the banks around the time of the heists. By searching these voluminous records, agents discovered that two phones had made calls near twelve of the robbed banks.[2]

1. *See* Press Release, Dep't of Justice, Federal Jury Convicts Scarecrow Bandits on Bank Robbery and Firearm Offenses (Aug. 13, 2009), http://www.justice.gov/usao/txn/PressRel09/scarecrow_bandits_convict_pr.html.

2. *See* Declan McCullagh, *Feds Push for Tracking Cell Phones*, CNET NEWS (Feb. 11, 2010), http://news.cnet.com/8301-13578_3-10451518-38.html.

Similarly, after two men robbed a Connecticut bank in July 2008, law enforcement agents obtained historical cell tower logs revealing 180 different phone numbers that had made or received calls near the bank at the time of the robbery. Although these logs led police to two brothers, both of whom were soon arrested, the police also obtained and retained location information associated with 178 innocent people who will never learn that their phone companies disclosed information to police.[3]

Law enforcement agencies—already using location information in their investigations—are likely to increase their reliance on such information as technology improves.[4] This is true of requests for all types of mobile device location data, whether historical or real-time (prospective),[5] in conducting criminal investigations and locating fugitives. For example, primarily due to the use of location information, the average time needed for the U.S. Marshals Service to find a fugitive has dropped from forty-two days to only two.[6] In recent congressional testimony, a senior Department of Justice ("DOJ") official explained how a homicide detective and his partner in Prince George's County, Maryland, used "cell tower [location] information" to pursue a man wanted for a triple murder, capturing him in only nine hours.[7] Having this information "immediately accessible" allowed the marshals to deploy "available law enforcement resources [effectively] . . . without placing officers, or the public, at undue risk."[8] Clearly, location information has become a powerful investigative tool in support of a range of law enforcement responsibilities.[9]

---

3. *See* Declan McCullagh, *ACLU: FBI Used 'Dragnet'-Style Warrantless Cell Tracking*, CNET NEWS (June 22, 2010), http://news.cnet.com/8301-31921_3-20008444-281.html.

4. A more technical explanation of location information is presented *infra* Part II, but for purposes of this example, location information means information about or derived from a portable device, such as a cellular phone, that reveals the location of the device either approximately or with a high degree of precision.

5. McCullagh, *supra* note 2 ("Obtaining location details is now 'commonplace,' says Al Gidari, a partner in the Seattle offices of Perkins Coie who represents wireless carriers.").

6. *See Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. on Crime, Terrorism and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 2 (2011) (statement of Dr. Susan Landau), *available at* http://judiciary.house.gov/hearings/pdf/Landau02172011.pdf.

7. *The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing before the S. Comm. on the Judiciary*, 112th Cong. 5 (2011) [hereinafter *Senate Judiciary 2011 ECPA Hearing*] (statement of James A. Baker, Assoc. Deputy Attorney Gen., U.S. Dep't of Justice), *available at* http://1.usa.gov/1sojNy.

8. *Id.*

9. *See* Michael Isikoff, *The Snitch in Your Pocket*, NEWSWEEK (Feb. 18, 2010), http://www.newsweek.com/2010/02/18/the-snitch-in-your-pocket.html.

The tool proved so effective that the number of "requests"[10] to carriers for location information grew "exponentially" over the past few years, with major wireless carriers now receiving thousands of requests per month.[11] Sprint Nextel received so many requests that it developed a web interface that gave law enforcement direct access to its subscribers' location data.[12] Law enforcement agents used the website to "ping" Sprint subscribers over eight million times in a single year.[13]

Law enforcement's increased use of location information has spurred courts to scrutinize more closely government applications to compel third parties to disclose location data, as certain magistrate judges question and examine what legal standards govern law enforcement access to historical and prospective location information. Prosecutors "were using the cell phone as a surreptitious tracking device," Judge Smith, a federal magistrate in Houston, told a reporter from Newsweek. "I started asking the U.S. Attorney's Office, What is the legal authority for this? What is the legal standard for getting this information?"[14]

All law enforcement demands (not involving voluntary emergency disclosures) for location information, whether seeking historical or prospective data, require some type of court order authorizing a compelled disclosure.[15] Determining the proper access standard—whether the *higher* "probable cause" standard, the *lower* 18 U.S.C. § 2703(d) order requiring "specific and articulable facts" that the information sought is "relevant and

10. The use of the word "requests" in this context means both compelled disclosures of location information where law enforcement presents a third-party provider with a probable cause warrant or an 18 U.S.C. § 2703(d) order and voluntary emergency disclosures pursuant to 18 U.S.C. § 2702, where providers may voluntarily share information with law enforcement in the case of an emergency involving danger of death or serious physical injury to any person.

11. Isikoff, *supra* note 9 ("Albert Gidari, a telecommunications lawyer who represents several wireless providers, tells NEWSWEEK that the companies are now getting 'thousands of these requests per month,' and the amount has grown 'exponentially' over the past few years.").

12. Chief Judge Kozinski, in a dissent in which he stressed the importance of maintaining Fourth Amendment protections in the face of increasingly sophisticated forms of government surveillance, noted that "[w]hen requests for cell phone location information have become so numerous that the telephone company must develop a self-service website so that law enforcement agents can retrieve user data from the comfort of their desks, we can safely say that 'such dragnet-type law enforcement practices' are already in use." United States v. Pineda-Moreno, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, J., dissenting from denial of rehearing en banc).

13. *Id.* at 1125.

14. *See* Isikoff, *supra* note 9.

15. *See* discussion *infra* Sections III.A and III.B.

material to an ongoing criminal investigation,"[16] or some other "hybrid" standard—is anything but clear under current law. As various courts struggle to apply the Electronic Communications Privacy Act ("ECPA")[17] and the Fourth Amendment to compelled disclosures of location information, a messy, inconsistent legal landscape has emerged: "within the same judicial district, you might have two magistrates who disagree and issue contrary orders for the standard upon which to disclose that [location] information."[18] Indeed, the degree of confusion over the appropriate standard to apply to location information is increasing and has spread across judicial districts.[19]

The House Judiciary Committee's Subcommittee on the Constitution, Civil Rights, and Civil Liberties began to respond to this landscape of uncertainty in 2010 by holding a series of ECPA reform hearings, one of which focused specifically on location information.[20] Prior to the hearings, a

16. 18 U.S.C. § 2703(d) (2010).

17. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.). This Article uses the term ECPA to describe the first three titles of the Electronic Communications Privacy Act: Title I ("Interception of Communications and Related Matters"), 100 Stat. at 1848, which amended the Wiretap Act (commonly referring to Title III ("Wiretapping and Electronic Surveillance") of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211–25 (codified as amended at 18 U.S.C. §§ 2511–2520 (2010))); Title II ("Stored Wire and Electronic Communications and Transactional Records Access"), commonly referred to as the Stored Communications Act (SCA), Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860–1868 (codified as amended at 18 U.S.C. §§ 2701–2712 (2010)); and Title III ("Pen Registers and Trap and Trace Devices"), commonly referred to as the Pen/Trap Devices statute, Pub. L. No. 99-508, tit. III, 100 Stat. 1848, 1868–1873 (codified as amended at 18 U.S.C. §§ 3121–3127 (2010)).

18. *Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 26 (2010) [hereinafter *House Judiciary 2010 ECPA Reform Hearing*] (written statement of Albert Gidari, Perkins Coie LLP), *available at* http://judiciary.house.gov/hearings/printers/111th/111-98_56271.pdf.

19. *See generally ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 81–85, 93–94 (2010), [hereinafter *Location Hearing*] (written statement of Judge Stephen Wm. Smith, U.S. Magistrate Judge), *available at* http://judiciary.house.gov/hearings/printers/111th/111-109_57082.pdf (summarizing and collecting inconsistent decisions).

20. *See Location Hearing*, *supra* note 19. The overarching goal of this hearing was to educate Subcommittee Members about how location-based technologies and services work, and how ECPA's application to location information was creating a state of legal chaos for Magistrate Judges, as well as industry, privacy, and law enforcement stakeholders. In his opening statement at the Location Hearing, Subcommittee Chairman Jerrold Nadler remarked that:

> any legislative changes to ECPA must . . . sustain the public's confidence in the security of their communications or it [could] harm both the robust

number of companies and civil liberties groups joined together to create the Digital Due Process ("DDP") Coalition in order to propose principles to guide congressional consideration of ECPA reform.[21] One principle proposed a new standard for law enforcement access to all types of location information, stating that "[t]he Government should obtain a search warrant based on probable cause before it can track, prospectively or retrospectively, the location of a cell phone or other mobile communications device."[22] This principle seeks to treat historical and prospective location information equally under the law and to require law enforcement to meet a probable cause standard before obtaining access to any location data.

Unfortunately for the privacy community, DDP's probable cause standard is a "non-starter" for law enforcement. One senior DOJ official recently told a Senate Committee that "if an amendment [to the ECPA] were to unduly restrict the ability of law enforcement to quickly and efficiently determine the general location of a terrorist, kidnapper, child predator, computer hacker, or other dangerous criminal, it would have a very real and very human cost."[23] The Department of Justice will indeed resist the imposition of a high, unitary standard for location data access and will likely find no shortage of allies in Congress itself to do so effectively. Even the

> market for cell phones and the rapid innovation that is fundamental to the market's health. Because ECPA inevitably involves the interaction of all these important and complex considerations, we are taking the time through multiple hearings to educate ourselves carefully and fully before engaging in legislative action.
>
> . . .
>
> We are honored to have certain witnesses here today, who are experts in these technologies. They can give us the necessary background to embark upon an understanding of how they work, what types of information and records they can generate and store, and how they can be of assistance to law enforcement in appropriate circumstances.
>
> This initial educational effort is in my view not only warranted, but essential before we undertake any effort at amending or otherwise reforming ECPA. After we hear the terrain described, we will move on to other questions today—namely, how is ECPA currently being applied to these location based technologies and services by the courts?

Id. at 5–6.

21. *See About the Issue*, DIGITAL DUE PROCESS COALITION (May 5, 2010), http://www.digitalddueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163; *see also House Judiciary 2010 ECPA Reform Hearing*, *supra* note 18, at 12 (written statement of James X. Dempsey, Vice President for Pub. Policy, Ctr. for Democracy & Tech.), *available at* http://judiciary.house.gov/hearings/pdf/Dempsey100505.pdf.

22. *See Our Principles*, DIGITAL DUE PROCESS COALITION (May 5, 2010), http://www.digitalddueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163.

23. *Senate Judiciary 2011 ECPA Hearing*, *supra* note 7, at 5 (statement of James A. Baker, Assoc. Deputy Attorney Gen., U.S. Dep't of Justice).

DDP Coalition acknowledges that ECPA reform must "preserve the 'building blocks' of criminal investigations."[24] In other words, any amendments to the ECPA must continue to enable an investigative system that allows law enforcement to compel the disclosure of various types of non-content information under lower legal standards at the early stages of an investigation. Applying these less stringent standards to non-content information avoids the premature foreclosure of valid investigations, in that it allows agents to pursue early investigative leads and "build up" to the use of more intrusive tools to obtain more sensitive information protected by higher access standards, such as the contents of communications.

But the difficulty with imposing a probable cause standard upon law enforcement access to all location data, as a matter of policy, does not minimize or negate the need for Congress to examine how law enforcement uses location information and to assess the privacy impact of current law enforcement access standards for location information. That examination will reveal an urgent need for Congress to amend the ECPA—both to clarify the law and reestablish the balance of interests among law enforcement, privacy, and industry equities.[25]

The unitary probable cause standard advocated by the privacy community and rejected by law enforcement has led to a stalemate. So, where do we find ourselves? As co-authors who approach ECPA reform from very different backgrounds and perspectives, we recognize the need to propose law enforcement standards for location information that: (1) articulate clear rules for courts to apply and law enforcement agents and industry to follow; and (2) strike a reasonable balance among the interests of law enforcement,

---

24. *Id.*; *see also House Judiciary 2010 ECPA Reform Hearing*, *supra* note 18, at 16–17 (written statement of James X. Dempsey). The DDP Coalition recognizes that:

> [u]nder current law, government investigators often work their way up the ladder to probable cause, starting with subpoenas for subscriber identifying information and stored transactional data, then moving to court orders under 2703(d) for more detailed transactional data and court orders, based on less than probable cause, for real-time interception of signaling and routing information. Based on analysis of this and other data, they may have probable cause to obtain a search warrant.

Id.

25. Even the Department of Justice "applaud[s] [Senate Judiciary Committee] efforts to undertake a renewed examination of whether [ECPA's] current statutory scheme . . . adequately protects privacy while at the same time fostering innovation and economic development." *See Senate Judiciary 2011 ECPA Hearing*, *supra* note 7, at 6 (testimony of James A. Baker). Mr. Baker further notes that "[i]t is legitimate to have a discussion about our present conceptions of privacy, about judicially-supervised tools the government needs to conduct vital law enforcement and national security investigations, and how our statutes should accommodate both." *Id.*

privacy, and industry such that they could be included in legislation that might be passed by Congress. Articulating such a reasonable proposal requires knowledge of technology, law, policy, and politics.

For the purpose of offering a reasonable legislative proposal, we assume as an incontestable value that law enforcement should have access to location information that is necessary and sufficient to ensure the safety of the public by apprehending criminal perpetrators and disrupting future criminal activity—but no more. We also assume as a second and equally uncontestable value that people should be, and know they are, free from any government scrutiny of their location data that is not necessary to that public safety function. Neither of these values is an absolute one. As such, our proposal is neither the most "privacy protective" standard possible, nor the most "law enforcement friendly" standard imaginable. Indeed, what we offer in Part VI is the product of a dialogue between the authors: one a committed privacy advocate and technologist, the other a former federal prosecutor who has both used location tools in that role and considered them from a legislative perspective while working for the House Judiciary Committee.

We believe this Article will advance the debate by proposing a policy framework, including model access standards that will be palatable to all stakeholders insofar as each of their positions will be improved in some appreciable way. Part II of this Article provides a brief background discussion of various current location technologies and the level of location precision they offer. Part III explores the confusion currently plaguing courts over law enforcement access standards to location data and examines what those standards require the government to show. Part IV discusses some "lessons learned" from congressional hearings and advocacy efforts during the 111th Congress, specifically informed by Stephanie's work on the House Judiciary ECPA reform hearings. Part V examines how courts considering law enforcement access to global positioning system ("GPS") location information have articulated privacy impacts and other social harms using the interpretive frames of Orwell's dystopia in *1984*, as well as what has come to be called the "panoptic effect"—the anxious response produced by the presumed omnipresence of the government's gaze. Part V ultimately suggests that location privacy is best addressed by the legislative branch. Finally, Part VI presents a model legislative privacy framework for location information, including law enforcement access standards and other types of "downstream" privacy protections to ensure that, among other things, law enforcement agencies do not retain location data longer than needed for legitimate law enforcement purposes.

II. TECHNOLOGY

Over the past few decades, the mobile phone has evolved from a luxury status symbol to a necessity. By the end of 2010, more than ninety-five percent of the U.S. population subscribed to a mobile telephone service.[26] As consumers have embraced cellular phones, law enforcement agencies have gained access to several methods through which to obtain both historical and real-time (prospective) location information. Generally speaking, this information can be separated into two categories: passive collection of information incident to the delivery of cellular services, and active surveillance in which information is collected and processed solely to benefit law enforcement agencies. In addition to this distinction, there are several different technologies that can be used to obtain location information—some highly accurate, others much less so, but with the general direction of innovation tending towards greater precision. The purpose of this Part is to provide the reader with a brief introduction to each of these technologies and the ways in which they can be used to determine or track the location of individuals.

A. A BRIEF INTRODUCTION TO CELL PHONE TECHNOLOGY

Unlike conventional "wireline" phones, mobile phones use radio to communicate between the customer's telephone and the carrier's network. Service providers maintain large numbers of radio base stations (also called "cell sites") spread throughout their geographic coverage areas.[27] These cell sites are generally located on "cell towers" serving geographic areas of varying sizes, depending upon topography and population concentration. Service providers are deploying higher-capacity network architectures, with the potential to provide more precise information regarding a phone user's location.

As part of their normal function, mobile phones periodically identify themselves to the nearest cell site as they move about the coverage area.[28]

---

26. *Wireless Quick Facts*, CTIA—WIRELESS ASS'N (2011), http://www.ctia.org/advocacy/research/index.cfm/aid/10323.

27. Press Release, Informa Telecoms & Media, The Shape of Mobile Networks Starts To Change as Femtocells Outnumber Macrocells in US (Oct. 21, 2010), http://femtoforum.org/fema/pressreleases.php?id=269 ("[F]emtocells now outnumber conventional outdoor cell sites in the United States marking a major milestone in the evolution of mobile networks. Conservative estimates suggest there are currently 350,000 femtocells and around 256,000 macrocells in the US. Furthermore by March 2011, there are expected to be at least twice as many femtocells as macrocells in the US.").

28. *Location Hearing*, *supra* note 19, at 13 (testimony of Prof. Matt Blaze, Univ. of Pa.) ("Cell phones, as they move and as they are turned on, discover the base station with the

This enables wireless carriers to know how to reach a particular subscriber's phone when it receives a call. Of course, mobile telephones (as their name suggests) are portable, and so when a phone moves away from the cell site with which it started a call and nearer to a different cell site, the call is "handed over" from one cell site to another without interruption.[29]

Each cell site has a large but fixed maximum capacity that can transmit a limited number of concurrent calls and data streams. In an area with a low number of users (or users who make few calls and who are not heavy users of data services), only a few cell sites will be necessary, and each can serve a large geographical area. In areas with large numbers of active users, however, and particularly those who make heavy use of data services, a carrier will need to place far more cell sites, each serving a smaller geographic area, to compensate for the relatively larger usage burden placed on the local network.[30] Carriers that do not or cannot deploy more cell sites to cope with increased demand suffer from slow data speeds and frequent dropped calls.[31] As such, rural areas tend to have fewer cell sites, each with greater service areas, than urban areas, which generally have far more sites that are spaced closer together. Obviously, the proximity of one cell site to another in a geographic area is one factor in the production of more accurate location data.

---

strongest radio signal and perform a registration process identifying themselves, establishing that the user has a valid cell phone service, and identifying the local base station that is best equipped to process the call by virtue of the strength of its radio signal."); *see also id.* at 20 (written statement of Prof. Matt Blaze).

29. *Id. See generally* Nishith D. Tripathi, Jeffrey H. Reed & Hugh F. VanLandingham, *Handoff in Cellular Systems*, IEEE PERS. COMM., Dec. 1998, at 26, *available at* http://www.scss.tcd.ie/Hitesh.Tewari/papers/tripathi98.pdf.

30. *Location Hearing*, *supra* note 19, at 15 (testimony of Prof. Matt Blaze) ("[T]oday the limiting factor in how far apart [cell sites] can be is the number of customers they have to serve. And as this technology has exploded, the number of customers in any given area has gone explosively up, particularly in urban and densely populated areas.").

31. For example, one carrier has a reputation for dropped calls in some urban areas like San Francisco, due to the presence of large numbers of tech-savvy users with data-hungry iPhones, combined with the three-year waiting time required by the local authorities to get permission to erect new cell towers (which is often combined with further local obstructionism, whether motivated by opportunistic financial holdups or by NIMBY reactions to cell tower construction from individuals and communities with valuable real estate holdings). *See* Edward Wyatt, *AT&T and T-Mobile Chiefs Field Skeptical Questions on Capitol Hill*, N.Y. TIMES (May 11, 2011), http://www.nytimes.com/2011/05/12/technology/12phone.html ("T-Mobile ads made merciless fun of AT&T's reputation for dropped calls and sluggish wireless data connections"); MG Siegler, *Steve Jobs Continues To Answer the Questions That AT&T Won't*, TECHCRUNCH (July 18, 2010), http://techcrunch.com/2010/07/18/steve-jobs-att-2/ ("[Apple CEO Steve Jobs] said that it takes [AT&T] three years to get approval for a new cell tower in San Francisco. Yes, three years. '*That's the single biggest problem they're having*,' Jobs said. . . . Jobs also noted at the press conference that it takes '*about three weeks*' to add a new cell tower in Texas.").

B. CELL SITE DATA

Wireless service providers retain detailed logs for diagnostic, billing, and other purposes. These logs reveal the calls and Internet connections made and received by wireless subscribers, as well as detailed technical information regarding the cell sites that were used.[32] Such logs generally only reveal which particular cell site a phone was near at the time of the call.

Data from multiple towers can be combined to pinpoint (or "triangulate") a phone's latitude and longitude with a high degree of accuracy (typically under fifty meters).[33] This triangulated cell site data is generally only available prospectively, either due to a 911 call by a subscriber, or because a law enforcement agency has asked a carrier to collect it. Some carriers do routinely track and record triangulated data, and movement toward this practice is a general trend in the industry, although it is not yet the dominant practice, much less the common policy of all companies.[34] As such, law enforcement agencies can also obtain high-accuracy, triangulated historical data when it is available due to a specific company's data collection practices.

C. GLOBAL POSITIONING SYSTEM ("GPS")

Many mobile phones now include special hardware that enables the device to receive signals from a constellation of global position satellites.[35] Software on the phone can use these signals to calculate latitude and longitude,

---

32. McCullagh, *supra* note 2 ("Cellular providers tend not to retain moment-by-moment logs of when each mobile device contacts the tower, in part because there's no business reason to store the data, and in part because the storage costs would be prohibitive. They do, however, keep records of what tower is in use when a call is initiated or answered . . . ."); *see also* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, DEP'T OF JUSTICE, RETENTION PERIODS OF MAJOR CELLULAR SERVICE PROVIDERS (2010), *available at* http://www.wired.com/images_blogs/threatlevel/2011/09/retentionpolicy.pdf (listing, in chart form, data retention periods by the major cellphone carriers).

33. This requires the placement of special radio equipment at each cell site. *See generally Location Hearing*, *supra* note 19, at 38–41 (statement of Michael Amarosa, Sr. Vice President for Public Affairs, TruePosition Inc.).

34. *Location Hearing*, *supra* note 19, at 26–27 (written statement of Prof. Matt Blaze) ("(Whether locations are routinely tracked and recorded at times other than when calls are made or received depends on the policy of the particular carrier.) . . . Some carriers also store frequently updated, highly precise, location information not just when calls are made or received, but about every device as it moves about the networks. Maintaining such detailed records about the locations of phones as they move from place to place makes good engineering sense, and we should expect this trend to continue as part of the natural progression of technology.").

35. This communication is one-way. Phones receive signals from the satellites but do not transmit anything back to them.

often with a high degree of accuracy (less than twenty-five meters).[36] Although GPS is often more accurate than any other location technology, there are a few limitations: GPS signals are weak, high-frequency signals that do not penetrate walls, and as a result GPS often does not work when indoors. Moreover, for the same reason, GPS often does not function well in "urban canyons" due to signal deflection off of the sides of tall buildings. Furthermore, the GPS functionality tends to use significant amounts of power, which can lead to shorter battery life.[37] When GPS functionality is available, wireless carriers can prospectively obtain a device's location, such as when the user dials 911, or when asked to do so by law enforcement agencies. Carriers do not generally have historical GPS data to deliver.

Many smartphones now provide access to the GPS functionality to third-party "apps" installed on the devices. As such, app developers and location service providers also have access to users' GPS location data, often far more than the wireless carriers, although this is usually with the user's knowledge and consent.[38] Law enforcement agencies can compel these location service providers to disclose the historical GPS data in their possession, although prospective disclosures are limited to user-initiated "check-ins," as these companies are usually not able to generate their own GPS queries.

D. WiFi

Many smartphones include wireless internet ("WiFi") functionality, enabling device owners to browse the web at much faster speeds (and without impacting their carrier-imposed data cap) when at home, work, or in many public places. In addition to providing a connection to the Internet, the WiFi connections can also be used to determine the approximate location of the device.

---

36. *Location Hearing*, *supra* note 19, at 55 (attachment to written statement of Michael Amarosa).

37. Letter from Andy Lees, President, Mobile Commc'ns Bus., Microsoft Corp., to Rep. Fred Upton et al. (May 9, 2011), *available at* http://blogs.technet.com/cfs-file.ashx/__key/communityserver-blogs-components-weblogfiles/00-00-00-82-95/2451.Consumer-Privacy-_2600_-Windows-Phone-7-_2D00_Submission-to-House-Energy-and-Commerce-Committee-_2D00_-5.9.2011.pdf ("Windows Phone 7 generally relies upon WiFi access point or cell tower information to determine a phone's approximate location because GPS location data is not always available, and when it is, it can draw more heavily on battery power . . . .").

38. If a user "checks in" with a location provider like Foursquare, that location provider will learn their location, but the wireless carrier will not, as the information is sent directly to the location provider.

Several companies have created databases listing wireless networks and their approximate geographic location.[39] Initially, these databases were populated with data obtained by driving through the streets of cities around the world, collecting the data with a laptop or other special hardware.[40] In recent years, however, Google, Apple, and Microsoft have all enlisted the "crowdsourced" assistance of millions of smartphones to collect this data for them.[41]

By determining the available WiFi networks and submitting this list to one of the database providers, applications on the device and the platform mobile vendor (e.g., Google, Apple) can quickly determine the user's approximate location without using GPS, which would consume significantly more battery power.[42] Location data is increasingly valuable, enough so that the major platform vendors have been "willing to push the envelope on privacy to collect it."[43] Not only is location data used for maps and

39. *See* Greg Stirling, *Google Ends Street View WiFi Data Collection, May Now Need Other Sources for Location*, SEARCH ENGINE LAND (Oct. 20, 2010), http://searchengineland.com/google-ends-street-view-wifi-data-collection-potentially-needs-other-sources-for-location-53373 ("One of the purposes of collecting WiFi locations is to enable Google to identify user location (on handsets, laptops and PCs to some degree) through triangulation using a database of hotspots."); *see also Frequently Asked Questions*, SKYHOOK WIRELESS, http://www.skyhookwireless.com/howitworks/faq.php (last visited Mar. 17, 2012) ("Skyhook deploys vehicle-based signal scanning and data collection technologies, a common practice in the digital mapping and data collection industries. These Skyhook-equipped vehicles conduct systematic and comprehensive signal surveys by traveling every public road and highway in targeted coverage areas. These signal surveys capture the data output of individual access points and pair them with a date, time, and location stamp at the point where they are received by the data collection device.").

40. *See* Brad Stone, *Google Says It Collected Private Data by Mistake*, N.Y. TIMES (May 14, 2010), http://www.nytimes.com/2010/05/15/business/15google.html ("[B]ecause of a programming error in 2006, the company had . . . been mistakenly collecting snippets of data that happened to be transmitted over non-password protected wi-fi networks that the Google camera cars were passing."); *see also* Jenna Wortham, *Cellphone Locator System Needs No Satellite*, N.Y. TIMES (May 31, 2009), *available at* http://www.nytimes.com/2009/06/01/technology/start-ups/01locate.html (explaining how the company Skyhook "uses the chaotic patchwork of the world's wi-fi networks, as well as cell towers, as the basis for a location lookup service").

41. Julia Angwin & Jennifer Valentino-Devries, *Apple, Google Collect User Data*, WALL ST. J. (Apr. 22, 2011), http://on.wsj.com/zp2Euo ("Apple Inc.'s iPhones and Google Inc.'s Android smartphones regularly transmit their locations back to Apple and Google, respectively . . . as part of their race to build massive databases capable of pinpointing people's locations via their cell phones.").

42. *See generally* John Morris, *Apple Trades Privacy for Battery Life, Instead of Protecting Both*, CENTER FOR DEMOCRACY & TECH. (Apr. 22, 2011), https://www.cdt.org/blogs/john-morris/apple-trades-privacy-battery-life-instead-protecting-both.

43. Miguel Helft, *Apple and Google Use Phone Data To Map the World*, N.Y. TIMES (Apr. 25, 2011), https://www.nytimes.com/2011/04/26/technology/26locate.html.

navigation services on mobile devices, but it is also used to customize advertising aimed at people in a particular place. Such ads are far more lucrative than other ads and are becoming a major portion of the mobile advertising market, which industry experts estimate will be a $2.5 billion market by 2015.[44] Not only do these economic factors encourage companies to collect more location data, but they also encourage the collection of data with greater accuracy, allowing merchants to pitch advertisements to consumers walking past their store, rather than just those in the neighborhood.

E. PINGS

Most of the location information described in this Part is collected in the process of providing wireless voice and data services, or due to users calling 911 or using a location-enabled app on their smartphones. For such information, law enforcement agencies can either request historical data already stored by the provider, or request prospective surveillance that will provide data to the law enforcement agency as soon as the carrier receives it. In either case, the information collection is passive, in that no new data is generated due to the law enforcement surveillance request.

It is also possible, however, for carriers to monitor their customers actively, generating new data specifically in response to a request from law enforcement agencies. In such scenarios, the wireless carriers can covertly "ping" a subscriber's phone in order to locate them when a call is not being made. Such pings can merely reveal the nearest cell site to the subscriber,[45] or more accurate GPS or triangulated data if requested.[46] In addition to the

---

44. *Id.*

45. *See* Stone v. State, 941 A.2d 1238, 1244 (Md. Ct. Spec. App. 2008) ("Trooper Bachtell obtained the appellant's cell phone number and contacted his cell phone service provider. At Trooper Bachtell's request, the service provider conducted a 'ping' of the appellant's cell phone, which revealed that the phone was 'within a two mile radius of the Frederick County Detention Center.' ").

46. *See* Comments of CTIA—The Wireless Association on U.S. Department of Justice Petition for Expedited Rulemaking at 17, *In re* Petition for Expedited Rulemaking To Establish Technical Requirements and Standards Pursuant to Section 107(b) of the Communications Assistance for Law Enforcemenet Act, Docket No. RM-11376 (Fed. Commc'ns Comm'n July 25, 2007), *available at* http://fjallfoss.fcc.gov/ecfs/comment/viewid=5514711157 ("Law enforcement routinely now requests carriers to continuously 'ping' wireless devices of suspects to locate them when a call is not being made . . . so law enforcement can triangulate the precise location of a device and [seek] the location of all associates communicating with a target."); *see also* Devega v. State, 689 S.E.2d 293, 299 (Ga. 2010) ("[T]he investigators requested that Devega's cell phone provider 'ping' his phone, which the officers described as sending a signal to the phone to locate it by its global positioning system (GPS). The company complied and informed the police that the phone was moving north on Cobb Parkway.").

carrier-initiated pings, law enforcement agencies have also performed "low tech" pings by calling a target and hanging up before the phone rang, in order to generate cell site data that could then be requested from the carriers.[47]

F. TRENDS

The increasing accuracy and use of location data is motivated by the proliferation and advancement of mobile technology, as well as the lucrative commercial market for location-based services and marketing. Within that general context, there are several trends worth noting that suggest that single cell site data will become increasingly accurate. This postulation is particularly significant for evaluating current DOJ policies governing the legal standards for law enforcement's compelled disclosures of prospective location information.[48]

First, in an attempt to "fill the gaps" in their coverage, wireless carriers have, in the past few years, distributed hundreds of thousands of "microcells," "picocells," and "femtocells" to customers, which connect to the user's broadband internet connection and provide cellular connectivity to phones within tens or hundreds of meters. Industry estimates indicate that there are already more than 350,000 femtocells deployed in the United States, as compared to the more than 250,000 traditional carrier cell sites.[49] As these devices often broadcast a signal no further than a subscriber's home, the accuracy of single cell site location data can in some cases be more accurate than GPS, depending on whether the target is connected to a traditional cell site, or a residential femtocell.

Second, the success of Apple's iPhone and other smartphones has led to a massive increase in the use of data by mobile users. For example, AT&T has seen an 8,000 percent increase in data traffic between 2007 and 2010.[50] In response to this increased demand on their networks, carriers are deploying new cell sites and reducing the coverage area of existing towers.[51] As carriers

47. United States v. Forest, 355 F.3d 942, 947 (6th Cir. 2004) ("In order to reestablish visual contact, a DEA agent dialed Garner's cellular phone (without allowing it to ring) several times that day and used Sprint's computer data to determine which cellular transmission towers were being 'hit' by Garner's phone. This 'cell site data' revealed the general location of Garner.").

48. *See infra* Section III.A.1.

49. Press Release, Informa Telecoms & Media, *supra* note 27.

50. Dan Meyer, *AT&T Filing Provides Interesting Industry Data*, RCR WIRELESS (Apr. 25, 2011), http://www.rcrwireless.com/article/20110425/CARRIERS/110429949/att-filing-provides-interesting-industry-data.

51. Tracy Ford, *Tower Industry Primed for Growth with Carrier Buildouts*, RCR WIRELESS NEWS (Mar. 3, 2010), http://www.rcrwireless.com/ARTICLE/20100303/INFRASTRUCTURE/100309979/tower-industry-primed-for-growth-with-carrier-buildouts ("LTE

embrace faster 4G mobile data technologies, they will need even more cell sites, further reducing the coverage area around each tower.

As the coverage area around each traditional cell tower shrinks, and consumers increasingly embrace femtocells in their homes and businesses, single cell site data will become far more accurate—in some cases as good as GPS, and in others pinpointing someone's location to an area the size of a few blocks.

III. THE LAW

This Article proposes a policy framework that balances the interests of stakeholders affected by law enforcement access standards for provider-held location information. Before turning to policy proposals, the Article first discusses how law enforcement currently justifies its collection of prospective and historical location data—both under the DOJ's current interpretation of the law and the suggested policy guidance it gives to prosecutors and agents in the field.

This Part describes how the DOJ's and courts' various statutory interpretations have created a set of conflicting standards for law enforcement access to location data. Changes in technology, combined with the instability in the law created by conflicting legal standards for location data, create a critical need for Congress to amend the law to produce a better balance among privacy, law enforcement, and industry equities—a balance that would ideally benefit all stakeholders in some appreciable way. As such, this Part seeks to identify where that balance, as a matter of policy, may lie and how new law enforcement access standards or other "downstream" privacy protections might serve that legislative end. This Part therefore focuses on the policy implications of the current law, not on how the Fourth Amendment might apply to law enforcement access to location data held by a third party. When and under what circumstances the Fourth Amendment might require law enforcement to obtain a warrant to obtain location information from third-party providers remains a contested area of the law[52] and one that is

is going to be driving revenue for the tower companies . . . as a result of the incredible demand supported by LTE 700 MHz spectrum and the resulting splitting and additional coverage and capacity that the carriers are going to have to put in place to meet that demand.").

52. *Compare* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 677, 717 (2011) (arguing that courts should require a warrant for access to location data in all cases because such acquisition is a search under the Fourth Amendment), *with* Orin S. Kerr, *Court Rules That Police Cannot Use Warrants To Obtain Cell Phone Location of Person Who Is Subject of Arrest Warrant*, VOLOKH CONSPIRACY (Aug. 8, 2011), http://volokh.com/2011/08/08/court-rules-that-police-cannot-use-warrants-to-obtain-cell-phone-location-of-person-who-is-subject-of-arrest-warrant/ (arguing that location

beyond the scope of this Article to reconcile. To the extent that the discussion touches upon Fourth Amendment issues, it does so in the service of describing and developing a policy discussion, not to offer an opinion on the correct application of the Fourth Amendment to location information.

A. LEGAL BACKGROUND FOR REAL-TIME OR "PROSPECTIVE" CELL SITE DATA

Locating the proper law enforcement access standard for prospective location data in the current law is, in some respects, like the quest for the Holy Grail, the search for the fountain of youth, or the hunt for a truly comfortable pair of high heels—one is unlikely to find them. This legal mystery remains unsolved primarily for two reasons. First, the ECPA[53]—the primary law governing law enforcement access to wire, oral, and electronic communications and other stored subscriber records and information—does not contain the word "location" in any part of the statute or otherwise provide language that could be easily interpreted to cover law enforcement access to real-time location data from third-party providers.[54] Second, Congress, in a different statute, has only expressed what is *insufficient* for purposes of law enforcement access to prospective location information from a third-party provider, but not what is either *necessary* or *sufficient* for such compelled disclosures. Indeed, the Communications Assistance for Law Enforcement Act ("CALEA") merely instructs that "any information that may disclose the physical location of [a telephone service] subscriber" may

information of phones is not protected by the Fourth Amendment under *Smith v. Maryland*, 442 U.S. 735 (1979)).

53. *See supra* note 17.

54. Consider, for example, the testimony of Judge Smith describing the difficulty he and other Magistrate Judges have faced in determining the proper law enforcement access standard for real-time location information:

> Moreover, none of the other categories of electronic surveillance seemed to fit. The pen register standard was ruled out by a proviso in a 1994 statute known as CALEA. The wiretap standard did not apply because CSI does not reveal the contents of a communication. The Stored Communications Act (SCA) standard did not seem to apply for two reasons: the definition of "electronic communication" specifically excludes information from a tracking device; and the structure of the SCA was inherently retrospective, allowing access to documents and records already created, as opposed to prospective real time monitoring.

Location Hearing, *supra* note 19, at 82–83 (footnotes omitted); *see also* Kevin S. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. REV. 589, 606–09 (2007) (analyzing how the Wiretap Act and Pen/Trap statute do not provide the requisite authority for such "tracking" and the SCA only authorizes retrospective access to previously stored communications content and non-content information).

not be acquired "solely pursuant to the authority for pen registers and trap and trace devices."[55] Therefore, with respect to a compelled disclosure, if real-time location data cannot be provided to law enforcement "*solely pursuant*" to a court order for a Pen/Trap device, there must be some further requirement. But that requirement, unfortunately, remains undefined in the law. This exercise in *Via Negativa*[56] makes for great scholastic discussions about the incomprehensible character of an ineffable God but it is not very effective as a descriptive tool for discerning a legal standard. At best, it is a rather ineffective inversion of Justice Stewart's famous concurrence in *Jacobellis v. Ohio* about the similar difficulty the Court encountered in defining "hard core pornography" with any accuracy: "I know it when I [don't] see it."[57] Stated more precisely, if less concisely and memorably, "I'll know it when I can infer its existence and nature by seeing everything that it is not."

1. The DOJ's Interpretation of the Standard for Obtaining Prospective Cell Site Data

Lacking clear, affirmative statutory guidance, the DOJ has routinely acquired, since at least 2005, certain categories of "less precise" prospective cell site information through the *combination*[58] of two court orders: (1) a Pen/Trap court order pursuant to 18 U.S.C. § 3123,[59] and (2) a "D" Order pursuant to 18 U.S.C. § 2703(d), a section of the Stored Communications Act ("SCA") that permits the government to compel the production of non-

55. 47 U.S.C. § 1002(a)(2) (2010).

56. The "Via Negativa" is a method of philosophical and theological argument often associated with mysticism, sometimes referred to as "negative" or "apophatic" theology that attempts to describe God or the divine good by negation, specifically in terms of what God is *not* (*apophasis*), discerning instead only what may not be said accurately concerning the goodness and perfection(s) of God, which are beyond direct expression. The technique has its roots in several Greek philosophical schools, as well as several Western and Eastern religious traditions. *See Negative Theology*, THE BLACKWELL DICTIONARY OF WESTERN PHILOSOPHY 465–66 (Nicholas Bunnin & Jiyuan Yu eds., 2004); *see also* KAREN ARMSTRONG, THE CASE FOR GOD 317 (2009) (describing the potential resurgence of apophatic argument in postmodern theology).

57. Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

58. *See* Bankston, *supra* note 54, at 609–12 (describing the first publically known case where the DOJ articulated the "hybrid theory" in applying for a court order authorizing access to real-time cell site information).

59. 18 U.S.C. § 3123(a)(1) (directing that a court "shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device . . . if the court finds that the attorney for the Government [in an application pursuant to 18 U.S.C. § 3122(a)(1)] has certified to the court that the information likely to be obtained . . . is relevant to an ongoing criminal investigation").

content records or information pertaining to a subscriber or customer.[60] When combined, these two orders are known as a "hybrid order."[61] A DOJ manual documents that the rationale behind the DOJ's "hybrid" use of these two statutes derives from a combination of discrete statutory requisites.[62] First, because "cell-site data is 'dialing, routing, addressing or signaling information,' . . . 18 U.S.C. § 3121(a) requires the government to obtain a Pen/Trap order to acquire this type of information."[63] Second, however, because CALEA "precludes the government from relying 'solely' on the authority of the Pen/Trap statute to obtain cell-site data for a cell phone . . . some additional authority is required to obtain prospective cell-site information."[64] The DOJ asserts that "[s]ection 2703(d) provides this authority because . . . it authorizes the government to use a court order to obtain all non-content information pertaining to a customer or subscriber of an electronic communications service [or a remote computing service]."[65]

The same DOJ manual, published in its third edition in 2009, also provides guidance about the "precision" of the information likely to be obtained from cell site data (exclusive of GPS location technologies). The manual instructs that "[c]ell-site data identifies the antenna tower and, in some cases, the 120-degree face of the tower to which a cell phone is connected, both at the beginning and the end of each call made or received by a cell phone."[66] The manual further explains that "[t]he towers can be up to 10 or more miles apart in rural areas and may be up to a half-mile or more

60. *See id.* § 2703(c) (authorizing law enforcement to compel "a provider of electronic communications service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the government entity . . . obtains a court order for disclosure under subsection (d) of this section . . .").

61. U.S. DEP'T OF JUSTICE (DOJ), SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 160 (3d ed. 2009) [hereinafter DOJ MANUAL], *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

62. *Id.* at 159–60. Some published decisions also indicate that DOJ prosecutors have, at times, offered the All Writs Act, ch. 646, § 1651, 62 Stat. 869, 944 (codified as amended at 28 U.S.C. § 1651 (2010)), as a "mechanism for the judiciary to give [the government] the investigative tools that Congress has not." *In re* Application of the U.S. for an Order Authorizing the Use of a Pen Register and a Trap and Trace Device (*In re E.D.N.Y. Application*), 396 F. Supp. 2d 294, 325 (E.D.N.Y 2005); *see also In re* Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register (*In re W.D.N.Y. Application*), 415 F. Supp. 2d 211, 219 (W.D.N.Y 2006). These courts did not endorse this theory.

63. DOJ MANUAL, *supra* note 61, at 159–60.

64. *Id.* at 160.

65. *Id.*

66. *Id.* at 159.

apart even in urban areas."[67] Relying on this description of cell tower technology, the manual concludes: "[A]t best, these data reveal the neighborhood in which a cell phone user is located at the time a call starts and at the time it terminates; it does not provide continuous tracking and is not a virtual map of a cell phone user's movements."[68]

This description of the relative precision of cell site data, even if it is intended only to apply to single cell tower data (i.e., no multi-tower, triangulation, or GPS location information), will soon be—if it is not already—outdated with the deployment of microcell, picocell, and femtocell technology that, in some cases, can be more accurate than GPS.[69] Indeed, in urban areas and other environments where microcell technology is present, a cell phone's location can be identified on an individual floor or room within a building.[70] Moreover, the precision of single cell tower data will only increase as providers deploy new cell sites to cope with the surge in mobile user data traffic.[71]

The DOJ manual further advises prosecutors that *in most districts* they may obtain prospective cell site information with the use of hybrid orders, but it also acknowledges that some magistrate judges require a "probable cause" showing before authorizing law enforcement access to any type of prospective cell site data.[72] This split among magistrate judges, characterized by one federal prosecutor as the "Santa Ana Judicial Revolt,"[73] is discussed next.

2. Judicial Resistance to the Government's Use of Hybrid Orders

A growing number of magistrate judges within and across various judicial districts have rejected the government's use of the hybrid theory to obtain any type of prospective cell site information.[74] Some courts have held that, as

67. *Id.* (citing *In re* Application of the United States of America for an Order for Disclosure of Telecomm. Records and Authorizing the Use of a Pen Register and Trap and Trace (*In re S.D.N.Y. Application*), 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005)).

68. *Id.*

69. *See Location Hearing*, *supra* note 19, at 25 (written statement of Prof. Matt Blaze, Univ. of Pa.).

70. *Id.*

71. *Id.*

72. DOJ MANUAL, *supra* note 61, at 159–60.

73. E-mail from Tracy Wilkison re: Changes to GPS / Cell Site for Investigations Form (July 28, 2008) (informing other prosecutors about changes in office procedures for obtaining GPS and cell site information), *in* U.S. Dep't of Justice, Response to Freedom of Information Act Request No. 07-4123 re: Mobile Phone Tracking 13 (Sept. 8, 2008), *available at* http://www.aclu.org/pdfs/freespeech/cellfoia_release_074123_20080911.pdf.

74. *Location Hearing*, *supra* note 19, at 81–85, 93–94 (testimony of Judge Stephen Wm. Smith, U.S. Magistrate Judge). FED. R. CRIM. P. 41(d)(1) directs that "after receiving an

a matter of statutory construction, the Pen/Trap order and the D Order cannot be used to obtain prospective cell site information, but that Rule 41 provides the necessary authority because "it governs any matter in which the government seeks judicial authorization to engage in certain investigative activities."[75] More specifically, some of these courts have found that compelled disclosure of prospective cell site data is more akin to a tracking device placed under a vehicle, as defined in 18 U.S.C. § 3117,[76] than to the combination of elements comprising the government's hybrid theory and, therefore, would prompt the prudent prosecutor to obtain a Rule 41 warrant.[77]

Even the magistrate and district judges that have accepted hybrid orders and issued published decisions on the question have restricted law enforcement access to limited cell site information "yielding only generalized location data."[78] Magistrate Judge Gorenstein from the Southern District of New York, in what may be the "most cogent expression"[79] by a court in accepting the government's hybrid theory, specifically noted:

> [The government's request pertained to cell site information] tied only to telephone calls actually made or received by the telephone user . . . [with] no data provided as to the location of the cell phone when no call is in progress. [And], at any given moment, data is provided only as to a single cell tower with which the cell phone is communicating. Thus, no data is provided that could be "triangulated" to permit the precise location of the cell phone user.[80]

---

affidavit or other information," a judge "must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device."

75. *In re E.D.N.Y. Application*, 396 F. Supp. 2d 294, 322 (E.D.N.Y 2005); *see also In re W.D.N.Y. Application*, 415 F. Supp. 2d 211, 219 (W.D.N.Y 2005) ("[T]he challenge here is to the *statutory* justification for . . . [the government's] application. . . . The Court does not agree with the government that it should impute to Congress the intent to 'converge' the provisions of the Pen Statute, the SCA, and CALEA to create a vehicle for disclosure of prospective cell information on a real time basis on less than probable cause.").

76. "As used in this section, the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b) (2010).

77. *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Authority (*In re 2005 S.D. Tex. Application*), 396 F. Supp. 2d 747, 753–64 (S.D. Tex. 2005); *In re E.D.N.Y. Application*, 396 F. Supp. 2d at 322.

78. *Location Hearing*, *supra* note 19, at 93–94 (Exhibit B to written statement of Judge Stephen Wm. Smith) (collecting Magistrate and District Court published decisions where courts have accepted hybrid orders for limited cell site data pertaining to single cell tower and call-related information).

79. *Id.* at 83.

80. *In re S.D.N.Y. Application*, 405 F. Supp. 2d 435, 437–48 (S.D.N.Y 2005). Judge Gorenstein notes differences between the instant case and three published decisions denying

Judge Gorenstein further explained that his analysis for the instant Order was based on the "technology that is available to the Government in the District," recognizing that, with respect to future cases, "[he could not] know how . . . technology may change."[81]

For Judge Gorenstein, then, the current capacity of the cell tower network in question (the court even looked at a map of the location of various cell towers in lower Manhattan—an area it described as "densely populated by cell towers")[82] was a factor in authorizing law enforcement access to the cell site data with a hybrid order.[83] If that network's capabilities were to change due to an evolution in technology that yielded more precise location information, the court might rule differently in future cases. Indeed, the court's order might be as ephemeral as the capacities of the specific network the opinion seeks to comprehend at a specific moment in time. Any upgrade to that network that would enhance the accuracy of its geolocation capabilities in the district, made any time after the signing of the opinion, tied as it is to the facts describing the network's capacities, could render that opinion legally moot.

3. Divergent Interpretations of the Standard for Requiring Disclosure of Prospective Cell Site Data Create Legal Uncertainty

When seeking to compel "more precise" prospective location data generated by GPS or similar technologies, the DOJ's policy is to obtain a warrant based on probable cause.[84] While privacy advocates might view this as a small concession by the government, it is at best a transient one, since a policy decision by the DOJ is by no means a permanent or legally binding

government access to cell site information with a hybrid order insofar as "[t]hese cases appear to involve requests for cell site information that go beyond both what has been sought in this case and what has actually been received by the Government pursuant to any cell site application in this District." *Id.* (citing *In re 2005 S.D. Tex. Application*, 396 F. Supp. 2d 747; *In re E.D.N.Y. Application*, 396 F. Supp. 2d 294; *In re* Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register and Caller Identification Sys. on Tel. Numbers |Sealed|, 402 F. Supp. 2d 597 (D. Md. 2005)).

81. *In re S.D.N.Y. Application*, 405 F. Supp. 2d at 450.

82. *Id.* at 437.

83. *See also In re* Application of U.S. for an Order, 411 F. Supp. 2d 678, 680–82 (W.D. La. 2006) (granting an application for cell site information consistent with Judge Gorenstein's reasoning and scope of production of cell site information, recognizing that Judge Gorenstein "limit[ed] his opinion to the particular application before him" and characterizing the single cell site technology of that time as "not permit[ting] detailed tracking of a cell phone user within any residence or building").

84. *Senate Judiciary 2011 ECPA Hearing*, *supra* note 7, at 7 (testimony of James A. Baker, Assoc. Deputy Attorney Gen., U.S. Dep't of Justice).

decision.[85] To the extent that this policy decision protects privacy, it can be so unstable as to be subject to changes in leadership at various levels, even within a single administration, whose individual decisions implement the enforcement and oversight of a particular policy across various field offices.[86]

More troubling from a systemic perspective, however, is the inconsistent legal landscape that conflicting magistrate and district court decisions create across the country, sometimes even within the same district.[87] The system neither serves law enforcement needs nor protects privacy interests when legal standards are so uncertain. Moreover, as Judge Gorenstein's opinion illustrates, such uncertainty is magnified into legal instability, potentially to the point of unreliability, when a court's analysis is so tied to the state of

85. A DOJ policy decision, such as a policy requiring a warrant for law enforcement to acquire GPS-generated location data, has no binding authority on state or local law enforcement practices, and state investigators do not always follow DOJ policies. For example, in *Devega v. State*, investigators, without a warrant, requested a defendant's cell phone provider to "ping" his phone, which involved sending a signal to locate it through GPS information. 689 S.E.2d 293, 299 (Ga. 2010).

86. Consider, for example, Magistrate Judge Feldman's exchange with an Assistant United States Attorney ("AUSA") at oral argument. *See In re W.D.N.Y. Application*, 415 F. Supp. 2d 211, 218 (W.D.N.Y. 2006). While the government was only seeking "general [prospective cell site] location information" in the instant case, the AUSA conceded that in previous "hybrid" applications, the government had sought "prospective cell site data that could be used by law enforcement to triangulate the location of a cell phone to a degree perhaps beyond 'general location information.' " *Id.* The court pressed government counsel regarding whether the position that a hybrid order was appropriate for anything other than "general location information" had been abandoned. The AUSA responded:

> Well there's a couple of practical things going on. One, we're before magistrate judges that are the gatekeepers—we're trying to convince them that the government isn't being some ruthless, overbearing entity—we're trying to be reasonable. So, therefore, if we can get the magistrate's ear and we don't have to fight this fight a zillion times, we'll back off. If you have this internal radar that's going "privacy interest, privacy interest", okay we'll back off. But is it possible the argument could be made that we could be here on another day having gotten to floor one and now we're trying to get to floor two? Yes. Has that been suggested by anyone? Absolutely not.

Id. at 218 n.5; *see also* Freiwald, *supra* note 52, at 717 (discussing one U.S. Attorney's Office's failure to comply with DOJ policy advising agents to establish probable cause when seeking location data indicating a target's latitude and longitude (using either GPS or similarly precise data)).

87. *See Location Hearing*, *supra* note 19, at 83–85, 93–94 (written statement of Judge Stephen Wm. Smith and Exhibit B thereto). *Compare In re* an Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., No. 06 CRIM. MISC. 01, 2006 WL 468300 (S.D.N.Y. 2006) (denying application for limited single tower data), *with In re S.D.N.Y. Application*, 405 F. Supp. 2d 435 (granting application for limited single tower data).

technology in a particular district at a particular moment in time that it hinges upon a court's own examination of a network map of cell towers in a particular district—which would now include microcells, picocells, and femtocells—combined with expert opinion on the accuracy of location data that network could produce.[88] The court analyzed and accepted the government's hybrid theory (while, at the same time, limiting its ruling to the state of the technology available to the government in the district at that time), but it declared the result "unsatisfying" given Congress's lack of clear guidance regarding the appropriate standard for law enforcement access to prospective cell site data.[89]

Even the DOJ has acknowledged the need for legislation to clarify the standard governing compelled disclosures of prospective cell site data. The DOJ, however, carefully limited its recommendation to "cell tower information associated with cell phone calls," which is perhaps the particular area where the DOJ seeks specifically to retain the more nimble and efficient investigative standard provided by the hybrid order,[90] as opposed to the higher probable cause standard.[91] In the DOJ's view, "[s]ome courts . . . have conflated cell site location information with more precise GPS (or similar) location information"[92] and, as previously noted, they are already advising prosecutors to seek probable cause warrants for "more precise" GPS location data.

With location information—including single cell tower data—becoming only more precise over time and courts continuing to search for an illusory "intended" congressional standard to govern law enforcement access to prospective location data, the search for clarity remains an uncertain one at best in the absence of congressional action.

B. LEGAL BACKGROUND FOR HISTORICAL CELL SITE DATA

If the uncertainty over what standard to apply to prospective location information has left courts without a strong sense of direction, that

88. *See In re W.D.N.Y. Application*, 415 F. Supp. 2d at 213 n.3 (reviewing a letter from Verizon's Court Order Compliance Manager "which states that the information sought will only 'identify the general area that the target mobile phone located at the time of a specific call' and that it 'cannot pinpoint the exact location of the mobile phone' ").

89. *In re S.D.N.Y. Application*, 405 F. Supp. 2d at 442.

90. *Senate Judiciary 2011 ECPA Hearing*, *supra* note 7, at 5 (testimony of James A. Baker).

91. Mr. Baker explains earlier in his congressional testimony that "if an amendment were unduly to restrict the ability of law enforcement to quickly and efficiently determine the *general location* of a terrorist, kidnapper, child predator, computer hacker, or other dangerous criminal, it would have a very real and very human cost." *Id.* at 6.

92. Mr. Baker's testimony does not cite to specific examples where the DOJ believes courts have conflated cell site information with more GPS location information. *See id.* at 7.

confusion is becoming even more pervasive with regard to historical cell site data. Lower courts are now beginning to split over the proper access standard to apply to it as well. In this context, as with prospective cell site location data, 18 U.S.C. § 2703(c) permits the government to compel "a provider of electronic communications service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the government entity . . . obtains a court order for disclosure under subsection (d) of this section."[93] Stated more simply, a D Order "compels [production of] all non-content records."[94]

1. The DOJ's Interpretation of the Standard for Obtaining Historical Cell Site Data

The DOJ takes the position that historical cell site information satisfies each of the three elements necessary to fall within the scope of 18 U.S.C. § 2703.[95] First, a cell phone company is a provider of "electronic communications service" to the public.[96] Second, "cell site information constitutes 'a record of other information pertaining to a subscriber or to a customer of such service (not including the contents of communications).' "[97] More specifically, historical cell site information "is a record stored by the provider concerning the particular cell tower used by a subscriber to make a particular cell phone call, and is therefore 'a record or

93. 18 U.S.C. § 2703(c) (2010).

94. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1222 (2004).

95. Brief for the United States at 8–9, *In re* the Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. To Disclose Records to the Gov't (*Appeal of In re W.D. Pa. Application*), 620 F.3d 304 (3d Cir. 2010) (No. 08-4227), 2009 WL 3866618.

96. *Id.* at 10. The Wiretap Act and SCA define electronic communication service ("ECS") to mean "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. §§ 2510(15), 2711(1). Cell phone service providers provide their customers with the ability to send "wire communications," and thus they are providers of electronic communications service. *See* § 2510(1), (15). Moreover, the DOJ takes the position that:

> [a] "wire communication" necessarily involves the human voice. *See* § 2510(1) (defining "wire communication") and § 2510 (defining "aural transfer"); S. Rep. No. 541, 99th Cong., 2d Sess. 11 (1986), *reprinted in* 1986 U.S. Code Cong. & Admin. News 3555, 3565 ("cellular communications—whether they are between two cellular telephones or between a cellular telephone and a 'land line' telephone—are included in the definition of 'wire communications' and are covered by the statute").

Brief for the United States, *supra* note 95, at 11 n.10.

97. Brief for the United States, *supra* note 95, at 11.

other information pertaining to a subscriber or customer.' "[98] Finally, "cell site information is non-content information, as it does not provide the content of any phone conversation the user has had over the cell phone."[99] Based on this analysis, prosecutors and agents regularly use D Orders to compel historical location information from third-party providers.

2. Judicial Interpretation of the Standard for Obtaining Historical Cell Site Data

Lower courts have, for the most part, accepted the government's use of a D Order to compel historical cell site information.[100] However, one circuit court has held that there may be circumstances in which a judge can require a probable cause showing before authorizing a government-compelled disclosure of historical cell site information.

a) The Third Circuit Finds That Magistrate Judges Have the Discretion To Require Probable Cause

A government appeal of a magistrate judge's opinion[101] denying the use of a D Order to compel historical cell site data led the Third Circuit to consider whether a D Order based on "specific and articulable facts" can be sufficient to allow the government to compel the production of historical cell site data and whether, in some cases, a court should apply the Fourth Amendment's probable cause requirement in place of the more relaxed provisions of the SCA governing the disclosure of historical cell site information.[102] The Third Circuit held that historical cell site data "is obtainable under a § 2703(d) order and that such an order does not require

98. *Id.* (citing *In re S.D.N.Y. Application*, 405 F. Supp. 2d 435, 444 (S.D.N.Y 2005), and noting that cell site data is "information" and " 'pertain[s]' to a subscriber or customer of cellular telephone service").

99. *Id.* (citing 18 U.S.C. § 2510(8) and defining the "contents" of communications to include information concerning its "substance, purport, or meaning").

100. *See In re* Applications of the U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d 76, 82 (D. Mass. 2007) (granting the government's application for historical cell site information based on the government's statutory analysis of 18 U.S.C. §§ 2703(c), (d)); *id.* at 79 n.5 (collecting cases where courts have assumed or applied in dicta that compelling disclosure of historical cell site data is proper under § 2703(d) of the SCA).

101. *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. To Disclose Records to the Gov't (*In re W.D. Pa. Application*), 534 F. Supp. 2d 585 (W.D. Pa. 2008). On appeal from the Magistrate Judge to the District Court, the court "recognized 'the important and complex matters presented in this case,' but affirmed in a two page order without analysis." *Appeal of In re W.D. Pa. Application*, 620 F.3d 304 (3d Cir. 2010) (citing *In re W.D. Pa. Application*, 534 F. Supp. 2d 585).

102. *Appeal of In re W.D. Pa. Application*, 620 F.3d 304.

the traditional probable cause determination."[103] The Third Circuit also found, however, that magistrate judges have the discretion to turn down a government application for a D Order even when the D Order standard has been satisfied and, instead, require a probable cause showing. This determination is based upon the Third Circuit's reading of D Order statutory language as "language of permission rather than mandate."[104] The extent to which a magistrate judge has discretion to deny a D Order is unclear, as the opinion merely instructs that the option to require a warrant "be used sparingly because Congress also included the option of a § 2703(d) order," that judges do not have "arbitrary" discretion, and in those cases where a magistrate judge does require a warrant, she must "make fact findings and give a full explanation that balances the government's need (not merely desire) for the information with the privacy interests of cell phone users."[105]

In his concurring opinion, Judge Tashima noted his agreement with most of the reasoning of the majority opinion, but he was concerned that "contradictory signals" leave magistrate judges and prosecutors with a lack of "standards by which to judge whether an application for a § 2703(d) order is or is not legally sufficient."[106] Judge Tashima explained that "the majority suggests that Congress did not intend to circumscribe a magistrate's discretion in determining whether or not to issue a court order, while at the same time, acknowledging that [o]rders of a magistrate judge must be supported by reasons that are consistent with the standard applicable under the statute[.]' "[107] Contrary to the majority's statement that "a magistrate judge does not have arbitrary discretion," Judge Tashima suggests that the majority's opinion perpetuates exactly that, because:

> it provides *no* standards for the approval or disapproval of an application for an order under § 2703(d) . . . [and it] vests magistrate judges with arbitrary and uncabined discretion to grant

103. *Id.* at 313.

104. *Id.* at 316 ("We begin with the text. Section 2703(d) states that a 'court order for disclosure under subsection (b) or (c) *may be* issued by any court that is a court of competent jurisdiction and *shall* issue *only if*' the intermediate standard is met. 18 U.S.C. § 2703(d) (emphasis added). We focus first on the language that an order 'may be issued' if the appropriate standard is met. This is the language of permission, rather than mandate. If Congress wished that courts 'shall,' rather than 'may,' issue § 2703(d) orders whenever the intermediate standard is met, Congress could easily have said so. At the very least, the use of 'may issue' strongly implies court discretion, an implication bolstered by the subsequent use of the phrase 'only if' in the same sentence.").

105. *Id.* at 316, 319.

106. *Id.* at 320 (Tashima, J., concurring).

107. *Id.*

> or deny issuance of § 2703(d) orders at the whim of the magistrate, even when the conditions of the statute are met.[108]

Indeed, the very instability that currently plagues the prospective cell site data legal landscape might also "fester" with respect to historical access standards if the Third Circuit's "rule," giving magistrate judges discretion to deny a D Order without standards or guidance about when such denial is appropriate, were to become the law of the land.[109]

In the wake of the Third Circuit's opinion, some magistrate judges who once granted access to historical cell site data with a D Order are now revisiting that practice. In Magistrate Judge Smith's recent opinion, however, the court placed more significance on "new technology" that has "altered the legal landscape even more profoundly than the new caselaw."[110] Judge Smith's opinion meticulously documents the changes in technology leading to his determination that "court decisions allowing the Government to compel cell site data without a probable cause warrant were based on yesteryear's assumption that cell site data (especially from a single tower) could locate users only imprecisely."[111] After establishing the state of current technology and its rapid pace of change in the direction of increased accuracy for the factual record, Judge Smith conducted a constitutional analysis and ultimately concluded that a compelled *warrantless* disclosure of sixty days of historical cell site data violates the Fourth Amendment.[112]

b) The D.C. Circuit's "Mosaic Theory"

Prior to Judge Smith's opinion, Magistrate Judge Orenstein, another judge who previously granted requests for historical cell site data pursuant to a D Order, also denied the government's application absent a warrant based

108. *Id.*

109. For a more extended analysis and critique of the Third Circuit opinion, see Orin S. Kerr, *Third Circuit Rules That Magistrate Judges Have Discretion To Reject Non-warrant Court Order Applications and Require Search Warrants To Obtain Historical Cell Site Records*, VOLOKH CONSPIRACY (Sept. 8, 2010), http://volokh.com/2010/09/08/third-circuit-rules-that-magistrate-judges-have-discretion-to-reject-court-order-application-and-require-search-warrants-to-obtain-historical-cell-site-records/.

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

111. *Id.* at 830.

112. The court's reasoning can be summarized as follows: (1) under current location technology, cell site information reveals non-public information about constitutionally protected spaces; (2) historical cell site records are subject to Fourth Amendment protection under the prolonged surveillance doctrine of *United States v. Maynard*, 615 F.2d 544 (D.C. Cir. 2010); and (3) the government has not demonstrated that the location data sought was voluntarily conveyed by the user and therefore *Smith v. Maryland*, 442 U.S. 735 (1979), does not eliminate a legitimate expectation of privacy.

on a probable cause showing.[113] In finding the government's D Order application for historical cell site data over a fifty-eight-day period to be an unreasonable search and seizure under the Fourth Amendment,[114] Judge Orenstein's opinion relies heavily on a recent D.C. Circuit Fourth Amendment decision, *United States v. Maynard*.[115] The court in *Maynard* considered whether the government's warrantless use of a GPS device placed on a vehicle to track a suspect's movements for twenty-eight days, twenty-four hours a day, was an unreasonable search under the Fourth Amendment. In concluding that the long-term GPS surveillance of movements exposed to public view was a search,[116] the *Maynard* court recognized a novel "mosaic theory" of the Fourth Amendment.[117] Specifically, the court explained:

> Prolonged surveillance reveals types of information not revealed by short term surveillance . . . [and] can reveal more about a person than does any individual trip viewed in isolation . . . . A person who knows all of another's travels can deduce 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.[118]

As Professor Orin S. Kerr observes, under the mosaic theory, a court determines whether government conduct is a search "not by whether a particular individual act is a search, but rather whether an entire course of conduct, viewed collectively, amounts to a search."[119] Individual acts that

113. *In re* Application of the U.S. for an Order Authorizing Release of Historical Cell-Site Info. (*In re 2010 E.D.N.Y. Application*), 736 F. Supp. 2d 578 (E.D.N.Y 2010). *But see In re* Application of the U.S. for an Order Authorizing Disclosure of Historical Cell Site Info. for Tel. No. [redacted], Misc. No. 11-449, at 5 (D.D.C. Oct. 3, 2011) (Lamberth, C.J.), *available at* http://legaltimes.typepad.com/files/lamberth_ruling.pdf (holding that a D Order permits the government to compel disclosure of historical location data without a probable cause search warrant and that *Maynard* does not control the question).

114. *In re 2010 E.D.N.Y. Application*, 736 F. Supp. 2d at 582.

115. United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *reh'g denied sub nom.* United States v. Jones, 625 F.3d 766 (D.C. Cir. 2010), *aff'd*, 132 S. Ct. 945 (2012).

116. In reaching its decision, the court explained how the reasoning of *Knotts* did not foreclose the conclusion that long-term surveillance constitutes a search. *Maynard*, 615 F.3d at 556–58. Indeed, the Court interpreted the *Knotts* opinion as reserving the question of whether *prolonged* use of a beeper device would require a warrant. *Id.* at 556. The court acknowledged, however, that appellate courts in three other circuits have reached opposite conclusions under *Knotts*. *Id.* at 557–58.

117. *Id.* at 562.

118. *Id.* (footnote omitted).

119. *See* Orin S. Kerr, *D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, VOLOKH CONSPIRACY (Aug. 6, 2010), http://

may not, in their own right, be searches can become searches when committed in particular combinations.[120] Thus in *Maynard*, the court does not look at individual data recordings from the GPS device to determine whether, for example, individual trips are searches.[121] Instead, "the Court examines the entirety of surveillance over a one-month period and views it as one single 'thing' " subject to Fourth Amendment analysis.[122] But at what point would a single act or a series of acts amount to the prolonged surveillance that triggers the mosaic theory and how does a prosecutor, judge, or defense attorney recognize the phenomenon? The *Maynard* court gives no real guidance in this regard.[123] Indeed, the Solicitor General in the government's brief filed in *Jones* (formerly *Maynard*)[124] has argued: "[T]he 'mosaic' theory is unworkable. Law enforcement officers could not predict when their observations of public movements would yield a larger pattern and convert legitimate short-term surveillance into a search. Courts would be hard pressed to pinpoint that moment even in retrospect."[125]

While acknowledging primary factual differences between the real-time GPS vehicle tracking in *Maynard* and the government's application for two months' worth of historical cell site data, Judge Orenstein finds the *Maynard* opinion "persuasive" support for his analysis that the Fourth Amendment

volokh.com/2010/08/06/d-c-circuit-introduces-mosaic-theory-of-fourth-amendment-holds-gps-monitoring-a-fourth-amendment-search/.

120. *Id.*

121. *Id.*

122. *Id.*

123. In *United States v. Cuevas-Perez*, 640 F.3d 272 (7th Cir. 2011), the Seventh Circuit considered whether *Maynard* applied to a 60-hour, "factually straightforward" warrantless GPS surveillance. *Id.* at 274. In determining that *Maynard* did not apply to the case, the majority opinion reasoned that *Maynard*'s 28-day surveillance was much lengthier than the 60-hour surveillance before the Seventh Circuit and the "single trip" in the instant case did not "expose or risk exposing" the "twists and turns" of the defendant's life, "including possible criminal activities, for a long period." *Id.* at 274. In concluding *Maynard* did not apply, however, the majority emphasized "the present case . . . is not meant to approve or disapprove the result the D.C. Circuit reached under the facts of that case." *Id.* at 274 n.3. The concurring and dissenting opinions in *Cuevas-Perez* do provide some analysis of *Maynard*. Indeed, the concurring opinion generally finds *Maynard's* mosaic theory "unworkable," with Judge Flaum indicating that it is not "obvious" to him where the *Maynard* Court would "draw constitutional lines around Cuevas-Perez's sixty-hour journey." *Id.* at 282. In contrast, Judge Wood's dissent rejects the majority's "single trip" description, finding much more similarity between Cuevas-Perez's "60 hour odyssey across 1,650 miles" and the prolonged surveillance in *Maynard*. *Id.* at 293.

124. *See supra* note 115.

125. Brief for the United States at 14, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259), 2011 WL 3561881. Indeed, Respondent Jones does not employ the *Maynard* "mosaic theory" in his brief to the Supreme Court. *See* Brief for Respondent Antoine Jones at 45, *Jones*, 132 S. Ct. 945 (2012) (No. 10-1259), 2011 WL 4479076.

requires the government to obtain a warrant to compel the location information.[126] Lower courts' reliance on *Maynard*'s "mosaic theory," however, raises questions, once again, about the viability of a series of cases that give prosecutors and judges little to no guidance about when and what amount of location data is subject to Fourth Amendment protection. Judge Orenstein, for example, found that fifty-eight days of historical cell site data required a warrant under the reasoning in *Maynard* but, in a later opinion applying *Maynard*, he granted an application for discreet amounts of data spanning a twenty-one-day period under a D Order.[127] While such opinions may be heralded as a "victory" for privacy interests because, among other things, they have the effect of destabilizing the government's use of the D Order, they serve neither privacy nor law enforcement interests insofar as they perpetuate a legal landscape in which lower courts continue to "search," in vain, for the appropriate standards to apply.

3. The Jones *Decision*

Notwithstanding such criticism of the mosaic theory in *Maynard*, the concurring opinions in *United States v. Jones*[128] suggest that, in some future case, there may be five votes for a mosaic-type Fourth Amendment theory holding that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[129] Indeed, Justice Alito's

126. *In re 2010 E.D.N.Y. Application*, 736 F. Supp. 2d 578, 584 (E.D.N.Y. 2010). This Article does not focus on appropriate standards for law enforcement use of GPS tracking devices installed on vehicles—which do not involve compelled disclosures from third-party ECPA-covered providers—and which, therefore, as a matter of policy, may implicate slightly different equities and interests for Congress to consider when drafting legislation.

127. *In re* Application of the U.S. for an Order Authorizing Release of Historical Cell-Site Info., No. 11-MC-0113, 2011 WL 679925 (E.D.N.Y. 2011). The government's application for historical cell site data sought information from one phone for a three-day period, a six-day period from the same phone commencing less than a month later, and a twelve-day period from a second phone believed to have been used in furtherance of the offenses under investigation. *Id.* at *1. The court distinguished the result of the instant case from that of *Maynard* primarily because the court could not "assume that the information gleaned over such shorter periods, separated by breaks of weeks or months, would necessarily be as revealing as the sustained month-long monitoring at issue in *Maynard*." *Id.* at *2. In making this distinction, however, the court acknowledged that "any such line drawing is, at least to some extent, arbitrary and the need for such arbitrariness arguably undermines the persuasiveness of *Maynard*, and of [this court's] prior decisions." *Id.* For further analysis and critique of this decision, see Orin S. Kerr, *Applying the Mosaic Theory of the Fourth Amendment to Disclosure of Stored Records*, VOLOKH CONSPIRACY (Apr. 5, 2011), http://volokh.com/2011/04/05/applying-the-mosaic-theory-of-the-fourth-amendment-to-disclosure-of-stored-records/.

128. 132 S. Ct. 945 (2012).

129. *Id.* at 964 (Alito, J., concurring). Justices Ginsburg, Breyer, and Kagan joined Justice Alito's concurrence. While Justice Sotomayor did not join the Alito concurrence, she states

concurrence invokes the novel aggregative Fourth Amendment theory first articulated by the D.C. Circuit in *Maynard*. The Alito concurrence posits that "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable" while law enforcement's "secretly monitor[ing] and catalogu[ing] every single movement of an individual's car for a very long period" does not accord with reasonable expectations of privacy.[130] Likewise, *Maynard* previously recognized that "[p]rolonged surveillance reveals types of information not revealed by short term surveillance."[131]

While Justice Alito's concurrence applies the *Katz*[132] "expectation-of privacy test," the majority opinion, authored by Justice Scalia, bases its holding partially on a trespass theory: "We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.' "[133] Justice Scalia defines the offending conduct further stating "the Government physically occupied private property for the purpose of obtaining information."[134] Consequently, though "[t]respass alone does not qualify [as a search]," a search does occur when it is "conjoined" with "an attempt to find something or to obtain information."[135]

Justice Alito criticizes this approach because, among other things, it "largely disregards what is really important (the *use* of a GPS for long-term tracking) and instead attaches great significance to something that most would view as relatively minor (attaching to the bottom of a car a small, light object that does not interfere in any way with the car's operation)."[136] Indeed, the attachment-focused majority opinion does not address instances where the use of GPS solely involves the transmission of radio or other electronic

in her own concurrence, "I agree with Justice ALITO that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.' " *Id.* at 955 (Sotomayor, J., concurring). *See also* Orin S. Kerr, *What's the Status of the Mosaic Theory After* Jones*?*, VOLOKH CONSPIRACY (Jan. 23, 2012), http://volokh.com/2012/01/23/whats-the-status-of-the-mosaic-theory-after-jones/ (explaining that the mosaic theory "lives").

130. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

131. United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *reh'g denied sub nom.* United States v. Jones, 625 F.3d 766 (D.C. Cir. 2010), *aff'd*, 132 S. Ct. 945 (2012).

132. Katz v. United States, 389 U.S. 347 (1967). "As Justice Harlan's oft-quoted concurrence described it, a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." Kyllo v. United States, 533 U.S. 27, 33 (2001) (citing *Katz*, 389 U.S. at 361).

133. *Jones*, 132 S. Ct. 945.

134. *Id.*

135. *Id.* at 951 n.5.

136. *Id.* at 961 (Alito, J., concurring).

signals not enabled by the government's direct physical trespass—such as tracking a target's cell phone.[137] While acknowledging that government tracking though electronic means without actual physical trespass may be "an unconstitutional invasion of privacy," the majority opinion asserts "the present case does not require us to answer that question."[138] Moreover, the majority opinion criticizes the line-drawing problems the Alito concurrence presents:

> [I]t remains unexplained why a 4-week investigation is "surely" too long and why a drug-trafficking conspiracy involving substantial amounts of cash and narcotics is not an "extraordinary offens[e]" which may permit longer observation. What of a 2-day monitoring of a suspected purveyor of stolen electronics? Or of a 6-month monitoring of a suspected terrorist?[139]

Indeed, consistent with the difficulties *Maynard* raised, Justice Alito's adoption of a mosaic-type theory provides no significant guidance to law enforcement, judges, and industry about when Fourth Amendment concerns materialize: "We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark."[140] Rather than creating clarity in the law, the Alito concurrence perpetuates, perhaps even intensifies, the confusion surrounding appropriate law enforcement standards for access to location data.

4. *The Importance of Legislative Clarity in the Face of Rapid Technological Change*

Scholars and advocates may legitimately disagree about Fourth Amendment theory and about courts' application of the Fourth Amendment to government-compelled disclosures of cell site data. Notwithstanding this constitutional debate, however, the current pace of technological change in this area has given rise to inordinately difficult analytical challenges and highlighted a consequent need for Congress to clarify or amend the law. Chief among these challenges is the current instability in the law created when courts must struggle to find congressional intent in laws that predate the current state of location technology—in short, to find intention in the absence of a stable object. In the face of this ultimately futile search for historical interpretive authority, courts must grapple directly with the legal

137. *Id.* at 953 ("Situations involving merely the transmission of electronic signals without trespass would *remain* subject to the *Katz* analysis.").

138. *Id.*

139. *Id.* (citation omitted).

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

implications that enormously complex and quickly evolving location technologies raise in conjunction with the facts of a given case. Finally, courts must try to perform the foregoing analysis while simultaneously confronting any implications the rapid rate of change in the capabilities of location technology might have upon the reasonable scope of their decisions. To avoid these difficult acts of legal navigation, policymakers should enact laws containing *clear* standards that strike the right balance among law enforcement needs and privacy and industry interests. These standards must also be flexible enough to accommodate the pace of technological change to a degree that renders it a moot consideration in any court's analysis.

C. QUESTIONS RAISED BY THE TWO EXISTING STANDARDS FOR COMPELLING DISCLOSURE OF LOCATION DATA

1. What Does a "D" Order Require the Government To Show?

The call by some advocates for a probable cause standard to govern all law enforcement compelled disclosures of location data is, of course, a recognition that the D Order affords a less stringent showing by law enforcement than that required to meet probable cause.[141] Specifically, to obtain a D Order, law enforcement must provide "specific and articulable facts that there are reasonable grounds to believe" that the information to be compelled "is relevant and material to an ongoing investigation."[142] Some scholars have referred to the D Order standard as a "*Terry*-stop" standard, a reference to *Terry v. Ohio*, where the Supreme Court created the reasonable suspicion standard for sidewalk stop-and-frisk encounters.[143] The *Terry* standard is met "when an officer 'point[s] to specific and articulable facts which, taken together with rational inferences from those facts, evince more

141. *See* H.R. REP. NO. 103-837, at 31 (1994) (indicating that the D Order is "an intermediate standard . . . higher than a subpoena, but not a probable cause warrant").

142. 18 U.S.C. § 2703(d) (2010).

143. 392 U.S. 1, 30 (1968); *see also* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 175–76 (2007) (arguing that the D Order standard, although perhaps intended to be more demanding than the relevance standard required for a subpoena, may not be much different: "[e]ven if *material* is meant to augment *relevant*, it does not add much; materiality, in evidence law, means merely that the evidence be logically related to a proposition in the case"); Freiwald, *supra* note 52, at 692 (discussing that the D Order standard permits much broader inquiries into a much wider range of targets than the probable cause standard); Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards*, 54 MINN. L. REV. 1514, 1521–22 (2010) (noting that the D Order standard "is probably much more stringent than the mere-relevance subpoena standard" and is set by Congress "at a high enough level to prevent police fishing expeditions").

than an inchoate and unparticularized suspicion or hunch of criminal activity.' "[144]

From a practical standpoint, the D Order standard facilitates law enforcement access to non-content records at the early stages of an investigation, when the government is unlikely to meet the higher probable cause standard. In a recent case not involving location information, the DOJ asserted that the D Order standard "derives from the Supreme Court's decision in *Terry*" and thus "is no more onerous than the *Terry* rule."[145] As such, the word "material" in 18 U.S.C. § 2703(d) "does not transform the § 2703(d) standard into one that requires a showing that the records sought are 'vital,' 'highly relevant,' or 'essential.' "[146] Indeed, the scope of a D Order may be "appropriate even if it compels disclosure of some unhelpful information," as " '§ 2703(d) is routinely used to compel disclosure of records, only some of which are later determined to be essential to the government's case.' "[147] For example, if investigators compel location information for every cell phone in the vicinity of a murder scene for a specific period of time, they are likely to obtain *irrelevant* location information about innocent people who just happened to be in a particular place at a particular time in addition to information about the presence of the murderer or witnesses who might have seen the murderer.

Broadening the scope of a request for location information beyond, but in relation to, a known target can advance an investigation strategically. Law enforcement, in certain circumstances, might request the location information of all individuals who were called by or made calls to a particular target.[148] This practice, sometimes referred to as a "community of interest" request, is of particular concern to privacy advocates,[149] but it can, for

144. United States v. Mason, 628 F.3d 123, 128 (4th Cir. 2010) (quoting United States v. Branch, 537 F.3d 328, 336 (4th Cir. 2008)).

145. Government's Response to Objections of Three Twitter Subscribers to Magistrate Judge's March 11, 2011 Opinion Denying Motion To Vacate and Denying in Part Motion To Unseal at 8–9, *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 2011 WL 5508991 (E.D. Va. 2011) (Misc. Nos. 1:11-DM-3, 10-GJ-3793 & 1:11-EC-3), *available at* http://files.cloudprivacy.net/goverment_opp.pdf.

146. *Id.* at 8–9 (quoting Subscribers' Objections).

147. *Id.* at 8 (quoting Magistrate Judge Buchanan's Opinion and Order of March 11, 2011).

148. *See House Judiciary 2010 ECPA Reform Hearing*, *supra* note 18, at 29–30 (written statement of Albert Gidari, Perkins Coie LLP) (explaining that with respect to location information of specific users, many orders now require disclosure of the location of all of the associates who were called by or made calls to a target).

149. Some privacy scholars express strong concerns with a standard that "allows the government to seek location information about apparently innocent parties regularly," noting that community of interest requests provide law enforcement with information about

example, enable law enforcement to identify unknown suspects potentially involved in criminal activity with a known target.[150]

Law enforcement often needs the ability to cast a wider investigative net at early stages of an investigation and, assuming the government's interpretation is correct, the D Order standard facilitates this "over-collection" of information. But insofar as the D Order standard does facilitate an often *necessary* over-collection of information, to what extent does it adequately prevent *unnecessary* over-collection of information? In other words, should not the D Order standard explicitly require that a sufficient nexus exist between the scope of the location information requested and the criminal activity being investigated?

If so, how should this nexus standard be examined by courts? Determining whether an application reflects a time period tailored to the criminal activity being investigated is one inquiry for courts to make in an effort to legitimately cabin the amount of information collected. A single

individuals only tenuously connected to a crime without the judicial oversight that a warrant guarantees. *See* Freiwald, *supra* note 52, at 718.

150. Consider the following scenario: British authorities at an airport package transit x-ray station in Coventry, England x-rayed a package and discovered a .375 Magnum revolver hidden inside a child's toy boat. More packages containing weapons and ammunition concealed inside children's toys were also discovered. When the revolver from the first package was removed, agents noticed that the gun's serial number had been filed down, but forensic analysis reconstructed the number, allowing law enforcement to trace the gun back to a dealer with a known identity and a *female* gun purchaser with a known identity in South Florida. The packages had also been mailed from South Florida via express mail, which allowed agents to identify the location, time, and date that the package was mailed. Cameras inside those post offices recorded video showing two men mailing the first package containing the .357 Magnum revolver. No further information identifying those men was known at the time. It is reasonable to assume that the woman who purchased the revolver (whose identity law enforcement had confirmed) called or was called by the men who mailed the package. One way to assist law enforcement in identifying the men (who continued to mail packages ultimately discovered at Coventry airport) would be to obtain location information focused on the individuals in contact with the known female gun purchaser.

This factual scenario is taken from a real case, *United States v. Claxton*, No. 99-06176 (S.D. Fla. June 13, 2000) (Ferguson, J.), prosecuted by Stephanie in 1999–2000 involving a cell of IRA operatives who came to the United States, purchased weapons illegally, hid them in children's toys and large, hollowed-out computer towers, and mailed them to the Republic of Ireland where they would be smuggled into Belfast. This operation was occurring during a critical time in the peace process and the weapons were intended to replace the cache of weapons being turned over as part of the Good Friday Agreements. The factual narrative described is condensed to illustrate how a "community of interest" request would have assisted in identifying the identities of the men mailing the packages, had such a practice been in use at that time. For more information about the case, see Mike Clary, *Lax Florida Laws Attracted IRA*, REGISTER-GUARD (Eugene, Or.), June 8, 2000, at 6A, *available at* http://goo.gl/S6BgC.

bank robbery occurring over the course of an hour committed by a few suspects, for example, would likely require a narrower collection of information than a sophisticated drug conspiracy covering multiple jurisdictions with multiple conspirators occupying different roles and performing different tasks. Not only would the length of time reflected in the bank robbery D Order application likely be shorter than in the drug conspiracy application, but the number of individuals targeted (known and unknown) might also be fewer. In certain types of investigations, identities of targets are not initially known, but locations where crimes or activities relevant to determining the identities of suspects are known. When the request for the location data is centered on a place where an activity occurred, courts can ensure that the length of the request (i.e., from "Time *X*" to "Time *Y*") is sufficiently tailored to when the investigation suggests that the suspects were present at the location. Similarly, when community of interest requests are made, courts could ensure that the breadth of location information requested about individuals who called or were called by a target is reasonable in light of investigative facts described in the application. There are, of course, many permutations of how the scope of a request for location data would manifest in a particular investigation. Considering that D Orders necessarily facilitate an over-collection of information, however, Congress could amend the language of § 2703(d) to ensure that courts are examining whether a sufficient nexus exists between the scope of the location information requested and the criminal activity being investigated.

2. Probable Cause of What?

A strict probable cause standard for the disclosure of location information could interfere with legitimate law enforcement objectives. Some of the privacy concerns motivating the advocacy for the application of a probable cause standard to all law enforcement compelled disclosures of any and all location information are discussed later in Part V. At this stage in the analysis, however, it is useful to explore how a strict definitional application of the probable cause standard—as articulated in Rule 41[151]—might unduly limit some of the basic law enforcement uses of prospective and historical location information to the degree that legitimate investigative activities

151. *See* FED. R. CRIM. P. 41(c) (listing categories of probable cause: "(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").

dependent upon the use of these tools would be inhibited, even thwarted, from the start.[152]

If required to obtain a Rule 41 warrant for compelled disclosures of location information, the government would need to establish probable cause to believe that the location information *itself* is evidence of a crime.[153] In some instances, the location of a cell phone, insofar as it reveals a suspect's location, would qualify as evidence of a crime. Location information, for example, may rebut a defendant's alibi, place a defendant at the scene of a crime, or show that a defendant's movements are consistent with activities or overt acts alleged in furtherance of a criminal conspiracy.

But not every use of location information by law enforcement easily fits into the "evidence of a crime" element of Rule 41. If, for example, a person has committed a crime in the past, her current location may not be evidence of a crime, yet there might exist circumstances in which law enforcement has a legitimate need to find her.[154] If law enforcement has evidence to suggest that a person is about to commit a crime, her current location or prospective location leading up to the commission of that crime may or may not, itself, be evidence of a crime, yet our society generally accepts that law enforcement has a legitimate need to prevent her from committing a crime. Indeed, when addressing the DDP proposal that a probable cause warrant should be required for law enforcement access to all location data, Professor Kerr posed the question, "probable cause *of what*?"[155] Is it "probable cause to believe the person tracked is guilty of a crime" or "probable cause to believe the evidence of location information obtained would *itself* be evidence of a crime?"[156] Professor Kerr noted that the difference is important because, in the case of a search warrant, probable cause generally refers to probable

152. We do not claim to know, nor are we able to anticipate, all of the ways in which law enforcement uses prospective and historical location information in investigations.

153. *See In re* Application of the U.S. for an Order Authorizing the Release of Prospective Cell Site Info., 407 F. Supp. 2d 134, 135 (D.D.C. 2006) (explaining the difference between the D Order standard and probable cause as being that the latter requires a finding that there is probable cause to believe that the information sought is itself evidence of a crime rather than reasonable grounds to believe that the information sought is relevant and material to an ongoing investigation).

154. Some courts, however, have construed the probable cause requirement more broadly with respect to tracking devices or cell site data. *See, e.g.*, *In re* Application of the United States for and [sic] Order: (1) Authorizing the Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Info.; and (3) Authorizing the Disclosure of Location-Based Servs., 727 F. Supp. 2d 571, 581–82 (W.D. Tex. 2010).

155. *House Judiciary 2010 ECPA Reform Hearing*, *supra* note 18, at 39 (written statement of Prof. Orin S. Kerr, The George Washington Univ. Law Sch.).

156. *Id.*

cause to believe that the information sought is *itself* evidence of a crime.[157] Cell phone location data will be evidence of a crime in only certain kinds of cases and will not normally be evidence of a crime when investigators need to learn the current location of someone who committed a past crime.[158]

Magistrate Judge Susan K. Gauvey amplified this analysis in a recent decision when she concluded that a probable cause search warrant does not permit law enforcement to acquire GPS location information solely to execute an arrest warrant.[159] Specifically, the court noted that the government's "probable cause" theory for obtaining the GPS location data to locate the subject of the arrest warrant was that the "evidence sought will aid in a particular apprehension," not that it was evidence of a crime itself.[160] The government's request was for "broad information concerning [a] defendant's ongoing location" with no alleged relationship whatsoever between the "defendant's ongoing movements and his crime."[161] The court therefore reasoned that, because the government had not established the "requisite nexus between the information sought and the alleged crime, no search warrant may issue" for the location data.[162]

Moreover, in certain circumstances, law enforcement may compel historical location information to *exclude* someone from a criminal investigation. In that instance, the location information would not, under any reasonable stretch of Rule 41, be evidence of a crime but rather would serve the important function of "clearing" someone of criminal activity. Clearing a suspect would thus prevent further investigation, potentially avoiding a needless expenditure of government resources and a gratuitous government intrusion into his life by focusing the investigation more accurately upon the true perpetrator. These are just a few examples of how the "evidence of a crime" element of Rule 41 may not encompass important law enforcement investigative activities. To the extent that good policy may dictate a probable cause standard for location information, that standard would need to accommodate the diverse, legitimate uses of location information by law enforcement.

157. *Id.*

158. *Id.*

159. *In re* Application of the U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., No. 10-2188, 2011 U.S. Dist. LEXIS 85638 (D. Md. Aug. 3, 2011).

160. *Id.* at 93.

161. *Id.* at 105.

162. *Id.*

IV. LESSONS LEARNED

In 2010, the House Judiciary Subcommittee on the Constitution, Civil Rights, and Civil Liberties held three ECPA reform hearings (with Stephanie serving as lead counsel). The second of those hearings, and the most challenging to conceive and execute, explored issues pertaining to law enforcement access of location data (Location Hearing).[163] The hearing focused on supplying members of Congress with the knowledge necessary to clarify or propose new law enforcement access standards for location information.[164]

Some of the challenges Stephanie encountered in developing this hearing stemmed from factual and policy questions and quandaries that continue to inform the search for reasonable access standards and other reforms that will strike the right balance among the interests of law enforcement, consumer privacy, and industry. This Part discusses these challenges, which now motivate and shape the recommendations for the policy framework presented later in this Article.

A. ACQUIRING FACTS TO MAKE GOOD POLICY IS DIFFICULT

Location technology and the uncertain legal landscape governing law enforcement access to location information are complex subjects. As with most complicated issues, Congress needs information from all stakeholders—in this case from law enforcement, consumer privacy and civil liberties advocacy groups, and industry representatives—to judge the relative necessity for legislative action and discern the best directions for policy. When compared, however, with other new technologies prompting Subcommittee consideration of ECPA reform, such as cloud computing, the subject of location-based information and services inspires an unusual degree of secrecy on the part of both industry and law enforcement.

At a later Subcommittee ECPA reform hearing focused on cloud computing, five major cloud computing companies testified.[165] Industry testimony included explanations of business models and services offered by the various cloud companies and a discussion about how current ECPA standards are often difficult to apply to cloud services like Google Docs and

163. *See Location Hearing*, *supra* note 19.

164. *See id.*

165. *See generally ECPA Reform and the Revolution in Cloud Based Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. (2010) [hereinafter *Cloud Based Computing Hearing*], *available at* http://judiciary.house.gov/hearings/printers/111th/111-149_58409.PDF. Industry witnesses included representatives from Google, Microsoft, Salesforce, Rackspace, and Amazon.

Google Calendar.[166] Moreover, some of these companies asserted that weak ECPA privacy protections for information stored "in the cloud," versus the full Fourth Amendment protections afforded information stored on personal laptops, limits the expansion of the cloud market, particularly to foreign customers who are concerned that the U.S. government has overly broad access to cloud-stored information.[167]

In contrast to that very public cloud computing discussion, no wireless carriers or other providers of location-based services to consumers testified at the location hearing. While industry witnesses willingly discussed details about cloud-based services, as well as the challenges the law presents for the industry's compliance with law enforcement requests for information stored in the cloud, no similar public discussion occurred vis-à-vis law enforcement requests for location information or the types of location information carriers collect and retain.

Law enforcement is equally reticent to discuss publicly the investigative practices and processes they employ to obtain location information. While they willingly talk about how critical location information is for a variety of enforcement responsibilities,[168] they will confirm only very general information about the acquisition and uses of the location data. Of course, when overly detailed information about sources and methods becomes public, these sources and methods may cease to be useful investigative tools.[169] But, unlike Wiretaps or Pen/Trap surveillance, Congress does not even have a sense of the number and scope of law enforcement requests for

166. *See id.* at 20 (statement of Richard Salgado, Senior Counsel, Law Enforcement & Info. Sec., Google Inc.).

167. *See id.* at 40 (testimony of David Schelhase, Exec. Vice President & Gen. Counsel, Salesforce.com) (explaining that customers considering storing their information in the cloud want assurances that the U.S. government will not access their data without appropriate due process).

168. *See Senate Judiciary 2011 ECPA Hearing*, *supra* note 7, at 5 (testimony of James A. Baker); *see also Location Hearing*, *supra* note 19, at 60–61 (written statement of Richard Littlehale, Assistant Special Agent in Charge, Technical Servs. Unit, Tenn. Bureau of Investigation) (describing how cell phone location information frequently permits law enforcement an opportunity to find and rescue a victim or apprehend an offender in a matter of hours).

169. We are not in a position to assess all of the circumstances where location information as an investigative tool could become less useful to law enforcement upon more disclosure about the method and frequency of this tool. We do note, however, that cellphones are increasingly becoming a necessary tool for society, and as a result, it is extremely difficult to avoid the possibility of location surveillance without turning off a phone, and losing all the benefits of that technology.

location information, statistics that would not necessarily require the exposure of detailed sources and methods.[170]

While we can debate the motivations for the lack of detailed information in the public record about industry and law enforcement practices pertaining to location information, at the end of the day, Congress needs comprehensive information to legislate good policy. For both Wiretap and Pen/Trap authorities, for example, Congress mandated annual Wiretap and Pen/Trap reports, recognizing the need for accurate reporting on law enforcement's use of these tools.[171] As Senator Patrick Leahy has stated, reporting requirements are a "far more reliable basis than anecdotal evidence on which to assess law enforcement needs and make sensible policy in this area,"[172] as well as providing some degree of transparency and oversight of these surveillance powers.[173] No reporting requirements currently exist for location information.[174] Back in 2000, however, the Republican-controlled House Judiciary Committee proposed legislation concerning law enforcement access standards for prospective location information.[175] This bill included new reporting requirements that would have given Congress some sense of the scale of law enforcement compelled disclosures, as well as the number of people whose data was provided to law enforcement.[176] The

170. *See generally* Christopher Soghoian, The Law Enforcement Surveillance Reporting Gap (Apr. 10, 2011) (unpublished manuscript), *available at* http://ssrn.com/abstract=1806628.

171. *See* 18 U.S.C. § 2519(2)–(3) (2010) (outlining what the intercepted communications report issued by the Administrative Office of the United States Courts must contain). These reports are detailed, revealing for each wiretap the city or county where it was executed, the type of interception (phone, computer, pager, fax), the number of individuals whose communications were intercepted, the number of intercepted messages, the number of arrests and convictions that resulted from interception, as well as the financial cost of the wiretap. *See also id.* § 3126.

172. 145 CONG. REC. 30,868 (1999) (statement of Sen. Leahy).

173. S. REP. NO. 90-1097, at 79 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2196 ("[The wiretap reports] are intended to form the basis for a public evaluation of its operation. The reports are not intended to include confidential material. They should be statistical in character. . . . [They] will assure the community that the system of court order electronic surveillance envisioned by the proposed chapter is properly administered and will provide a basis for evaluating its operation.").

174. *See* Soghoian, *supra* note 170, at 22.

175. *See Electronic Communications Privacy Act of 2000, Digital Privacy Act of 2000 and Notice of Electronic Monitoring Act: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 106th Cong. (2000) [hereinafter *House Judiciary 2000 ECPA Hearing*].

176. *See* Digital Privacy Act, H.R. 4987, 106th Cong. (2000). While the DOJ opposed the particular formulation of these reporting requirements because they were overly burdensome, they could be structured to be less onerous on investigators and prosecutors. *See House Judiciary 2000 ECPA Hearing*, *supra* note 175, at 51 (statement of Kevin DiGregory, Deputy Assoc. Attorney Gen., Dep't of Justice) ("[T]he imposition of such extensive

bill did not become law and now, more than ten years later, Congress has little more information than it did in 2000.[177]

B. THE SINGULAR ADVOCACY FOCUS ON LAW ENFORCEMENT STANDARDS HAS NARROWED A DISCUSSION THAT SHOULD INCLUDE MINIMIZATION AND OTHER "DOWNSTREAM" PRIVACY PROTECTIONS

The advocacy regarding the appropriate standard for law enforcement access to location information has largely focused on the DDP Coalition principle calling for a Rule 41 probable cause requirement for all law enforcement compelled disclosures of location information (historical and prospective, regardless of accuracy).[178] This unitary standard, however, is a "non-starter" for law enforcement insofar as it will unduly limit the acquisition of non-content information at the early stages of an investigation and will likely prohibit some basic investigative uses of location information.[179] Indeed, it is one side of what has appeared to become a rather intractable stalemate.

The singular advocacy focus on a "high" law enforcement access standard unduly limited a discussion of other downstream, post collection privacy protections, which were neither included in the DDP proposal nor adequately considered publicly. Such additional protections are a significant component, along with reasonable access standards, in the broader privacy framework proposed in Part VI. Such measures, mandated by Congress for other surveillance authorities, include: minimization, a process by which information not relevant to the investigation is purged from law enforcement databases;[180] notice to individuals whose location information has been disclosed to law enforcement at a time that does not harm an ongoing investigation;[181] and the publication of statistical reports on law enforcement use of location surveillance authorities.[182] These sorts of protections are one

reporting requirements for cyber-crime investigators would come at a time when law enforcement authorities are strapped for resources to fight cyber-crime. The reporting requirements for wiretaps, while extensive, are less onerous because law enforcement applies for such orders relatively rarely. Extending such requirements to orders used to obtain mere transactional data would dramatically hinder efforts to fight cyber-crime, such as the distribution of child pornography and Internet fraud.").

177. *See* Soghoian, *supra* note 170, at 23.

178. *See Our Principles*, *supra* note 22.

179. *See supra* Part III.

180. *See* 18 U.S.C. § 2518(5) (2010); 50 U.S.C. § 1804(a)(5) (2009); *id.* § 1861(b)(2)(B).

181. *See* 18 U.S.C. § 2518(8)(d) (1998).

182. *See* 18 U.S.C. § 2519 (2010).

way to balance or offset access standards authorizing broader law enforcement collection of data.

C. THE POLARIZED VIEWS OF LAW ENFORCEMENT AND PRIVACY ADVOCATES MAKE CONSENSUS BUILDING DIFFICULT

It is not particularly insightful to observe that when one side of a debate starts from a position that is completely unworkable for the other side and will not move, it is difficult to build consensus. If, at the end of the day, the only standard for location data that is acceptable to privacy advocates is a Rule 41 probable cause standard, then they risk letting the proverbial perfect be the enemy of the good. The advocacy message for overall ECPA reform—while supported through industry participation in the DDP Coalition and echoed by strong industry voices outside of the coalition calling for Congress to enact clear legal rules and shelter industry from liability—was driven primarily by privacy advocates. Thus, the burden to suggest new, workable, and more privacy-protective standards falls primarily on the shoulders of the community of privacy advocates. This is not an area where law enforcement will likely act as a willing catalyst for new access standards that place restrictions on their own investigative tools in the name of better privacy protections, even if they are prepared to agree to a fair compromise in the end. Moreover, law enforcement has strong advocates in Congress who will fight against overly broad proposals to restrict investigative authorities. Consider, for example, the opening statement by then Ranking Member Sensenbrenner (now Chairman of the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security and author of the USA PATRIOT Act) at the Location Hearing. Having clearly read the proposal for a unitary probable cause standard, the Ranking Member announced, "While there may very well be a need to clear up the confusion in the area of obtaining prospective cell site information, it does not necessarily follow that the appropriate remedy to any ambiguity would be a Rule 41 search warrant based upon probable cause."[183]

Notwithstanding such strong allies in Congress, however, the DOJ should carefully measure the practical impact of *Jones*. While *Jones* does not hold that a warrant is required for the installation and use of a GPS tracking device,[184] a prudent prosecutor interested in ensuring that GPS tracking

183. *Location Hearing*, *supra* note 19, at 3 (opening statement of ranking member Rep. Jim Sensenbrenner).

184. The Court declined to reach the question of whether a warrant is required to install a GPS device. *See* United States v. Jones, 132 S. Ct. 945, 954 (2012) ("The Government argues in the alternative that even if the attachment and use of the device was a search, it was reasonable—and thus lawful—under the Fourth Amendment because 'officers had

evidence is admissible at trial would, absent further judicial or congressional guidance, be wise to obtain one in every instance. Only time will tell whether this new strategic necessity will have a measurable adverse impact on law enforcement investigations.

A more urgent concern for the DOJ, however, should be the threat of continued judicial application and expansion of the mosaic theory inspired by the signals in the *Jones* concurrences. The signals in the *Jones* concurrences indicate that a majority of the Court could, in the future, incorporate some version of the theory into its Fourth Amendment jurisprudence. As we have seen, absent clear congressional guidance regarding standards for law enforcement access to location data, some courts are already applying the mosaic theory to government applications for historical cell location data with varying interpretations about how much data forms a mosaic and triggers a Fourth Amendment issue.[185] Justice Alito's answer for how to deal with the thorny line drawing problem under a theory that does not define when the mosaic materializes is simple: "where uncertainty exists with respect to whether a certain period of GPS surveillance is long enough to constitute a Fourth Amendment Search, police may always seek a warrant."[186] But this simple dictate is hardly a viable one for law enforcement in every instance.[187] If the DOJ finds this potential reality to be unworkable and harmful to future law enforcement investigations (as it has suggested in congressional testimony),[188] it should engage earnestly in the legislative process and be prepared to agree to some reasonable additional privacy protections. Indeed, the prospect of a majority that would make the mosaic

reasonable suspicion, and indeed probable cause, to believe that [Jones] was a leader in a large-scale cocaine distribution conspiracy.' We have no occasion to consider this argument. The Government did not raise it below, and the D.C. Circuit therefore did not address it." (citation omitted)); *see also* Orin S. Kerr, *What* Jones *Does* Not *Hold*, VOLOKH CONSPIRACY (Jan. 23, 2012), *available at* http://volokh.com/2012/01/23/what-jones-does-not-hold/ ("[W]e actually don't yet know if a warrant is required to install a GPS device; we just know that the installation of the device is a Fourth Amendment 'search.' ").

185. *See supra* Section III.B.2.b.

186. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

187. *See supra* Section III.A.3.

188. *See Senate Judiciary 2011 ECPA Hearing*, *supra* note 7, at 5 (testimony of James A. Baker, Assoc. Deputy Attorney Gen., U.S. Dep't of Justice) ("If an amendment [to ECPA] were to unduly restrict the ability of law enforcement to quickly and efficiently determine the general location of a terrorist, kidnapper, child predator, computer hacker or other dangerous criminal, it would have a very real and very human cost.").

theory the law of the land should concentrate the Department's mind wonderfully upon resolving this issue through the legislative process.[189]

V. WHAT IS THE HARM, AND WHO CAN ADDRESS IT MOST EFFECTIVELY?

In proposing that Congress reform existing location privacy law, we confront a logical threshold question: just what harms would we seek to prevent? When it first enacted the Electronic Communications Privacy Act back in 1986, Congress sought to reestablish the balance of interests between law enforcement and privacy[190] that had been upset—to the detriment of privacy—by advances in wireless and computing technologies.[191] Congress also recognized that consumers might not embrace new technologies if privacy interests were not appropriately protected.[192] As technology continues to develop—simultaneously enriching our lives and facilitating more prevalent government (and private) surveillance—Congress, once again, is preparing to confront the task of establishing an appropriate balance among stakeholder equities,[193] which prompts us, yet again, to ask this threshold question.

In recent years, prominent judges have, in written opinions, described and voiced concern over the harms associated with modern location tracking technologies. In doing so, they have suggested that Congress, not the judiciary, might be in the best position to provide appropriate incentives and

189. "Depend upon it, Sir, when a man knows he is to be hanged in a fortnight, it concentrates his mind wonderfully." JAMES BOSWELL, LIFE OF JOHNSON 849 (Oxford Univ. Press 1960) (1791).

190. *See House Judiciary 2010 ECPA Reform Hearing*, *supra* note 18, at 8–9 (written statement of James X. Dempsey, Vice President for Pub. Policy, Ctr. for Democracy & Tech.) (discussing balance of interests Congress sought to strike in enacting ECPA).

191. Among the developments noted by Congress were "large-scale electronic mail operations, cellular and cordless phones, paging devices, miniaturized transmitters for radio surveillance, and a dazzling array of digitized networks . . . ." H.R. REP. NO. 99-647, at 18 (1986). Privacy, Congress concluded, was in danger of being gradually diminished as technology advanced. S. REP. NO. 99-541, at 2–3, 5 (1986); *see also* H.R. REP. NO. 99-647, at 18 (stating that "legal protection against the unreasonable use of newer surveillance techniques has not kept pace with technology").

192. *See* S. REP. NO. 99-541, at 5 (noting that legal uncertainty over the privacy status of new forms of communications "may unnecessarily discourage potential customers from using innovative communications systems"); *see also* H.R. REP. NO. 99-647, at 19 (noting that legal uncertainty over confidentiality "may unnecessarily discourage potential customers from using . . . [new] systems").

193. As of the writing of this Article, five separate hearings on ECPA reform were held during the 111th and 112th sessions of Congress (three hearings held in the House Judiciary Committee and two hearings in the Senate Judiciary Committee).

remedies. We take our cue from these judges and their stated concerns to identify potential harms Congress should consider when it evaluates the relative necessity for legislative action and discerns the best policy direction.[194]

A. THE GOVERNMENT'S GAZE AND THE PANOPTIC EFFECT

As we shall see, some judges who have considered cases involving law enforcement access to location data posit that the persistent gaze of government may itself represent an objective harm to the public.[195] In doing so, these judges have alluded to surveillance theories found in literature, social theory, and philosophy. To evaluate and discuss their conclusions fully, we must briefly describe some of that material and how it appears, directly or allusively, in their opinions.

Late eighteenth-century theories of surveillance as an instrument to administer discipline and enforce social control, such as Jeremy Bentham's "Panopticon" prison architecture,[196] suggest that the potency of the government's gaze is such that, when imposed strategically and with suggested if not actual universality and constancy, it becomes internalized in the very minds of those subjected to its influence as a mechanism of rehabilitative discipline.[197] Moreover, Bentham envisioned the Panopticon's design as appropriate not only to prisons, but to any environment where enhanced discipline is desired: schools, asylums, factories, and more. In short, for Bentham, the panoptic gaze of the state could serve as a secular version of the all-seeing eye of the Judeo-Christian God, and the normative behavioral conformity religious conscience once inspired would be supplanted on more certain ground by the discipline this modern gaze could inspire.

The twentieth-century French social theorist Michel Foucault rigorously analyzed Bentham's project in the Panopticon and expanded it into an interpretive metaphor for coercive social power. Foucault examines "Panopticism" as an instance of modern society's ability to compel

194. What follows in this Section is not an attempt to describe an authoritative legal or philosophical theory of the harms inherent in unjustified disclosure of location data, though we shall have occasion to allude to law, philosophy, and literature in service of the task of describing those harms as expressed by judges who have confronted them and chosen to discuss them in recent opinions.

195. *See* United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring) ("The constitutional ill of prolonged or mass use of GPS technology would not necessarily be based on the information acquired by the device but on the fact of the government's gaze.").

196. *See* JEREMY BENTHAM, THE PANOPTICON WRITINGS 29–95 (Miran Bozovic ed., 1995) (1787).

197. *Id.*

compliance with its approved behavioral norms through its institutions and their various discourses.[198] The presence of modern surveillance mechanisms, visible and imperceptible, public and private, promotes the "Panoptic effect"—a general sense of being omnisciently observed. The state may choose to deploy this effect to amplify and mystify the power of its own "gaze" as a coercive instrument, and to promote the internalization of that gaze in the service of discipline.[199]

Bentham's plan for the Panopticon was fairly simple: a model prison consisting of a central tower surrounded by a ring of prison cells, each of them backlit, so that anyone in the tower could see all of the prisoners at once. Bentham posited that a single inspector in the tower could control the behavior of all of the prisoners through making each prisoner "always feel themselves as if under inspection, at least as standing a great chance of being so."[200] Eventually, since the backlit cells and the tower structure made it impossible for prisoners to observe him, the monitor in the tower would actually become superfluous and the inmates, having internalized the presumption of his continued surveillance, would literally *watch themselves*.

198. *See* MICHEL FOUCAULT, DISCIPLINE & PUNISH: THE BIRTH OF THE PRISON 195–228 (1978). Discourse in this case does not refer merely to the word's common denotation as written or spoken communication or debate, but to the word as used in modern social theory, particularly the work of Foucault, referring to the various systems of linguistic usages associated with complex social practices (e.g., law, medicine, religion) deployed as instruments of social power, particularly the power of the state. *See generally* MICHEL FOUCAULT, THE ORDER OF THINGS (1970); MICHEL FOUCAULT, THE ARCHEOLOGY OF KNOWLEDGE (1972). For an extended discussion of the diffuse nature of power in society and the role this concept of discourse plays in analyzing how ideas and language encode power in social spaces and, therefore, have the potential to play a role in historical change, see MICHEL FOUCAULT, *Two Lectures*, *in* POWER/KNOWLEDGE: SELECTED INTERVIEWS & OTHER WRITINGS 78 (Colin Gordon ed., 1980).

199. It is important to note that more recent writers on "surveillance theory" have qualified Bentham and Foucault usefully. *See, e.g.*, GILLES DELEUZE, POSTSCRIPT ON THE SOCIETIES OF CONTROL 3–7 (1992) (distinguishing Foucault's "disciplinary" society from his own "control" society in critique of the Panopticon); DAVID LYON, THEORIZING SURVEILLANCE: THE PANOPTICON AND BEYOND (2006); DAVID LYON, SURVEILLANCE STUDIES: AN OVERVIEW 54–62 (2007) (summarizing contemporary criticism qualifying the application of Foucault's analysis to contemporary surveillance). While the rigor and depth of recent surveillance theory is indispensible background to anyone who would consider surveillance in all its profundity, its presence in legal opinions to date, which is the focus in this Article, has been predominantly restricted to metaphorical allusions to Orwell's dystopia in *1984* and some consideration of the government's "gaze" as discussed in Foucault's interpretation of the Panopticon. Since these interpretive frames are effectively canonical and, as such, disseminated commonly enough to drive judicial decision making, as well as the appeal by the judiciary for legislation in this area, we place our own main focus on them at this moment in the policy debate.

200. Jeremy Bentham, *Letter V: Essential Points of the Plan*, *in* BENTHAM, *supra* note 196.

Foucault claimed this internalization of surveillance made the Panopticon a quintessential figure for a peculiarly modern and secular form of state power that arose in the Enlightenment, "a new mode of obtaining power of mind over mind, in a quantity hitherto without example."[201]

As modern location surveillance techniques increase in precision and their pervasive distribution throughout society becomes known, though the instruments themselves may or may not remain invisible, people become increasingly aware of, and potentially influenced by, a palpable sense of the omniscient gaze similar to that produced by Bentham's prison design.

Consider, for example, that through the use of modern surveillance technologies, a single police officer can now monitor the movement of tens, even hundreds, of targets from the comfort of her desk[202] and, because there is no statutory notice provided to those under such surveillance, targets have no way of knowing if and when they are being or have been watched.[203] While surveillance has traditionally been very expensive in terms of human resources (often requiring multiple shifts of agents to watch a single target for a twenty-four-hour period), the ubiquity of cellular phones and innovations in GPS tracking technology has made surveillance easier, cheaper, and consequently more prevalent.[204] A law enforcement agency's gaze is no longer limited by the number of agents available to drive around a city, but only by the amount of money available in its budget to pay wireless carriers for their assistance, or to purchase GPS tracking devices or other similar technologies.[205] Moreover, although such surveillance is supposed to

201. *Id.* at Preface.

202. United States v. Pineda-Moreno, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, J., dissenting from denial of rehearing en banc).

203. *See Appeal of In re W.D. Pa. Application*, 620 F.3d 304, 317 (3d Cir. 2010) (noting that "it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information").

204. *See* United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007) ("The new [surveillance] technologies enable, as the old (because of expense) do not, wholesale surveillance. . . . Technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive.").

205. Christopher Soghoian, *An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government*, 12 MINN. J.L. SCI. & TECH. 191, 222–23 (2011). ("Many telecommunications companies and ISPs seek and typically receive payment from government agencies for the surveillance services they provide, a practice that the law often permits."). The cost of location surveillance by some carriers appears to have plummeted over the past decade—a savings that they were obligated to pass on to law enforcement, though no public data exists for comparison. For example, in 2003, Nextel communications charged $150 per "ping." *See* NEXTEL, SUBPOENA & COURT ORDERS: NEXTEL'S GUIDE FOR LAW ENFORCEMENT 6 (2003), *available at* http://info.publicintelligence.net/nextelsubpoena.pdf. In 2009, it was revealed that law enforcement agencies had performed 8 million pings

be invisible, it is becoming more perceptible through media stories, making the fact of its pervasive existence known, at least in an abstract sense.[206] This simultaneous visible and invisible presence of surveillance is precisely what produces the anxiety that is the foundation of the panoptic effect.[207] These particular location technologies partake of a whole system of surveillance instruments and mechanisms, both governmental and private, which construct and project the government's gaze.[208]

Echoing the conclusions hinted at by the history of surveillance, its coercive utility, and the rapid innovation in contemporary surveillance technology, including geolocation systems, Seventh Circuit Judge Flaum, while criticizing the reasoning of *Maynard* in *Cuevas-Perez*, suggests that the fact of the "government's gaze" itself, as exerted by "mass use of GPS

via a website created by Sprint/Nextel. *See Pineda-Moreno*, 617 F.3d at 1125 (Kozinski, J., dissenting from denial of rehearing en banc). Although we have no direct evidence to suggest that the carrier has reduced the cost of its pings (or moved to a fixed fee, rather than per-ping charges), even without adjusting for inflation, had Sprint charged $150 for each of the 8 million pings, it would have made $1.2 billion. Since law enforcement certainly did not spend that much money for this purpose, some new billing arrangement must have motivated the increased activity level.

206. *See generally The Wire* (HBO cable television series, 2002–2008); *see also* Anders Albrechtslund, *Surveillance and Ethics in Film:* Rear Window *and* The Conversation, 15 J. CRIM. JUST. & POPULAR CULTURE, no. 2, 2008, at 129–44.

207. Regarding the "Panoptic effect" of the state's gaze, Professor Daniel Solove points out that:

> Although concealed spying is certainly deceptive . . . [i]t is the awareness that one is being watched that affects one's freedom. . . . A more compelling reason why covert surveillance is problematic is that it can still have a chilling effect on behavior. In fact, there can be a more widespread chilling effect when people are generally aware of the possibility of surveillance but are never sure if they are being watched at any particular moment.

DANIEL SOLOVE, UNDERSTANDING PRIVACY 109 (2008). This is true, unequivocally, regarding the specular value of strategically displaying and withholding evidence of state power. Moreover, revelations of the covert commercial use of location-based tools, such as the recently divulged use of Apple's iPhone and Google's Android phones in WiFi mapping, have the indirect effect of reinforcing the general sense of the state's coercive gaze and its power to influence compliance with social norms, whether or not there is any actual convergence of interest between the state and private actors in a given case. *See* Angwin & Valentino-Devries, *supra* note 41.

208. *See* Christopher Slobogin, *Is the Fourth Amendment Relevant in a Technological Age?*, FUTURE CONST. (Brookings Inst., Washington, D.C.), Dec. 8, 2010, *available at* http://www.brookings.edu/~/media/Files/rc/papers/2010/1208_4th_amendment_slobogin/1208_4th_amendment_slobogin.pdf (describing the negative, real world impacts of surveillance even when the government makes no use of the surveillance product).

technology," may represent a "constitutional ill" which amounts to a cognizable harm.[209]

Historical location information produced by mobile devices adds another layer of implication to the panoptic effect. Such information is, of course, a record of where we have been. These data are stored by companies providing wireless services to consumers and on mobile devices for periods of time unknown to the user since retention policies vary by company.[210] Some companies may store more precise data than others,[211] but through these data the government may get an accurate picture of most everywhere we have been.[212] Moreover, once information is disclosed, the government entities responsible for the investigation add it to databases and keep it for an indefinite period of time.[213] In effect, modern location technology can give the government an increasingly perfect memory of our activities, thus making it impossible to escape one's past. Data retention policy, at this point, might be considered a relatively unknown and thus "immature" source of panoptic power. We are only now beginning to learn the details and scope of the heretofore hidden commercial use of location data on smartphones,[214] and Congress is currently considering data retention legislation that will require providers to store subscriber data for twelve months.[215] These developments

209. United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring).

210. Soghoian, *supra* note 205, at 210 ("[M]ost technology providers and communications carriers now have established data retention policies that govern the length of time before which they will delete customer records, communications, logs, and other data. Unfortunately, outside of the search engine market, where pressure from European regulators has led to companies publicly touting their policies, few other firms will publicly reveal their own data retention rules.").

211. *See Location Hearing*, *supra* note 19, at 27 (written statement of Prof. Matt Blaze, Univ. of Pa.).

212. *See* People v. Weaver, 12 N.Y.3d 433, 441–42 (2009) (describing the types of information that tracking devices can record about an individual's life).

213. *See generally* Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435 (2008). Moreover, the data of innocent individuals who are not targets of government surveillance can get "swept up" by community of interest requests or other compelled disclosures of data that seek to discover everyone who was at or near a particular location at a particular time.

214. *See* Jennifer Valentino-DeVries & Julia Angwin, *Latest Treasure Is Location Data*, WALL ST. J. (May 10, 2011), http://on.wsj.com/xJGP9u ("Location information is emerging as one of the hottest commodities in the tracking industry . . . . [T]he Journal's 'What They Know' series found that 47 of the 101 most popular smartphone apps sent location information to other companies.").

215. The Protecting Children from Internet Pornographers Act of 2011 was favorably reported out of the House Judiciary Committee on July 28, 2011 and requires certain types of providers to retain some types of data for at least 12 months. *See* H.R. 1981, 112th Cong. § 4 (2011), *available at* http://1.usa.gov/xeBBB6.

will inevitably lead to a broader public discussion of both the commercial and law enforcement uses of historical location data. These discussions will ostensibly be conducted in the name of protecting the public from the government's intrusive eye, which will serve ironically to enhance its power to reinforce the panoptic effect.

More than forty years ago, Vice President Hubert Humphrey observed that "[w]e act differently if we believe we are being observed. If we can never be sure whether or not we are being watched and listened to, all our actions will be altered and our very character will change.[216] Justice Douglas made the same point a few years later, observing that "[m]onitoring, if prevalent, certainly kills free discourse . . . ."[217] Humphrey and Douglas both anticipate Foucault in their conclusions in describing the effect of being observed. To these men, one of politics, the other of law, the observing gaze of the state was, intuitively, a powerfully coercive force that changes people, as surely and utterly as the Medusa's gaze was said to change men to stone.

The ever-improving accuracy of location technology has given the government's gaze a degree of clarity hitherto undreamed of, except perhaps in dystopian novels such as Orwell's *1984*. Notably, as they confront the powerful gaze of modern surveillance technologies, judges around the country are voicing their own anxiety regarding the impact of this technology on individuals and society, often turning to sources like Orwell to illustrate their conclusions. In *People v. Weaver*, a case about a GPS tracking device placed on a car, Judge Lippman expressed his concern over the very personal profile of an individual's life captured by tracking technologies:

> The whole of a person's progress through the world, into both public and private spatial spheres, can be charted and recorded over lengthy periods possibly limited only by the need to change the transmitting unit's batteries. Disclosed in the data retrieved from the transmitting unit, nearly instantaneously with the press of a button on the highly portable receiving unit, will be trips the indisputably private nature of which takes little imagination to conjure: 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. What the technology yields and records with breathtaking quality and quantity is a highly detailed profile, not simply of where we go, but by easy inference, of our associations—political, religious, amicable and amorous, to name only a few—and of the pattern of our

216. Hubert H. Humphrey, *Foreword*, *in* EDWARD V. LONG, THE INTRUDERS, at viii (1967).
217. United States v. White, 401 U.S. 745, 762 (1971).

> professional and avocational pursuits. When multiple GPS devices are utilized, even more precisely resolved inferences about our activities are possible. And, with GPS becoming an increasingly routine feature in cars and cell phones, it will be possible to tell from the technology with ever increasing precision who we are and are not with, when we are and are not with them, and what we do and do not carry on our persons—to mention just a few of the highly feasible empirical configurations.[218]

Likewise, in his dissent in *United States v. Pineda-Moreno*,[219] a case where the Ninth Circuit rejected en banc review of a panel decision involving GPS technology, the ever-witty[220] Judge Kozinski turns deadly serious, invoking his own childhood in Communist Romania and alluding directly to the setting of *1984* as he describes the tracking technology in question:

> 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. This case, if any, deserves the comprehensive, mature and diverse consideration that an en banc panel can provide. We are taking a giant leap into the unknown, and the consequences for ourselves and our children may be dire and irreversible. Some day, soon, we may wake up and find we're living in Oceania.[221]

---

218. People v. Weaver, 12 N.Y.3d 433, 441–42 (May 12, 2009).

219. United States v. Pineda-Moreno, 617 F.3d 1120, 1121–26 (9th Cir. 2010) (Kozinski, J., dissenting from denial of rehearing en banc).

220. In criticizing the underlying panel's conclusion that the defendant has no expectation of privacy in his driveway, Judge Kozinski explains:

> The panel authorizes police to do not only what invited strangers could, but also uninvited children—in this case crawl under the car to retrieve a ball and tinker with the undercarriage. But there's no limit to what neighborhood kids will do, given half a chance: They'll jump the fence, crawl under the porch, pick fruit from the trees, set fire to the cat and micturate on the azaleas. To say the police may do on your property what urchins might do spells the end of Fourth Amendment protections for most people's curtilage.

Id. at 1123.

221. *Id.* at 1126. Further, the court in *United States v. Sparks* refused to find a Fourth Amendment violation in the government's use of GPS placed on the defendant's vehicle under the specific facts of the case, but it nonetheless acknowledged that the court "is not unsympathetic to the sentiment expressed by Chief Justice Kozinski and his Ninth Circuit

Judge Kozinski's language echoes the disturbing uncertainty that results when the instruments of the state's panoptic gaze become even partially visible. Indeed, as we have discussed, the very partial nature of their visibility is essential to produce the uncertainty and anxiety of the panoptic effect. In response, Judge Kozinski appeals to a locus of greater authority, here an en banc panel of the Ninth Circuit, to assert the control (i.e., "comprehensive, mature and diverse consideration") necessary to govern the state's panoptic gaze in the name of preserving the specifically "American" way of life it seems to threaten.

Judge Flaum, in his concurring opinion in *Cuevas-Perez*, goes further still, suggesting the government's increasingly powerful and clear sense of sight with regard to the lives of individuals, using new, more accurate location technologies, might offend the Fourth Amendment in a manner explicitly proscribed by the Founders as it was being crafted:

> There may be a colorable argument . . . that the use of GPS technology to engage in long-term tracking is analogous to general warrants that the Fourth Amendment was designed to curtail, because of the technology's potential to be used arbitrarily or because it may alter the relationship between citizen and government in a way that is inimical to democratic society.[222]

---

brethren, that there is something 'creepy' about continuous surveillance by the government." 750 F. Supp. 2d 384, 395–96 (D. Mass. 2010). While noting that "[a]dvances in technology, like GPS devices, provide neutral and credible evidence and thus facilitate the ultimate (and yet amorphous) goal of 'justice,' " the court also recognizes that "it is easy to envision the worst-case Orwellian society, where all citizens are monitored by the Big Brother government." *Id.* at 394–95; *see also In re* Application of the U.S. Authorizing the Release of Historic Cell-Site Info., 809 F. Supp. 2d 113, 127 (E.D.N.Y. 2011) ("While the government's monitoring of our thoughts may be the archetypical Orwellian intrusion, the government's surveillance of our movements over a considerable time period through new technologies, such as the collection of cell-site-location records, without the protection of the Fourth Amendment, puts our county far closer to Oceania than our Constitution permits.").

222. United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring). In the same case, in her dissent, Judge Wood also appeals to Orwell for interpretive authority, with a sense of urgency matching that of Judges Flaum and Kozinski:

> This case presents a critically important question about the government's ability constantly to monitor a person's movements, on and off the public streets, for an open-ended period of time. The technological devices available for such monitoring 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.

Id. at 286 (Wood, J., dissenting).

Judge Flaum's concurrence strongly criticizes the reasoning of the *Maynard* court[223] (the case concluding that *United States v. Knotts*[224] does not govern prolonged GPS surveillance and instead applying a mosaic theory of the Fourth Amendment), yet he seems to go out of his way to propose an alternative theory of the Fourth Amendment that might, perhaps, offer a way to cabin or control the government's prolonged use of GPS tracking. This palpable concern on the part of senior jurists from two appellate courts is indicative of the general harm to society, to which all others are ancillary, created by location technology, and the issues this technology raises should be scrutinized accordingly.

But where should one turn for sufficient authority? A Ninth Circuit en banc panel? How about the ultimate authority in the judicial branch: the Supreme Court of the United States? Judge Flaum considers that option briefly, perhaps aware of the government's petition for certiorari in *Maynard*, later granted in *Jones*,[225] in further reducing his argument to its bare bones: "on this view, the constitutional ill of prolonged or mass use of GPS technology would not necessarily be based on the information acquired by the device but on the fact of the government's gaze."[226]

It may be tempting, as a judge on a federal appellate court, to urge the Supreme Court to employ the Fourth Amendment against the "ill" that can be inflicted by the mere "fact of the government's gaze." But Judge Flaum himself, having indulged in the Fourth Amendment argument and perhaps gauging the limited power of the judiciary to use the common law in an effort to assert control of technology changing at the pace of Moore's Law,[227] immediately withdraws it in favor of a legislative remedy:

---

223. *Id.* at 280 (Flaum, J., concurring) ("Neither of *Maynard*'s twin bases for ruling that the defendant had an objectively reasonable expectation of privacy is doctrinally sound—or all that workable as a practical matter.").

224. 460 U.S. 276 (1983) (holding that a person does not have a reasonable expectation of privacy in movements from one place to another on public thoroughfares).

225. *See* Petition for Writ of Certiorari, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259).

226. *Cuevas-Perez*, 640 F.3d at 285 (7th Cir. 2011) (Flaum, J., concurring).

227. Moore's law describes a long-term trend in the development of computer hardware, specifically that the number of transistors that can be placed inexpensively on an integrated circuit doubles approximately every two years, resulting in a corresponding, roughly exponential, increase in the capabilities of many digital devices—processors, computer memory, digital camera resolution, and more. Moore's projected rate of growth, which is used in the semiconductor industry to guide long-term planning and to set targets for research and development, has continued for over fifty years and is expected to remain constant through at least 2015 or later. It was named for Gordon E. Moore, the co-founder of Intel, who described the trend in a 1965 paper. Gordon E. Moore, *Cramming More Components onto Integrated Circuits*, 38 ELECTRONICS, no. 8, Apr. 19, 1965, *available at*

> Of course, the Supreme Court just last term reminded us that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." *City of Ontario v. Quon*, 130 S. Ct. 2619, 2629 (2010). In light of *Knotts*'s holding and *Quon*'s admonition, it strikes me not so much as insufficiently circumspect as simply beyond our mandate to conclude that what is permissible when accomplished with a beeper is impermissible when accomplished with a GPS unit. I agree with the dissent, however, that nothing would preclude Congress from taking the important questions implicated by GPS technology and imposing answers. Indeed, the unsettled, evolving expectations in this realm, combined with the fast pace of technological change, may make the legislature the branch of government that is best suited, and best situated, to act.[228]

The Supreme Court has now decided *Jones*. Where do we find ourselves? The concurring opinions echo the concerns Judge Kozinski and Judge Flaum expressed. Justice Alito's concurrence recognizes that law enforcement's secret, long-term monitoring of every single movement of an individual's car does not accord with society's reasonable expectations of privacy.[229] Justice Sotomayor even quotes Judge Flaum's concurrence in *Cuevas-Perez* as she asserts: "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.' "[230]

The majority opinion, however, functions only to limit the scope of the "government's gaze" with respect to the physical attachment and use of a GPS tracking device. Indeed, the majority's definition of "search" does not apply to situations where the transmission of radio or other electronic signals is not attained through the government's physical attachment of a device by trespass. Moreover, Justice Alito's adoption of a mosaic-type theory raises

---

http://download.intel.com/museum/Moores_Law/Articles-Press_releases/Gordon_Moore_1965_Article.pdf. *See generally* Bob Schaller, The Benchmark of Progress in Semiconductor Electronics (Sept. 26, 1996) (unpublished paper), *available at* http://research.microsoft.com/en-us/um/people/gray/Moore_Law.html.

228. *Cuevas-Perez*, 640 F.3d at 285–86 (Flaum, J., concurring) (citing Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805–06 (2004) (arguing that Congress should be the primary driver of privacy protections when technology "is in flux")).

229. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

230. *Id.* at 956 (Sotomayor, J., concurring) (quoting *Cuevas-Perez*, 640 F.3d at 285) (Flaum, J., concurring)).

the same thorny line drawing issues presented by *Maynard*.[231] Perhaps recognizing the limitations of this approach, Justice Alito acknowledges that "[t]he best we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated."[232] But like Judge Flaum, Justice Alito recognizes that "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."[233]

Certain judges and justices who have closely considered the implications of location technology have expressed concern, even anxiety, over the effects on society of the government's use of location technologies. Some of these jurists have further questioned the law's current ability to contain its effects and have found that ability, and hence their own powers, wanting. We share the jurists' skepticism. Cognizant of the power of the government's gaze and in agreement with Justice Alito's[234] and Judge Flaum's conclusion that the legislature is likely the branch of government best suited to fashion the appropriate protections against this gaze, we now present our model privacy framework for location information.

VI. LEGISLATIVE PROPOSAL

In an effort to try and bridge the gap between the currently polarized positions of privacy advocates and law enforcement, we offer a model privacy framework to govern law enforcement compelled disclosures of historical and prospective location information.[235] It is neither the most

231. *See supra* Section III.B.2.b.

232. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring). Furthermore, during the government's oral argument in *Jones*, shortly following Justice Breyer's stated concern over "what . . . a democratic society [would] look like if a large number of people did think that the government was tracking their every movement over long periods of time" and his search for a "reason and principle" that would "reject" this kind of government surveillance "but wouldn't also reject [government tracking] 24 hours a day for 28 days," Justice Scalia exclaimed, "Don't we have any legislatures out there that could stop this stuff?" Transcript of Oral Argument at 24–26, *Jones*, 132 S. Ct. 945 (2012) (No. 10-1259), *available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/10-1259.pdf.

233. *Id.* (citing Kerr, *supra* note 228, at 805–06).

234. Justice Ginsburg, Justice Breyer, and Justice Kagan all signed Justice Alito's concurrence regarding this conclusion.

235. We intend the privacy framework and access standards proposed in this Part only to apply to criminal law enforcement authorities. They are not intended to amend or affect intelligence or national security authorities that the government may use to acquire location information. The government's use of such intelligence tools is beyond the scope of this Article. Any actual legislation that seeks only to amend criminal law enforcement authorities would include appropriate statutory language to exempt relevant intelligence authorities.

friendly to law enforcement nor the most protective of privacy, but it is an attempt to find a reasonable balance among the interests of law enforcement, privacy, and industry.

Our proposal relies on several overarching principles that form a foundation for crafting the correct balance: a strong privacy framework that does not unduly limit law enforcement investigative activities or negatively affect industry innovation. These principles are influenced by a variety of sources including, but not limited to, ideas expressed by the DDP Coalition, off-the-record discussions with industry representatives, information revealed in public congressional hearings and elsewhere in the public record, and extensive discussions with private practitioners, academics, and privacy advocates.

A. OVERARCHING PRINCIPLES

1. Clear Rules

Law enforcement, judges, and industry all benefit from clear access standards.[236] When the ECPA was passed in 1986, location data was not a "routine tool" used by law enforcement and cell phones were a luxury affordable to only a small number of people. Congress, understandably, did not have the clairvoyance to foresee the explosion in wireless mobile devices. Nor did Congress anticipate the confusion[237] that would ensue due to the lack of any clear guidance in the ECPA in the form of standards governing law enforcement compelled disclosures for prospective location information.

In contrast to the uncertain, even chaotic, legal landscape that currently burdens the analysis of law enforcement access to location data, clear standards enable all stakeholders to execute their respective responsibilities certain in the knowledge that they are following the law. For prosecutors and agents, this means they can efficiently get access to location information because they won't have to "haggle" over the appropriate standard for access with certain judges. For magistrate judges, clear standards better enable them to ensure that the government follows the law in obtaining access to any location data. Moreover, industry can comply with the law without running

236. *See* Comments of CTIA—The Wireless Association, *supra* note 46, at 16 ("The lack of a consistent legal standard for tracking a user's location has made it difficult for carriers to comply with location demands."); *Senate Judiciary 2011 ECPA Hearing*, *supra* note 7, at 7 (testimony of James A. Baker, Assoc. Deputy Attorney Gen., U.S. Dep't of Justice); *Location Hearing*, *supra* note 19, at 85 (written statement of Judge Stephen Wm. Smith, U.S. Magistrate Judge).

237. *See supra* Part III.

the current risk of incurring liability for inappropriately disclosing customer information to the government.[238]

2. Technology Neutrality

In order for the ECPA to remain a "forward looking statute,"[239] even with respect to the next generation of smartphones, it is critical that law enforcement access standards do not depend on the precision and capabilities of particular location technologies, or with the general state of the industry at the time of drafting. There has been an explosion in the growth of location-based services over the past several years. During that time, the precision of the location information these technologies produce has increased dramatically, such that single cell tower data—particularly where enhanced by some of the 350,000 femtocells deployed around the country[240]—is becoming as accurate as GPS.[241] Indeed, the rapid pace of innovation, driven by market incentives to enhance the accuracy of location-based advertising, suggests that location information will continue to become increasingly precise.

A standard that is dependent on the precision of the location data requested creates an unstable, unworkable situation where, for example, certain magistrate judges feel compelled to examine deployment maps of cell towers or seek expert guidance to determine the precision of the location data produced in a particular district.[242] To foster clear rules that can be applied without undue confusion, ultimately leading to greater stability in the law, Congress should enact law enforcement access standards that are not dependent on the specific precision of location data.

3. Standards Alone Will Not Achieve the Appropriate Balance

Most of the privacy community's location information advocacy to date has focused on a "high" standard for law enforcement access. This focus has led to a stalemate with much of the law enforcement community and has put powerful members of Congress "on guard" to protect law enforcement equities. Regardless of the standard required for law enforcement access to

238. *See generally* Albert Gidari, Jr., *Companies Caught in the Middle*, 41 U.S.F. L. REV. 535 (2007).

239. *See House Judiciary 2010 ECPA Reform Hearing*, *supra* note 18, at 10 (written statement of James X. Dempsey, Vice President of Pub. Policy, Ctr. for Democracy & Tech.).

240. *See* Press Release, Informa Telecoms & Media, *supra* note 27.

241. *See In re 2010 S.D. Tex. Application*, 747 F. Supp. 2d 827, 834 (S.D. Tex. 2010) ("As cellular network technology evolves, the traditional distinction between 'high accuracy' GPS tracking and 'low accuracy' cell site tracking is increasingly obsolete, and will soon be effectively meaningless."); *see also supra* Section II.F.

242. *See supra* Sections III.A.2, III.A.3.

location data, there are some privacy concerns that can only be addressed through post collection process and rules, such as data minimization, subscriber notification, and statistical reporting. A regime of reasonable access standards combined with downstream privacy protections seems to present the best way forward.

4. Insistence on a Single Location Standard Is a "A Foolish Consistency"[243]

As stated in the Introduction, this proposal is not the most privacy protective, the least burdensome to industry, or the most law enforcement friendly. Rather, it is an attempt to eliminate the uncertainty and instability currently plaguing the law and to achieve a balance of equities that is more palatable insofar as it improves the positions of each of these stakeholders in some appreciable way. The process of passing legislation is largely about compromise. As a result, the "right" and politically feasible policy balance may not always create a perfectly "consistent" set of law enforcement access standards or privacy protections, if consistency is to be read as mere verbal or structural symmetry for its own sake.

Some privacy scholars have argued that the law, as a matter of policy, should treat historical and prospective location data the same, specifically calling for a justification for treating them anything other than the same.[244] Such an approach, however, would be a significant departure from existing statutory surveillance law, which has traditionally treated historical (stored) and prospective (real time) information differently, requiring more process when the government compels real time information.[245] Insistence upon a

243. "A foolish consistency is the hobgoblin of little minds, adored by little statesmen and philosophers and divines." Ralph Waldo Emerson, *Self Reliance*, *in* 2 THE COLLECTED WORKS OF RALPH W. EMERSON: ESSAYS: FIRST SERIES 33 (Joseph Slater et al. eds., 1979) (1841).

244. At the 2011 Privacy Law Scholars Conference, co-sponsored by the law schools at the University of California, Berkeley and The George Washington University, the authors workshopped a draft of this Article. Several privacy scholars and members of the privacy community questioned our justification for treating stored location information differently from real time location data, advocating for a standard that would require a warrant for all location data.

245. For example, the government can use a subpoena to obtain stored telephone toll records, *see* 18 U.S.C. § 2703(c)(2) (2010), but must get a Pen/Trap order from a court to obtain the same information in real time, *see id.* § 3121. In order to obtain the content of e-mails in real time, the government must meet higher hurdles of a wiretap "super" warrant, which requires a court to find that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous," *id.* § 2518(c), in addition to several other "probable cause" requirements, *see id.* § 2518 (a)–(b), (d). On the other hand, the government can get stored e-mail content by meeting the standard Rule 41 "probable cause" showing, or less. *See* § 2703(a)–(b); *see also Location Hearing*, *supra*

standard that is "consistent" in the sense only of being identically applied to this distinction would serve only to polarize the legislative process to the point of collapse. Law enforcement will predictably retreat to one corner in order to demonstrate how a probable cause standard for all location data would unduly limit investigative activities[246] while privacy advocates will just as predictably withdraw support for any legislation that authorizes law enforcement to compel all location information with a unitary standard lower than probable cause. Empathy is lost. Synthesis is precluded. This familiar impasse, which has become the norm in our recent political life, is here the fruit of a foolish consistency that would level a long-held distinction between two categories of data and, in doing so, likely derail a legislative balancing process that could improve the position of all stakeholders when measured against the current state of the law.

As a matter of legislative strategy then, mandating a single standard for the sake of this leveling form of consistency has risks. Such consistency can, of course, cut both ways: it would be equally consistent to allow law enforcement access to all location data with either a probable cause warrant or a D Order. Indeed, consistency for its own sake, argued in either direction, is a reductive, polarizing position that short-circuits any legislative effort to harmonize the competing policy interests of the privacy and law enforcement communities.

B. How To Define Location Information for Purposes of Amending the ECPA

There are many data forms that reveal an individual's location and that law enforcement can compel from third-party providers. These sources include wireless phone carriers and smartphone platform vendors (such as Apple and Google). Location information can also be discerned through transactional records, such as tollbooth, public transport, and credit card records.[247] Law enforcement agencies can also obtain location information directly, without going to third parties, by intercepting wireless phone signals

note 19, at 82 (written statement of Judge Stephen Wm. Smith) (explaining levels of privacy protection given to different surveillance authorities).

246. *See supra* Section IV.B.

247. *See* Ryan Singel, *Feds Warrantlessly Tracking Americans' Credit Cards in Real Time*, WIRED (Dec. 2, 2010), http://www.wired.com/threatlevel/2010/12/realtime/ ("Federal law enforcement agencies have been tracking Americans in real-time using credit cards, loyalty cards and travel reservations without getting a court order, a new document released under a government sunshine request shows. . . . [S]o-called 'Hotwatch' orders allow for real-time tracking of individuals in a criminal investigation via credit card companies, rental car agencies, calling cards, and even grocery store loyalty programs.").

using a Triggerfish, Stingray, or other similar tracking technologies,[248] or by covertly installing a GPS tracking device under a car. While law enforcement's access to these sources of data all raise legitimate privacy concerns, this Article focuses on the compelled disclosure of location information from communications carriers, such as mobile phone services. Congress can, and should, look into other forms of location surveillance, but they remain beyond the scope of this Article. Our proposed standard, directed at third-party communication carriers, begins with the following statutory definitions:

> An "electronic location service" ("ELS") is any service which possesses location information about a customer, subscriber, or user.
>
> "Location information" ("LI") is any information derived or otherwise calculated from the transmission or reception of a radio signal that reveals the approximate or actual geographic location of a customer, subscriber, or user.[249]
>
> "Historical location information" is location information that existed prior to the issuance of an order.
>
> "Current or prospective location information" is location information that comes into existence after a court order for disclosure of that information is issued.

---

248. *Cell Site Simulators, Triggerfish, Cell Phones* (last updated Feb. 23, 2007), *in* U.S. Dep't of Justice, Response to Freedom of Information Act Request No. 07-4130 re: Mobile Phone Tracking 18 (Aug. 12, 2008), *available at* http://www.aclu.org/pdfs/freespeech/cellfoia_release_074130_20080812.pdf (stating that Triggerfish can be deployed "without the user knowing about it, and without involving the cell phone provider"); Julian Sanchez, *FOIA Docs Show Feds Can Lojack Mobiles Without Telco Help*, ARS TECHNICA (Nov. 16, 2008), http://arstechnica.com/tech-policy/news/2008/11/foia-docs-show-feds-can-lojack-mobiles-without-telco-help.ars ("The Justice Department's electronic surveillance manual explicitly suggests that triggerfish may be used to avoid restrictions in statutes like CALEA that bar the use of pen register or trap-and-trace devices—which allow tracking of incoming and outgoing calls from a phone subject to much less stringent evidentiary standards—to gather location data."); *see also* Jennifer Valentino-DeVries, *'Stingray' Phone Tracker Fuels Constitutional Clash*, WALL ST. J. (Sept. 22, 2011), http://on.wsj.com/1hMb7d.

249. "Radio" refers to the radio frequency ("RF") portion of the electromagnetic spectrum, which is "generally defined as that part of the spectrum where electromagnetic waves have frequencies in the range of about 3 kilohertz [3000 hertz] to 300 gigahertz." FED. COMMC'NS COMM'N, BULLETIN NO. 56, QUESTIONS AND ANSWERS ABOUT BIOLOGICAL EFFECTS AND POTENTIAL HAZARDS OF RADIOFREQUENCY ELECTROMAGNETIC FIELDS 2–3 (4th ed., 1999), *available at* http://www.fcc.gov/Bureaus/Engineering_Technology/Documents/bulletins/oet56/oet56e4.pdf; *see also Radio*, MERRIAM-WEBSTER DICTIONARY ONLINE, http://www.merriamwebster.com/dictionary/radio (last visited Mar. 19, 2012) (defining radio as "of or relating to electric currents or phenomena (as electromagnetic radiation) of frequencies between about 3000 hertz and 300 gigahertz").

C. A STANDARD FOR LAW ENFORCEMENT COMPELLED DISCLOSURES OF HISTORICAL LOCATION DATA

Our proposed law enforcement access standard for historical location information is built around the current D Order standard with the addition of an element specifically requiring courts to examine whether the scope of the request is reasonable in light of the criminal activity being investigated. We have previously discussed certain examples of scope permutations in investigations[250]—it would be useless to try and define all of them in advance. A discussion of how Congress generally views the scope inquiry could also be developed in legislative history. A court, when applying the standard, will focus the scope of its inquiry on issues raised (and perhaps resolved) by the specific facts presented by the government in its application for a D Order. This standard could be drafted as follows:

> (a) DISCLOSURE UPON COURT ORDER.—Except as provided in paragraph (3), a provider of an electronic location service shall provide historical location information to a governmental entity only if the governmental entity obtains a court order issued by any court of competent jurisdiction establishing—
>
> > (1) specific and articulable facts showing that there are reasonable grounds to believe that the location information requested is relevant and material to an ongoing criminal investigation; and
> >
> > (2) specific and articulable facts showing that a reasonable and sufficient nexus exists between the alleged or suspected criminal activity described in paragraph (1) and the scope of the location data requested.
> >
> > (3) PERMITTED DISCLOSURES WITHOUT COURT ORDER.—A provider of an electronic location service may disclose historical location information with—
> >
> > > (A) the express consent of the customer, subscriber, or the user of the equipment concerned; or
> > >
> > > (B) as otherwise authorized in 18 U.S.C. § 2702(c)(3)–(6).

By maintaining the "relevant and material" language, our standard preserves law enforcement equities while limiting the unnecessary over-collection of historical location information by requiring courts specifically to approve the scope of a request. Moreover, this standard "forces" the government to articulate how the scope of the request is reasonable in light of the particular

250. *See supra* Section III.C.1.

facts and needs of the investigation.[251] We hope that this type of balancing can foster a compromise between privacy advocates and law enforcement insofar as it does not raise the historical data access standard up to probable cause that would unduly limit law enforcement in the early stages of an investigation, but it does require written justification and court approval for the scope of the request.

This standard also maintains the exceptions for disclosure of non-content records already present in the ECPA, including emergencies involving danger of death or serious physical injury.[252] Finally, this proposed language clearly establishes the standard the government must meet before obtaining access to historical location data, a change that benefits all stakeholders.

D. A STANDARD FOR LAW ENFORCEMENT COMPELLED DISCLOSURES OF PROSPECTIVE LOCATION DATA

Our proposed standard for prospective location information requires a probable cause showing. We expand the categories of that showing, however, to accommodate common, legitimate law enforcement uses of prospective location data, including location information pertaining to a person who has committed, is committing, or is about to commit a felony offense or is a victim of that offense.

The DOJ has acknowledged that, as a matter of policy, it already advises prosecutors and agents to obtain a probable cause warrant for GPS or similarly precise location information.[253] Our standard not only codifies the DOJ's existing practice regarding GPS and similarly precise location data but also requires a probable cause showing (based on the expanded categories) for all prospective location data. Insofar as single cell site data can now be as precise as GPS location information—and such precision will only continue to increase over time—drawing distinctions in the law based upon data precision is no longer logical or workable.[254]

---

251. Indeed, in Stephanie's experience as a federal prosecutor, when a standard calls for this type of explanation, prosecutors and agents are much more likely to tailor applications narrowly at the outset, in anticipation of court scrutiny.

252. One of the current ECPA exceptions, 18 U.S.C. § 2702(c)(6) (2010), puts no limits on providers sharing non-content information with third parties who are not law enforcement. In recent testimony, the DOJ has suggested that it may be appropriate for Congress to consider restricting disclosures of personal information by service providers. *See Senate Judiciary 2011 ECPA Hearing*, *supra* note 7, at 10 (testimony of James A. Baker, Assoc. Deputy Attorney Gen., U.S. Dep't of Justice). Insofar as this Article focuses on law enforcement access issues, it is beyond the scope of this Article to address this issue.

253. *See Senate Judiciary 2011 ECPA Hearing*, *supra* note 7, at 7 (testimony of James A. Baker).

254. *See supra* Sections III.A.1, III.B.1, III.C.1, IV.B; *see also Location Hearing*, *supra* note 19, at 85 (written statement of Judge Stephen Wm. Smith).

With the expansion of the categories of probable cause, we have once again attempted to accommodate law enforcement investigative needs[255] in order to foster a compromise between law enforcement and privacy advocates. This standard could be drafted as follows:

> (1) DISCLOSURE UPON COURT ORDER FOR A PERIOD NOT TO EXCEED 30 DAYS.—Except as provided in paragraph (2), a provider of an electronic location service shall provide a governmental entity current or prospective location information about a customer, subscriber, or user only if the governmental entity obtains a court order from any court of competent jurisdiction issued upon a finding that there is probable cause to believe that—
>
> (A) the information sought is evidence of a crime; or
>
> (B) a person is committing, has committed, or is about to commit a felony offense or is a victim of that offense; and the location information sought to be obtained concerns the location of the person believed to have committed, be committing, or be about to commit that offense or a victim of that offense.
>
> (2) PERMITTED DISCLOSURES WITHOUT COURT ORDER.—A provider of an electronic location service may provide the information described in paragraph (1)—
>
> (A) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services;
>
> (B) with the express consent of the customer, subscriber, or the user of the equipment concerned; or
>
> (C) as otherwise authorized in 18 U.S.C. § 2702(c)(3)–(6).
>
> (3) DEFINITION.—The term "public safety answering point" means a facility that has been designated to receive emergency calls and route them to emergency service personnel.
>
> (4) EXTENSIONS.—Extensions of such an order may be granted for up to 30 days upon a probable cause showing as defined in sections (A)–(B) of paragraph (1) of this provision.

This statutory language is not from the ECPA reform hearings of 2010–2011.[256] Rather, it is adopted from a bill, entitled the "Electronic Communications Privacy Act of 2000," reported out favorably by a

255. *See supra* Section III.C.

256. *See* discussion *supra* Parts I, IV.

Republican-controlled House Judiciary Committee. The bill never became law, but it applied the "expanded" probable cause standard to prospective location information.[257] These expanded probable cause standards address situations where, for example, law enforcement may have probable cause to believe someone has committed a crime yet the suspect's current or prospective location information may not itself be evidence of a crime.[258]

Consistent with other real-time surveillance authorities like Pen/Trap and the Wiretap Act, our proposal affords prospective location information a higher degree of privacy protection than that given to previously stored information.[259] Also mirroring the Wiretap Act,[260] our proposal places a time limit of thirty days for each individual order, without preventing the government from returning to a court for an extension. This standard also includes specific exceptions to allow for the operation of the E-911 system[261] while incorporating all of the exceptions for non-content information already present in the ECPA. Finally, this proposed language clearly establishes a standard the government must meet before getting access to prospective location data, a change that again benefits all stakeholders.

E. POST ACCESS RULES AND "DOWNSTREAM" PRIVACY PROTECTIONS

It is obviously important for Congress to select the right legal standard required for law enforcement to obtain location data. Equally important to an overall privacy framework, however, are rules regarding the retention of the data once it is acquired, notice to individuals whose information has been acquired by law enforcement, and reporting requirements to Congress.[262] Indeed, such "downstream" protections can offset any over-collection of information by law enforcement during the course of an investigation. This Section proposes three specific methods to protect privacy following the

257. *See* H.R. 5018, 106th Cong. § 6(a) (2000).

258. *See supra* Section III.C.2.

259. *See* discussion *supra* note 245 and accompanying text.

260. 18 U.S.C. § 2518(5) (2010).

261. *Location Hearing*, *supra* note 19, at 36 (statement of Michael Amarosa, Sr. Vice President for Public Affairs, TruePosition Inc.) (describing the FCC E-911 requirement).

262. *See* Orin S. Kerr, *Use Restrictions and the Future of Surveillance Law*, FUTURE CONST. (Brookings Inst., Washington, D.C.), Apr. 19, 2011, *available at* http://www.brookings.edu/papers/2011/0419_surveillance_laws_kerr.aspx ("[T]he law should still regulate the collection of evidence. But surveillance law shouldn't end there. The shift to computerization requires renewed attention on regulating the use and disclosure of information, not just its collection.").

disclosure of location information to law enforcement: minimization, notification, and congressional oversight through statistical reporting.[263]

1. Minimization

Given the large amount of data that law enforcement agencies now obtain via location requests and the number of innocent people whose information may be obtained through community of interest requests or requests associated with a specific place, we believe that minimization rules can and should play a role in limiting the privacy harms associated with such data collection. These minimization rules would focus on removing irrelevant location data from law enforcement databases at a time appropriate to the particular investigation or case. Minimization requirements are not a new idea. They already play a privacy protective role in several other surveillance statutes, including the Wiretap Act,[264] the USA PATRIOT Improvement and Reauthorization Act of 2005 ("PATRIOT Act"),[265] and the Foreign Intelligence Surveillance Act ("FISA").[266]

Although Congress has frequently enacted minimization requirements, it has never legislated the specific details of how such minimization would work with respect to particular surveillance authorities or investigations. In both the Wiretap Act and FISA, government lawyers submit minimization protocols as part of their applications, which are then approved by a judge and included in the court order. Likewise, in the PATRIOT Act, Congress directed the DOJ to adopt specific minimization procedures for records

263. There are other types of downstream privacy protections that could and perhaps should eventually be included in a privacy framework—e.g., the unsealing of court orders with appropriate redactions at a time when such unsealing would no longer jeopardize an investigation or place individuals involved in it at risk. *See, e.g.*, Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3 FED. CTS. L. REV. 177 (2009) (arguing that the overabundant, indefinite sealing of certain types of judicial orders undermines the legitimacy of those decisions). For the purpose of making good policy, unsealing, whether after a specified period or after specific conditions have been met, could facilitate greater transparency and provide Congress with better information about how the government uses and courts apply surveillance authorities. Notwithstanding the potential utility of such a policy, however, we believe that the unsealing of court records raises serious security and privacy issues that require a complex and lengthy analysis that is beyond both the scope of ECPA reform and this Article.

264. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 for the first time authorized law enforcement personnel to monitor private telephone conversations. Pub. L. No. 90-351, tit. III, 92 Stat. 197, 211–25 (codified as amended at 18 U.S.C. §§ 2511–2520 (2010)). The Act also provided strict guidelines and limitations on the use of wiretaps as a barrier to government infringement of individual privacy. One of the protections included by Congress was the minimization requirement of 18 U.S.C. § 2518(5).

265. 50 U.S.C. § 1861(g) (2009).

266. *Id.* § 1804(a)(5).

obtained pursuant to Section 215 orders. Section 215 is a national security collection authority that allows the government to obtain both content and non-content information.[267]

As such, we propose that Congress should require the DOJ, in consultation with State Attorneys General, to develop rules and procedures for the minimization of location information. Such rules would be intended to prevent the retention of information that is not relevant to reasonable law enforcement purposes. Statutory language could be drafted as follows:

> The Attorney General, in consultation with State Attorneys General, shall adopt specific minimization procedures governing the retention and dissemination by governmental entities of location information received in response to an order under this section.
>
> In this section, the term "minimization procedures" means specific procedures, reasonably designed in light of the form and purpose of an order for the production of location information, to minimize the retention and prohibit the dissemination of non-publicly available location information concerning non-consenting persons, consistent with the need of law enforcement to obtain, retain, produce, and disseminate information that: 1) is evidence of a crime; or 2) concerns the location of a person who is committing, has committed, is about to commit, or is a victim of a felony offense; or 3) is otherwise relevant and material to an ongoing criminal investigation and to be retained or disseminated for law enforcement purposes.

This language gives the Attorney General, in conjunction with the State Attorneys General, the flexibility and discretion to design minimization rules and procedures consistent with law enforcement needs while minimizing the retention and dissemination of location data that is not or is no longer relevant to legitimate law enforcement purposes.

2. Notification

Covert surveillance methods are investigative tools that by their very nature invade the privacy of those targeted and are, as history has shown, prone to abuse.[268] To ensure these surveillance powers are restricted to

---

267. Section 1861 of Title 50, commonly referred to as "Section 215 Business Records," permits the government to obtain, with a FISA court order, any "tangible thing" for certain types of national security investigations. Such Section 215 minimization procedures were intended to minimize the retention and prohibit the dissemination of non-publicly available information concerning United States persons consistent with national security interests. *See* § 1861(g).

268. *See* Julian Sanchez, *Wiretapping's True Danger*, L.A. TIMES (Mar. 16, 2008), http://articles.latimes.com/2008/mar/16/opinion/op-sanchez16 ("Without meaningful oversight, presidents and intelligence agencies can—and repeatedly have—abused their surveillance

legitimate law enforcement investigative needs, surveillance of innocent persons should be limited whenever possible and, whenever employed, it should not remain secret indefinitely. Such transparency facilitates social and congressional oversight of government use of surveillance techniques: individuals who may have been inappropriately or illegally monitored are provided with information and resulting incentives that may motivate them to pursue personal remedies, such as placing facts about the surveillance in the public record. Indeed, a disclosure mechanism that will raise public awareness of, and stimulate public discourse about, the scope and frequency of government surveillance activities may serve as an important deterrent to gratuitous use or abuse of these powers.

In both the Wiretap Act and the Stored Communications Act, Congress created mandatory notice requirements that guarantee that subjects of some forms of law enforcement surveillance would be told that their communications have been intercepted or accessed.[269] Such notice provisions act as an important privacy protection that particularly benefits those who are subjects of surveillance but never charged with a crime. While those who are eventually arrested and charged might otherwise learn that they have been the target of surveillance (through the disclosure of search warrants, affidavits, and other documents), those who are not charged would never know about their surveillance histories were it not for the existence of notice requirements in existing surveillance laws.

We propose a similar notice requirement for those individuals whose location information is obtained by law enforcement agencies. This requirement will apply to those individuals targeted in location orders, as well

authority to spy on political enemies and dissenters. . . . [A] thorough congressional investigation headed by Sen. Frank Church (D-Idaho) revealed that for decades, intelligence analysts—and the presidents they served—had spied on the letters and phone conversations of union chiefs, civil rights leaders, journalists, antiwar activists, lobbyists, members of Congress, Supreme Court justices—even Eleanor Roosevelt and the Rev. Martin Luther King Jr. The Church Committee reports painstakingly documented how the information obtained was often 'collected and disseminated in order to serve the purely political interests of an intelligence agency or the administration, and to influence social policy and political action.' ").

269. *See* 18 U.S.C. § 2518(8)(d) (Wiretap Act notifications) and §§ 2703(b)(1)(B), 2705 (ECPA notifications). ECPA notifications only apply to the disclosure of content (not non-content) and then only when a § 2703(d) order or subpoena is used to compel content. If using a Rule 41 warrant to compel content, at least one court held that the government only has to notify the service provider, not the customer or subscriber. *In re* Application for Warrant for E-mail Account [redacted]@gmail.com Maintained on Computer Servers Operated by Google, Inc., Headquartered at 1600 Amphitheater Parkway, Mountain View, CA, Mag. No. 10-291-M-01 (D.D.C. Nov. 1, 2010) (Lamberth, J.), *available at* http://www.dcd.uscourts.gov/dcd/sites/dcd/files/mag10-291.pdf.

as innocent individuals whose information may be obtained as part of disclosures associated with specific places or community of interest requests. In addition to facilitating transparency and providing notice to impacted individuals, this requirement will, similar to existing compensation requirements,[270] discourage law enforcement agencies from making unnecessary requests for large amounts of data,[271] as the cost of notifying 200 people will presumably be greater than that of notifying only twenty. This requirement could be drafted as follows:

(a) NOTIFICATION.—

(1) Within 90 days after the disclosure of historical location information, or the expiration of an order authorizing prospective location information, the governmental entity shall serve upon, or deliver by appropriate means,[272] the customer, subscriber, or user whose location was disclosed with notice that—

(A) states with reasonable specificity the nature of the law enforcement inquiry; and

(B) informs such customer, subscriber, or user that their location information was supplied to that governmental authority, and the date on which such disclosure was made.

(2) Extensions of the delay of notification of up to 90 days each shall be granted by the court upon application by a governmental entity if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (3) of this subsection.

(3) An adverse result for the purposes of paragraph (2) of this subsection is—

---

270. *See House Judiciary 2010 ECPA Reform Hearing*, *supra* note 18, at 32 (written statement of Albert Gidari, Perkins Coie LLP) ("When records are 'free,' such as with phone records, law enforcement over-consumes with abandon. . . . But when service providers charge for extracting data, such as log file searches, law enforcement requests are more tailored.").

271. William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 GEO. WASH. L. REV. 1265, 1275 (1999) ("[I]f you tax a given kind of [law enforcement] behavior, you will probably see less of it.").

272. Due to the widespread popularity of prepaid phones, many communications carriers do not have a name or address on file for large numbers of their customers. As a result, it would not be possible for the carriers to notify these customers via U.S. mail (something required for surveillance of internet communications content performed under 18 U.S.C. § 2705(a)(5)). The use of the term "appropriate means" is designed to enable companies to notify their customers via a communication medium that is appropriate to the service they offer, and the contact information they have on file. This could include, for example, email, or mobile text message ("SMS").

> (A) endangering the life or physical safety of an individual;
>
> (B) flight from prosecution;
>
> (C) destruction of or tampering with evidence;
>
> (D) intimidation of potential witnesses; or
>
> (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.
>
> (b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS.—A governmental entity acting under section [x] may apply to a court for an order commanding a provider of an electronic location service to whom a court order issued under section [x] is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the court order will result in—
>
> (1) endangering the life or physical safety of an individual;
>
> (2) flight from prosecution;
>
> (3) destruction of or tampering with evidence;
>
> (4) intimidation of potential witnesses; or
>
> (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

This section requires the law enforcement agency to notify all persons whose location information it obtains within ninety days after either the disclosure of historical data or the end of prospective surveillance. Individuals shall be notified via "appropriate" means, which could be a series of text messages, an email, or a letter, depending on the contact information known to law enforcement. As with other notification statutes, the proposed section also permits the government to seek further delay of notice with cause, as well as prohibit a location provider from telling a target that her location information has been disclosed. When notifying innocent third parties that their location information was disclosed (incidentally) as part of a "broad" authorization, the governmental entity making the notification should consider language that communicates the benign nature of the disclosure.

3. Surveillance Statistics

When Congress created both the wiretap and pen register/trap and trace interception statutes, it mandated the annual publication of aggregate

statistical reports[273] that were "intended to form the basis for a public evaluation of [the statute's] operation [and] will assure the community that the system of court-ordered electronic surveillance . . . is properly administered."[274] Since at least 1998, the Administrative Office of the United States Courts ("AO") has made copies of these reports available to the general public via its website.[275] The public release of the annual report usually leads to media coverage highlighting the increased use of wiretaps.[276]

These statistics also provide a rich source of information for scholars wishing to study and report on the ever-increasing use of electronic surveillance.[277] By comparing these reports, scholars have been able to observe several notable surveillance trends. These include that the majority of wiretaps are for drug crimes;[278] that courts rarely, if ever, refuse wiretap applications;[279] that the vast majority of wiretaps target mobile phones;[280] and the ever-growing use of wiretaps by state law enforcement agencies.[281]

---

273. *See supra* note 171.

274. S. REP. NO. 90-1097, at 69 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2185, *and available at* 1968 WL 4956, at *2185.

275. *See, e.g.*, ADMIN. OFFICE OF THE U.S. COURTS, 1997 WIRETAP REPORT (1998), http://web.archive.org/web/19981206135425/www.uscourts.gov/wiretap/contents.html.

276. *See, e.g.*, *National News Briefs; Record Total of Wiretaps Was Approved by Courts*, N.Y. TIMES (May 10, 1998), http://nyti.ms/IhNhQj; Susan Stellin, *Compressed Data; Who's Watching? No, Who's Listening In?*, N.Y. TIMES (June 3, 2002), http://nyti.ms/IhNp2d; Ryan Singel, *Police Wiretapping Jumps 26 Percent*, WIRED (Apr. 30, 2010), http://www.wired.com/threatlevel/2010/04/wiretapping/.

277. *See Cloud Based Computing Hearing*, *supra* note 165, at 130 (oral answer from Fred Cate, Prof. and Director, Ctr. for Applied Cybersecurity Research, Ind. Univ., to Chairman Nadler) ("[Surveillance] statistics gives Congress a sound empirical basis on which to evaluate how its laws are being used and whether they need to be changed. It also provides that same information for people such as those of us gathered at this table when making recommendations to Congress. And it provides information to the public and the press so that they know how those laws are being used and to what effect."); *see also* Soghoian, *supra* note 170.

278. Soghoian, *supra* note 170, at 9 ("[M]ore than 86 percent of the 2306 wiretap orders obtained [in 2009] by federal and state law enforcement agencies were sought in narcotics investigations.").

279. *See id.* at 6–7 ("Between 1987 and 2009, law enforcement agencies requested over 30,000 wiretap orders. . . . During the more than 20 years for which public data exists, requests for wiretap orders have been rejected just 7 times, twice in 1998, once in 1996, twice in 1998, once in 2002 and once in 2005.").

280. *See id.* at 7 ("96 percent (2,276 wiretaps) of all authorized wiretap for 2009 are for portable devices.").

281. *See id.* at 12 ("Over the last decade, the use of electronic surveillance orders has increased nationwide, although this is largely due to a massive increase in use by the states . . . . [California and New York] are now responsible for a combined 58 percent of all state wiretap orders.").

While much is known about the scale and use of wiretaps and, to a lesser extent, Pen/Trap surveillance, law enforcement requests for location information are largely a "known unknown."[282] Wireless companies and their representatives have provided, at best, a partial picture whose details emerge only through Freedom of Information Act requests and other investigative reporting techniques by privacy advocates.[283] That picture is not sufficiently clear to guide Congress regarding the use of this surveillance technique.[284] To remedy this deficiency, we propose a specific reporting requirement that will enable Congress to know as much about the state of location surveillance as it currently knows about wiretaps and would, as Senator Patrick Leahy has described, provide a "far more reliable basis than anecdotal evidence on which to assess law enforcement needs and make sensible policy in this area."[285] This standard could be drafted as follows:

> (a) GENERAL RULEMAKING AUTHORITY FOR REPORTS UNDER THIS SECTION.—The Director of the Administrative Office of the United States Courts may make rules regarding the content and form of the reports required under this section.
>
> (b) REPORTS CONCERNING DISCLOSURES.—
>
> (1) TO ADMINISTRATIVE OFFICE.—Not later than 30 days after the issuance or denial of an order under this chapter compelling the disclosure of location information, the issuing or denying judge shall report to the Administrative Office of the United States Courts—
>
> (A) the fact that an order was applied for;
>
> (B) the type of order applied for;
>
> (C) whether the order was granted as applied for, was modified, or was denied;
>
> (D) whether the court also granted delayed notice and the number of times such delay was granted;
>
> (E) the offense specified in the order or application, or extension of an order;

---

282. News Transcript, U.S. Dep't of Defense, DoD News Briefing—Secretary Rumsfeld and Gen. Myers (Feb. 12, 2002), *available at* http://www.defense.gov/transcripts/transcript.aspx?transcriptid=2636 ("[T]here are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know."); *see also supra* Part I (discussing details about what is known regarding the scale of location surveillance).

283. *See generally* Soghoian, *supra* note 170.

284. *Id.*

285. 145 CONG. REC. 31,311 (1999) (statement of Sen. Leahy).

(F) the identity, including district where applicable, of the applying investigative or law enforcement agency making the application and the person authorizing the application; and

(G) the type of information or records sought in the order.

(2) TO CONGRESS.—In April of each year the Director of the Administrative Office of the United States Courts shall report to Congress with respect to the preceding calendar year—

(A) the overall total number of each of the events described in the subparagraphs of paragraph (1), regarding applications reported to that Office; and

(B) a summary and analysis of the data described in paragraph (1).

(c) PROVIDER REPORTING REQUIREMENTS.—

(1) TO ADMINISTRATIVE OFFICE.—Except as provided in paragraph (2), in January of each year each provider of an electronic location service shall report with respect to the preceding calendar year to the Administrative Office of the United States Courts—

(A) the number of legal demands and emergency requests received from Federal law enforcement agencies during the preceding calendar year for location information;

(B) the number of legal demands and emergency requests received from State, local, and tribal law enforcement agencies during the preceding calendar for location information; and

(C) the number of accounts about which location information was disclosed, specifying the numbers disclosed pursuant to legal demand and the numbers disclosed voluntarily, to Federal, State, local, or tribal law enforcement agencies.

(2) EXCEPTIONS.—The requirement of paragraph (1) does not apply to a provider of an electronic location service that, during the reporting period—

(A) received fewer than 50 requests combined from law enforcement agencies; or

(B) disclosed account information concerning fewer than 100 subscribers, customers, or other users; or

(C) had fewer than 100,000 total customers or subscribers at the end of the calendar year.[286]

---

286. The purpose of these statistics is to provide Congress, scholars, and the general public with information necessary to determine the scale of surveillance and to observe

(3) COMPENSATION.—The Director of the Administrative Office of the United States Courts shall provide reasonable compensation to a provider for the costs of compiling a report required under this subsection.[287]

(4) CONFIDENTIALITY OF IDENTITY OF SERVICE PROVIDERS.—The Director of the Administrative Office of the United States Courts shall establish procedures to prevent the release to the public of the identity of service providers with respect to disclosures they make under this subsection.[288]

(5) TO CONGRESS.—In April of each year, the Director of the Administrative Office of the United States Courts shall report to Congress with respect to the preceding calendar year—

(A) the total numbers of legal demands and of disclosures required to be reported under paragraph (1); and

(B) a summary and analysis of the information required to be reported by paragraph (1), but without disclosing the identity of any service

---

general trends. Information from small providers who receive just a handful of requests per year will not significantly aid in the ability to observe such trends, in comparison to the tens of thousands of requests received by large providers. Furthermore, this notice requirement, while modest, could still be quite burdensome for a small provider. It is for this reason that we have opted to exempt such providers from the statistical reporting requirements.

287. As a general rule, companies are not in favor of regulations that are costly to comply with. Although we do not believe that the cost of compiling and submitting these reports will be exceedingly expensive (particularly given that Google already provides some data voluntarily), we have included a compensation provision to avoid giving companies a reason to lobby against it. We believe that the data that will be made public as a result of this provision is worth the modest cost to the taxpayer.

288. Although most large internet and telecommunications companies that handle user data receive both compulsory and voluntary location data requests from the government, few like to discuss the topic publicly. As such, many companies might vigorously oppose this statistical reporting requirement if it would mean that their names would be associated with the data that eventually becomes published. In order to respond to companies' concerns, this provision has been drafted to ensure that identities of the companies will remain confidential: only aggregate statistics will be published. In March 2010, Microsoft Associate General Counsel Mike Hintze told a reporter at *Wired* that the reason Microsoft does not publish statistical data regarding the number of legal requests the company receives for customer information is due to the fear of negative publicity. "We would like to see more transparency across the industry," Hintze said. "But no one company wants to stick its head up to talk about numbers." Ryan Singel, *Google, Microsoft Push Feds To Fix Privacy Laws*, WIRED (Mar. 30, 2010), http://www.wired.com/threatlevel/2010/03/google-microsoft-ecpa/; *see also* Letter from Michael T. Gershberg, Counsel to Yahoo! Inc, to William Bordley, FOIPA Officer, U.S. Marshals Serv. 9 (Sept. 15, 2009), *available at* http://cryptome.org/yahoo-price-list-letter.pdf ("[Surveillance pricing] information, if disclosed, would be used to 'shame' Yahoo! and other companies—and to 'shock' their customers. Therefore, release of Yahoo!'s information is reasonably likely to lead to impairment of its reputation for protection of user privacy and security, which is a competitive disadvantage for technology companies.").

provider with respect to the disclosures to law enforcement that service provider made.

This section creates a new statistical surveillance report for Congress that documents the issuance of orders compelling the disclosure of location information. The AO[289] will compile the annual report based on information submitted to it by judges who have issued orders in response to government applications to compel location information. The AO will then submit the compiled information in a report to Congress. This section also requires providers of an electronic location service (other than those falling below a *de minimis* threshold) to submit annual reports regarding the number of compelled and voluntary disclosures of location information they have made to the AO.[290] The AO will then compile the data collected, produce a statistical summary containing no reference to the names of individual providers, and submit the information in a report to Congress.

VII. CONCLUSION

The use of location information by law enforcement agencies is common and is becoming more so as technology improves and produces more accurate and precise location data. The legal mystery surrounding the proper law enforcement access standard for prospective location data remains unsolved and has created, along with conflicting rulings over the appropriate law enforcement access standard for both prospective and historical location data, a messy, inconsistent legal landscape where even judges in the same district may require law enforcement to meet different standards before authorizing law enforcement to compel location data. As courts struggle with these intertwined technology, privacy, and legal issues, some judges are expressing concern over the scope of the harms, from specific and personal to general and social, presented by unfettered government collection and use of location data.

289. The AO is the preferred entity to manage and execute this task because it is an objective, neutral organization and because it has historically produced the annual Wiretap Report (part of the Omnibus Crime Control and Safe Streets Act of 1968) in an accurate, timely manner. *See* 145 CONG. REC. 31,311 (1999) (statement of Sen. Leahy) ("The AO has done an excellent job of preparing the wiretap reports."). Placing the reporting burden with the AO also prevents law enforcement from complaining that the reporting requirements are turning "crimefighters into bookkeepers." *House Judiciary 2000 ECPA Hearing*, *supra* note 175, at 39 (statement of Kevin DiGregory, Deputy Assoc. Attorney Gen., Dep't of Justice).

290. The AO is only capable of compiling information on court orders for location information. Statistical data for voluntary disclosures made in emergencies can only come from the providers or law enforcement, and so we have opted to place this burden on the providers, who are then compensated for their trouble.

This Article proposes model law enforcement access standards and downstream privacy protections for location information. This proposal attempts to (1) articulate clear rules for courts to apply and law enforcement agents and industry to follow; and (2) strike a reasonable balance among the interests of law enforcement, privacy, and industry. We believe that our location information framework could form a solid basis for legislation because, among other things, when measured against the current state of the law, it improves the position of all stakeholders appreciably. Industry gains clear rules to follow and is not overly burdened or exposed by reporting requirements. Law enforcement gains clear rules to follow that will not unduly limit their investigative activities, especially in light of certain existing policies voluntarily adopted by the DOJ. Indeed, law enforcement's ability to acquire prospective location information to find individuals who have committed, are committing, or are about to commit a crime, when the location information itself is not evidence of a crime, is arguably improved by these proposed access standards. Moreover, law enforcement participation in a system that features tighter standards for initial access, as well as increased downstream privacy protections like minimization and notice, will promote increased public trust in the integrity of the system and a corresponding increase in law enforcement's own credibility.

While many privacy advocates have lobbied for a probable cause standard for all law enforcement access to location data, we have illustrated that this is not a realistic legislative goal in the current political climate or any immediately foreseeable one. Law enforcement will successfully argue that such a standard will unduly limit its investigative activities, including the ability to exclude someone from an investigation and spare her any unnecessary further inquiry into her personal life. Our proposal, however, offers privacy advocates clear rules that improve upon the current D Order standard and ensures that a probable cause standard will govern all law enforcement compelled disclosures of prospective cell phone location data. Moreover, this privacy framework offers privacy advocates a policy more protective than any threshold access standard alone can provide: downstream privacy protections that, among other things, ensure greater transparency and congressional oversight and minimize government authorities' retention of location data. As a legislative strategy, then, we submit that privacy advocates will stand on much firmer ground in supporting access standards aimed at a reasonable, legitimate balancing of stakeholder equities that also include downstream privacy protections. While privacy advocates can continue to fight for higher access standards for all location data in the courts, their constituents will not benefit from valuable downstream protections unless Congress includes them as part of reasonable, palatable ECPA legislative

reform. Our solution follows the suggestions of some jurists who have considered the potential social harms posed by location-based technologies and services: that Congress may be best suited to address these issues. We agree and offer the foregoing proposal as a strong initial step in that direction.[291]

291. During the writing of this Article, three bills in the 112th Congress were introduced proposing new law enforcement access standards for location data. *See* S. 1011, 112th Cong. (2011); S. 1212, 112th Cong. (2011); and H.R. 2168, 112th Cong. (2011). None of these bills currently contain downstream privacy protections. Two of the bills, S. 1212 and H.R. 2168, require a Rule 41 "probable cause" standard for all law enforcement compelled disclosures of location data, including the use of GPS tracking devices placed on cars. While S. 1011 allows law enforcement to compel historical location data with a D Order, there is no scope element addressing whether there is a sufficient nexus between the alleged or suspected criminal activity and the scope of the location data requested. *See supra* Sections III.C.1, III.C.2. S. 1011, like the two other bills, requires a Rule 41 "probable cause" showing for law enforcement to compel prospective data (including the use of GPS tracking devices) but similarly does not take into account the "probable cause of what" problem that may inhibit law enforcement from acquiring the current or prospective location of a subject who, for example, has committed a past crime when the subject's current or prospective location is not itself evidence of a crime.

Questions for the Record submitted to Mark Eckenwiler, Senior Counsel, Perkins Coie LLP*

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6216
(202) 225-3951
http://www.house.gov/judiciary

June 21, 2013

Mr. Mark Eckenwiler
Senior Counsel
Perkins Coie
700 Thirteenth Street N.W.
Washington, D.C. 20005-3960

Dear Mr. Eckenwiler,

The Judiciary Committee's Subcommittee on Crime, Terrorism, Homeland Security and Investigations held a hearing on "The Electronic Communications Privacy Act (ECPA), Part 2: Geolocation Privacy and Surveillance." on Thursday, April 25, 2013 at 10:00 a.m. in room 2141 of the Rayburn House Office Building. Thank you for your testimony.

Questions for the record have been submitted to the Subcommittee within five legislative days of the hearing. The questions addressed to you are attached. We will appreciate a full and complete response as they will be included in the official hearing record.

Please submit your written answers to Alicia Church at alicia.church@mail.house.gov or B-370B Rayburn House Office Building, Washington, DC, 20515 by July 26, 2013. If you have any further questions or concerns, please contact or at 202-225-5727.

Thank you again for your participation in the hearing.

Sincerely,

Bob Goodlatte

Bob Goodlatte
Chairman

*The Subcommittee had not received a response from this witness at the time this hearing record was submitted for printing, September 24, 2013.

Enclosure

Congressman John Conyers, Jr.

Questions for Hearing Record

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

The Subcommittee has received conflicting information regarding the extent to which the use of "microcells," "picocells" and "femtocells" impacts the accuracy of single tower location data obtained by law enforcement agencies.

In his written testimony, Mr. Eckenwiler stated that "user-owned microcells ... do not expand the network of towers available to the general population," adding that they "are only usable by their owners" and not by "other cell phone users" using the same wireless carrier.[1]

Professor Blaze, however, observed in his written testimony that the general trend is for "cellular sectors [to] become smaller and smaller[,] and [that] microcells, picocells, and femtocells are being deployed to provide denser coverage."[2]

The recently published memo from the Center for Democracy and Technology on "Trends in Cell Site Precision" describes in greater depth the industry trend towards the deployment of femtocells. It notes, for example, that Sprint has distributed free femtocells to customers with poor 3G coverage, and has now deployed more than 1 million femtocells nationwide.[3]

User manuals for the femtocells provided to consumers by AT&T, Verizon and Sprint are also very instructive on this issue.[4] According to this carrier-supplied documentation, AT&T femtocells only provide service for phones on an "approved user list,"[5] while Verizon and Sprint femtocells appear to provide service by default to any active subscriber.[6]

---

[1] See http://judiciary.house.gov/hearings/113th/04252013/Eckenwiler%2004252013.pdf at page 4.
[2] See http://judiciary.house.gov/hearings/113th/04252013/Blaze%2004252013.pdf at page 15.
[3] https://www.cdt.org/files/file/cell-location-precision.pdf at page 2.
[4] T-Mobile does not currently use femtocell technology.
[5] http://www.att.com/media/en_US/swf/3Gmicrocell/assets/ATT3GMicroCell_UserManual.pdf at page 3 ("All 3G and 4G cell phones that receive wireless service from AT&T will work with the MicroCell if they are added online to the MicroCell's approved user list.").
[6] http://support.verizonwireless.com/pdf/network_extender_user_manual.pdf at page 5 ("If you do not choose to manage the access to your Network Extender, other Verizon Wireless subscribers within range of

For each of the witnesses, please provide any additional information to clarify:

1. The extent to which femtocells generally expand the coverage of wireless networks;

2. Whether they provide service only to the phone of a customer which has installed the device, or to phones of other wireless subscribers who are nearby; and

3. Whether wireless carriers are able to "filter out" high-accuracy femtocell data from historical or "real time" single cell tower data provided to law enforcement agencies in response to an order issued under 18 U.S.C. § 2703(d) or a "hybrid order?"

---

your Network Extender will be able to use your Network Extender...."); See also http://support.sprint.com/global/pdf/user_guides/samsung/airave/airave_by_sprint_ug.pdf ("When the base station is set to open access, the first three callers detected within the base station's area are given access to place or receive calls through the base station. Your base station is set to open access by default.")

Response to Questions for the Record from Peter A. Modaferri, International Association of Chiefs of Police

THOMAS P. ZUGIBE
DISTRICT ATTORNEY

Office of the
District Attorney
County of Rockland

August 2, 2013

Hon. Robert Goodlatte
Committee on the Judiciary
Congress of the United States
House of Representatives
2138 Rayburn House Office Building
Washington DC 20515 – 6216

Attn: Congressman John Conyers Jr.

Re: Questions for hearing Record
"The Electronic Communications Privacy Act (ECPA) Part 2 Geolocation Privacy and Surveillance"

Dear Chairman Goodlatte:

Thank you for giving me the opportunity to respond in writing to Congressman Conyer's questions regarding my testimony before your committee. As noted in my written statement for this hearing, I am neither a Technical Expert nor a lawyer; I am a law enforcement executive with extensive experience in conducting, coordinating and supervising complicated criminal investigations on the local level.

As such my response to the issues raised in these questions are the result of my understanding of technical and legal issues as they have been explained to me by technical and legal experts both from within my agency and other law enforcement agencies. My answers will offer the perspective of local law enforcement and its efforts to address criminal activity on a daily basis.

1. The extent to which femtocells generally expand the coverage of wireless networks?

Response: I do not know how to quantify the expansion of coverage enabled by femtocells, but my understanding is that they do enable a more accurate location determination. My understanding is that the original idea of femtocells was actually to expand the networks by bringing home coverage to customers who got poor reception at their houses. The "genius idea" was that the provider would get the customer to pay for a device and the Internet bandwidth to power it in order to create coverage where none had previously existed. The debate then became whether the femtocells would provide service to phones not associated with the household of the person who bought and installed it, because the customer is paying for the "tower" (the femtocell) and the "backhaul" (bandwidth back to the cellular network over their personal high-speed data connection).

One South Main Street • Suite 500 • New City, NY 10956 • (845) 638-5001 • Fax (845) 638-5298 • rocklandcountyda.com

My understanding is that enhanced accuracy, which is the issue at hand, is a by-product of this business model – the service providers figured this business model was more cost effective than paying for a more towers and data connections in areas with only a few customers.

2. Whether they provide service only to the phone of a customer, which has installed the device, or to the phones of other wireless subscribers who are nearby?

Response: I am not certain whether femtocells are capable of only providing service to specific phones of individual customers. What confuses the issue is the conflicting information regarding the extent to which the use of "micro cells" "picocells " and "femtocells" impacts the accuracy of single tower location data obtained by law enforcement agencies can be found in the industries use of terminology. As I understand it, what is causing the confusion is the fact that the term "microcell" has been used in two ways in the cellular marketplace. Technically, a "microcell" is the next step down from a "macrocell" (usually antennas mounted on a big tower) Historically, a "microcell" was a lower-powered device that was attached to a water tower, tall building, church steeple, or whatever to fill in coverage gaps. So, it would cover a somewhat smaller area than a macrocell, but not dramatically smaller.

The devices that providers are selling/giving to customers in poor coverage areas actually only cover the area immediately around a residence, considerably smaller than a true microcell. From a technical/engineering standpoint, it is my understanding that these are technically "femtocells". However, for marketing purposes companies determined that "femtocell" was too complicated for the average consumer to understand, hence, companies started advertising them as "microcells." This has significantly confused an already "muddy" situation.

To complicate matters further, in the middle ground for this cell structure you have picocells, which are smaller than true microcells, but bigger than femtocells. Picocells are utilized for large government and private sector complexes. An example of this is can be seen in metropolitan subway stations.

For clarification, these are base stations (cell sites) in decreasing order of power, as I understand them:

Macrocell (big tower)
Microcell (lower-powered antenna to fill in coverage gaps in urban areas, attached to whatever is handy)
Picocell (lower-powered unit to cover a specific building or area)
Femtocell (little router-looking device that attaches to your home internet connection to make sure your cell phone works in your house...sometimes called a "microcell" for marketing purposes)

3. Whether the carriers are able to "filter out" high accuracy femtocell data from historical or real time single cell tower data provided to law enforcement agencies in response to an order issued under 18 U.S.C. § 2073d or a "Hybrid Order"?

Response: Assuming that cell service providers can cull out femtocell information from the inventory of data that they furnish to law enforcement – and it is not documented that they are able or willing to do so – the data that remains should pass constitutional muster. In fact, the 5th Circuit Court of Appeals in Texas recently found that such information is unprotected under the Fourth Amendment, precisely because it is not the solely the phone user's information, but, rather, a business record the service provider keeps as part of the whole record of the delivery of the communication:

> In the case of such historical cell site information, the Government merely comes in after the fact and asks a provider to turn over records the provider has already created.
>
> Moreover, these are the providers' own records of transactions to which it is a party. The caller is not conveying location information to anyone other than his service provider. He is sending information so that the provider can perform the service for which he pays it: to connect his call. And the historical cell site information reveals his location information for addressing purposes, not the contents of his calls. The provider uses this data to properly route his call, while the person he is calling does not receive this information.[1]

It is plain that cell phone data does not require a warrant merely because it is information about a cell phone. Instead, the analysis would begin and end with the intrusion level versus what, if any, privacy rights a subject surrenders when he allows a third party to access location information concerning his or her whereabouts.

Our core position is that the legal standard for accessing records should be based on how they are created (in the normal course of business vs. because of law enforcement demand, like a real-time remote geolocate), not how precise they are. Again, a call to a residential landline gives a very precise location, but no one is suggesting that it needs a higher level of protection.

I refer again to the quoted portion of the 5th Circuit opinion. The provider created the location record to properly route and deliver a phone call. That record may be a precise femtocell location or a less precise tower/sector location - it does not matter - the record was created by the provider for the same purpose. Precision or lack of precision should not be the determinant in the case of historical location information.

I know that many people do not believe they have an expectation that the location information associated with their cell phone is private. How so? Because in a variety of investigations I have directed, the subjects intentionally turned off their cell phones at some time prior to the crimes (even took the battery out of the devices) in order ensure that relevant location records were not created.

Thank you again for this opportunity. As always, I stand ready to answer any questions that committee members may have for me.

Very truly yours,

Peter A. Modafferi
Chief of Detectives
Rockland County District Attorney's Office

---

[1] In Re: Application Of The United States Of America For Historical Cell Site Data, No. 11-20884 (5th Cir. July 30, 2013).

Response to Questions for the Record from Catherine Crump, Staff Attorney, American Civil Liberties Union (ACLU)*

BOB GOODLATTE, Virginia
CHAIRMAN

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON THE JUDICIARY
2138 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6216
(202) 225–3951
http://www.house.gov/judiciary

JOHN CONYERS, JR., Michigan
RANKING MEMBER

June 21, 2013

Ms. Catherine Crump
Staff Attorney
ACLU
125 Broad Street, 18th Floor
New York, NY 10004

Dear Ms. Crump,

The Judiciary Committee's Subcommittee on Crime, Terrorism, Homeland Security and Investigations held a hearing on "The Electronic Communications Privacy Act (ECPA), Part 2: Geolocation Privacy and Surveillance." on Thursday, April 25, 2013 at 10:00 a.m. in room 2141 of the Rayburn House Office Building. Thank you for your testimony.

Questions for the record have been submitted to the Subcommittee within five legislative days of the hearing. The questions addressed to you are attached. We will appreciate a full and complete response as they will be included in the official hearing record.

Please submit your written answers to Alicia Church at alicia.church@mail.house.gov or B-370B Rayburn House Office Building, Washington, DC, 20515 by July 26, 2013. If you have any further questions or concerns, please contact or at 202-225-5727.

Thank you again for your participation in the hearing.

Sincerely,

Bob Goodlatte
Chairman

*The Subcommittee had not received a response from this witness at the time this hearing record was submitted for printing, September 24, 2013.

Enclosure

Congressman John Conyers, Jr.

Questions for Hearing Record

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

The Subcommittee has received conflicting information regarding the extent to which the use of "microcells," "picocells" and "femtocells" impacts the accuracy of single tower location data obtained by law enforcement agencies.

In his written testimony, Mr. Eckenwiler stated that "user-owned microcells ... do not expand the network of towers available to the general population," adding that they "are only usable by their owners" and not by "other cell phone users" using the same wireless carrier.[1]

Professor Blaze, however, observed in his written testimony that the general trend is for "cellular sectors [to] become smaller and smaller[,] and [that] microcells, picocells, and femtocells are being deployed to provide denser coverage."[2]

The recently published memo from the Center for Democracy and Technology on "Trends in Cell Site Precision" describes in greater depth the industry trend towards the deployment of femtocells. It notes, for example, that Sprint has distributed free femtocells to customers with poor 3G coverage, and has now deployed more than 1 million femtocells nationwide.[3]

User manuals for the femtocells provided to consumers by AT&T, Verizon and Sprint are also very instructive on this issue.[4] According to this carrier-supplied documentation, AT&T femtocells only provide service for phones on an "approved user list,"[5] while Verizon and Sprint femtocells appear to provide service by default to any active subscriber.[6]

---

[1] See http://judiciary.house.gov/hearings/113th/04252013/Eckenwiler%2004252013.pdf at page 4.
[2] See http://judiciary.house.gov/hearings/113th/04252013/Blaze%2004252013.pdf at page 15.
[3] https://www.cdt.org/files/file/cell-location-precision.pdf at page 2.
[4] T-Mobile does not currently use femtocell technology.
[5] http://www.att.com/media/en_US/swf/3Gmicrocell/assets/ATT3GMicroCell_UserManual.pdf at page 3 ("All 3G and 4G cell phones that receive wireless service from AT&T will work with the MicroCell if they are added online to the MicroCell's approved user list.").
[6] http://support.verizonwireless.com/pdf/network_extender_user_manual.pdf at page 5 ("If you do not choose to manage the access to your Network Extender, other Verizon Wireless subscribers within range of

For each of the witnesses, please provide any additional information to clarify:

1. The extent to which femtocells generally expand the coverage of wireless networks;

2. Whether they provide service only to the phone of a customer which has installed the device, or to phones of other wireless subscribers who are nearby; and

3. Whether wireless carriers are able to "filter out" high-accuracy femtocell data from historical or "real time" single cell tower data provided to law enforcement agencies in response to an order issued under 18 U.S.C. § 2703(d) or a "hybrid order?"

---

your Network Extender will be able to use your Network Extender...."); See also http://support.sprint.com/global/pdf/user_guides/samsung/airave/airave_by_sprint_ug.pdf ("When the base station is set to open access, the first three callers detected within the base station's area are given access to place or receive calls through the base station. Your base station is set to open access by default.")

Response to Questions for the Record from Matt Blaze, Professor, University of Pennsylvania

School of Engineering and Applied Science
Department of Computer and Information Science
3330 Walnut Street, Levine Hall
Philadelphia, PA 19104-6309
Tel 215.898.8560 Fax 215.898.0587
www.cis.upenn.edu

23 July 2013

Hon. Bob Goodlatte
US House of Representatives
Committee on the Judiciary
2138 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Goodlatte,

Thank you for the opportunity to testify at the ECPA, Part 2: Geolocation Privacy and Surveillance hearing on April 25th, and for the opportunity to respond to the three follow-up questions from Rep. Conyers. I will address those questions here.

Question 1: *The extent to which femtocells generally expand the coverage of wireless networks.*

Response: When a cellular telephone customer makes or receives a telephone call, text message or sends or receives data from their phone, the cellular handset's antenna communicates (via radio waves) with a cellular telephone "base station", consisting of one or more antennas, a network router (computer) to route the signals between cellular handsets and the carriers larger network and other infrastructural elements such as power and a network connection.

Femtocells are a type of "small cell" cellular telephone base station, a growing category that also includes devices known as "microcells" and "picocells". Small cellular base stations act as part of a cellular provider's infrastructure to improve and extend coverage of places that cannot be effectively served by the "large cell" base stations that historically made up early cellular networks. (Although the terms are not precisely defined, femotocells generally refer to small cell base stations that are installed and managed by customers to expand coverage in their homes or businesses; these may use the Internet to connect back to the network. Microcells and picocells, on the other hand, generally refer to small cell base stations that are managed and installed by the carrier

itself. Other than that, the various small cell technologies are largely similar.) From the telephone users' perspective, calls served by small cells and those served by large cells are effectively indistinguishable, and a user today is likely to encounter both large and small cells throughout the day or even during a mobile call.

Small cell base stations expand the coverage of wireless networks in two important ways. First, because they are typically located on or near the particular premises that they are intended to cover, they expand radio signal coverage of the network (the "bars" displayed on a phone handset) into areas where radio signals from large base stations may be blocked by opaque environmental features such as buildings, foliage, and terrain such as hills or valleys. Small cells are especially important for extending coverage into indoor areas such as private homes and businesses. Large base stations are typically located outdoors, atop buildings or on towers, and to serve a wider geographic area, but at the expense of complete coverage within that area.

Second, small cells expand the capacity of the network to serve more customers simultaneously. Each base station, whether small or large, has only a limited amount of bandwidth available to it, a fraction of which is occupied whenever a customer makes a call or uses a data service. (Wireless carriers have limited chunks of radio spectrum bandwidth that they can use to provide cellular service; this directly translates to a fixed number of phone calls, text messages, and data that a carrier can accommodate in a given geographic area.) Adding small cell base stations makes it possible to serve more customers by allowing the finite amount of radio spectrum allocated to wireless carriers to be re-used within a smaller area.

For these reasons – ensuring good coverage to indoor areas and more efficiently using scarce radio spectrum – the deployment of small cell base stations such as femtocells is growing and can be expected to continue to grow at a fast pace. They are often the only effective way a carrier can expand coverage to eliminate weak-signal areas and increase usage capacity. From the user's perspective, the increased proliferation of small cell base stations means that the likelihood that any given call will be served by a small cell is growing rapidly. This is especially true in urban areas and other places with a high density of cellular users.

Question 2: *Whether they provide service only to the phone of a customer which has installed the device, or to phones of other wireless subscribers who are nearby.*

Response: Carrier-maintained small cells (microcells, picocells, etc.) will generally serve the phone of any subscriber within range. For customer-maintained femtocells, whether they will provide service for other subscribers depends on how they are configured. Today, some carriers provide femtocells configured to serve only specifically-designated subscribers by default. Other providers, including Verizon Wireless and Sprint Nextel, currently provide femtocells configured to serve any subscriber by default.

Because small cells are an essential part of expanding future network coverage and capacity in dense areas, we can expect the trend to be toward open femtocells, either through default configuration or by carriers providing incentives for customers to turn the feature on. Also, as noted above, there are other kinds of small cells that are installed and maintained directly by the carrier (rather than by customers), and these cells are still open to all subscribers even when customer-maintained femtocells of that carrier might not be.

Question 3: *Whether wireless carriers are able to "filter out" high-accuracy femtocell data from historical or "real time" single cell tower data provided to law enforcement agencies in response to an order issued under 18 USC § 2703(d) or a "hybrid order?"*

Response: Whether a carrier can filter out customer-maintained femtocell records from data provided to law enforcement will depend on the policy and technical capabilities of the particular carrier. Among other things, it will depend upon how such cells are identified in a given carrier's internal databases and whether they can be distinguished from other base stations at the time records are extracted for law enforcement use.

For other kinds of small-cells, particularly those maintained by the carrier (as opposed to a customer), it will be more difficult for carriers to filter their records. This is because there is little technical distinction, for the purposes of a wireless carrier's operations, between a small cell and a large cell. Indeed, the difference between carrier-maintained small cells and large cells is more of a continuum of their coverage size than a bright-line distinction.

Moving forward, we can expect to see wireless networks with an increasing proportion of small cells (which will consist of a combination of carrier-maintained small cells and customer-maintained small cells), particularly in dense areas. Even if it were possible to do so, filtering out all small cells from call record data provided to law enforcement could, in many cases, leave location information in few or none of call detail records for many targets, because a large fraction of calls will be served by such cells.

Thank you again for the opportunity to respond to these questions. Please feel free to contact me if I can be of any further assistance. I can be reached via email at blaze@cis.upenn.edu.

Sincerely

Matt Blaze

○