AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

# GEOLOCATIONAL PRIVACY AND SURVEILLANCE (GPS) ACT

## HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

ON

**H.R. 2168**

MAY 17, 2012

**Serial No. 112–125**

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

74–259 PDF WASHINGTON : 2012

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

LAMAR SMITH, Texas, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
DENNIS ROSS, Florida
SANDY ADAMS, Florida
BEN QUAYLE, Arizona
MARK AMODEI, Nevada

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
MIKE QUIGLEY, Illinois
JUDY CHU, California
TED DEUTCH, Florida
LINDA T. SÁNCHEZ, California
JARED POLIS, Colorado

RICHARD HERTLING, *Staff Director and Chief Counsel*
PERRY APELBAUM, *Minority Staff Director and Chief Counsel*

---

## SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

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

BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
J. RANDY FORBES, Virginia
TED POE, Texas
JASON CHAFFETZ, Utah
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
SANDY ADAMS, Florida
MARK AMODEI, Nevada

ROBERT C. "BOBBY" SCOTT, Virginia
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
JUDY CHU, California
TED DEUTCH, Florida
SHEILA JACKSON LEE, Texas
MIKE QUIGLEY, Illinois
JARED POLIS, Colorado

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

# CONTENTS

MAY 17, 2012


Page

THE BILL

H.R. 2168, the "Geolocational Privacy and Surveillance (GPS) Act" ..... 185

OPENING STATEMENTS

The Honorable F. James Sensenbrenner, Jr., a Representative in Congress from the State of Wisconsin, and Chairman, Subcommittee on Crime, Terrorism, and Homeland Security ..... 1
The Honorable Jason Chaffetz, a Representative in Congress from the State of Utah, and Member, Subcommittee on Crime, Terrorism, and Homeland Security ..... 2
The Honorable Robert C. "Bobby" Scott, a Representative in Congress from the State of Virginia, and Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security ..... 22

WITNESSES

John R. Ramsey, National Vice President, Federal Law Enforcement Officers Association
Oral Testimony ..... 24
Prepared Statement ..... 26
Joseph I. Cassilly, Past-President, National District Attorneys Association
Oral Testimony ..... 27
Prepared Statement ..... 29
Edward J. Black, President and CEO, Computer & Communications Industry Association
Oral Testimony ..... 36
Prepared Statement ..... 38
Catherine Crump, Staff Attorney, American Civil Liberties Union (ACLU)
Oral Testimony ..... 47
Prepared Statement ..... 49

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Prepared Statement of the Honorable F. James Sensenbrenner, Jr., a Representative in Congress from the State of Wisconsin, and Chairman, Subcommittee on Crime, Terrorism, and Homeland Security ..... 1
Material submitted by the Honorable Jason Chaffetz, a Representative in Congress from the State of Utah, and Member, Subcommittee on Crime, Terrorism, and Homeland Security ..... 3

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the Electronic Privacy Information Center (EPIC) ..... 87
Letter from Walter A. McNeil, President, International Association of Chiefs of Police ..... 100
Berkeley Technology Law Journal ..... 101
Letter in opposition to H.R. 2168 ..... 180
Letter from the Federal Bureau of Investigation Agents Association (FBIAA) . 183

# GEOLOCATIONAL PRIVACY AND SURVEILLANCE (GPS) ACT

**THURSDAY, MAY 17, 2012**

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME, TERRORISM,
AND HOMELAND SECURITY,
COMMITTEE ON THE JUDICIARY,
*Washington, DC.*

The Subcommittee met, pursuant to call, at 10:03 a.m., in room 2141, Rayburn House Office Building, the Honorable F. James Sensenbrenner, Jr. (Chairman of the Subcommittee) presiding.

Present: Representatives Sensenbrenner, Goodlatte, Lungren, Chaffetz, Marino, Gowdy, Cohen, Johnson, Chu, Deutch, Jackson Lee, and Polis.

Staff Present: (Majority) Caroline Lynch, Subcommittee Chief Counsel; Arthur Radford Baker, Counsel, Tony Angeli, Counsel, Lindsay Hamilton, Clerk; (Minority) Bobby Vassar, Subcommittee Chief Counsel; Joe Graupensperger, Counsel; and Veronica Eligan, Professional Staff Member.

Mr. SENSENBRENNER. The Subcommittee will be in order. Without objection, the share will be authorized to declare recesses during votes on the floor. Today's hearing is on H.R. 2168, the "Geolocational Privacy Surveillance (GPS) Act." I would like to especially welcome our witness and thank you for joining us today. I am joined by my colleague from Virginia, the distinguished Ranking Member of the Subcommittee, Bobby Scott, and also the principal author of the bill, the gentleman from Utah, Mr. Chaffetz. At this time I would like to ask unanimous consent to insert my opening statement in the record and yield my time to Mr. Chaffetz for an opening statement.

[The prepared statement of Mr. Sensenbrenner follows:]

**Prepared Statement of the Honorable F. James Sensenbrenner, Jr., a Representative in Congress from the State of Wisconsin, and Chairman, Subcommittee on Crime, Terrorism, and Homeland Security**

Today's hearing examines H.R. 2168 the "Geolocational Privacy and Surveillance" or the "GPS Act." This bill introduced by the gentleman from Utah has bipartisan support and currently has 18 cosponsors. A similar measure has been introduced in the Senate.

The law 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 location –based technology. As GPS technology has become cheaper, more widely available, and used more frequently in our everyday lives, the legal authorities and restrictions that are, or should be, in place to govern when

such information about another person is accessed and used have become less than clear.

It is also not completely clear how location-based technology is used and exactly who is using it. We know that law enforcement uses it and we will hear about that today. But the technology is also used or can be used by commercial entities and really just about anyone that wants to spy on your whereabouts.

This bill defines what geolocation information is and establishes uniform legal authorities for obtaining this information. In short, this bill does what the Supreme Court invited, or challenged, the legislative branch to do when they decided the *Jones* case earlier this year. In that decision, Justice Alito stated "A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."

H.R. 2168 properly balances the appropriate use of the information obtained from the technology and the privacy rights of those enjoying the convenience and other benefits that the technology confers to us in our everyday lives.

No one doubts that this information is useful, especially to law enforcement officers and agents. The big question is how do we balance the needs of the police with the expectations of privacy of those that they protect? This bill tries to strike the appropriate balance and give the police the tools they need and our citizens the privacy that they expect.

It is no secret that *court ordered* electronic surveillance has long been a valuable tool for effective law enforcement. At least in terms of "content" interception, it is a technique that is typically used as a last resort, when other investigative techniques have failed or would be likely to fail or would even be too dangerous to try. When utilizing GPS and other location-based technology, the police often use it early in their investigations and there is generally no court order or supervision at all.

By incorporating a judicial process that must be followed to seek a court order authorizing this type of surveillance, we are assured that, like in the case of the interception of a communications "content," that this technique is not abused.

There would likely be internal layers of review before a judicial application was even made. Facts would have to be established and proved, and ultimately a judge would be the one who decides, based on all of the information presented, if such a technique is warranted.

Once authorized, law enforcement would comply with any reporting requirements of the court and there would be procedures to protect the rights of parties whose geolocational information was improperly obtained.

It is important to underscore the fact that this bill does not take away the use of GPS or other geolocational technology from law enforcement officials. The loss of this investigative technique would be a huge risk to both our public safety and our national security. The bill provides some common sense and perhaps some long overdue "rules of the road" regarding the use of these technologies.

I welcome our witnesses and look forward to hearing their testimony.

---

Mr. CHAFFETZ. Thank you, Mr. Chairman. I truly do appreciate your cosponsoring this legislation and for holding this hearing. I would ask unanimous consent to insert into the record four documents, the Salt Lake Tribune editorial of June 19, the Oregonian Editorial, as well as a statement from Professor Matt Blaze of University of Pennsylvania, and a statement of principles from the digital due process coalition.

Mr. SENSENBRENNER. Without objection.

[The material referred to follows:]

The Salt Lake Tribune

## Modern Privacy – Chaffetz' GPS bill is necessary – June 19th, 2011

If a police officer wants to follow you around, there's nothing to stop him. And that's just fine.

But if a police officer wants your cell phone to follow you for him, not only in real time but over the past however many days, there is also nothing to stop him. Or to stop menacing ex-boyfriends from using the same technology to annoy innocent women. Or to stop phone companies and data providers from selling a detailed record of your comings and goings, whether you want them to or not.

And that is a problem. A problem that Utah's Rep. Jason Chaffetz has a plan to solve.

Together with Sen. Ron Wyden, an Oregon Democrat, the Republican congressman from Utah's 3rd District is putting forward what's called the GPS Act. GPS in this case standing for Geolocation Privacy and Surveillance.

As Chaffetz points out, current law is mostly silent on how government, businesses and individuals can get hold of the data generated by cell phones, mobile computers and the GPS units found in more and more automobiles. That's because most of the laws we have that might be relevant were written when there was no such thing as GPS devices.

The purpose of these gizmos is to allow you to find your way to a new city or restaurant, or to allow your laptop or cell phone to find the network it will use to serve your needs. Those are things that benefit you, the person who owns the machine and pays the bill.

A side effect is that the network, and some human being looking over its shoulder, can use your private devices to find where you are now, or where you were last Thursday at midnight, and use that information to send you an advertisement you don't want, a threatening letter or an arrest warrant.

In the case of individuals and businesses, that ought to be against the law. And the Chaffetz-Wyden bill would make it as illegal to do those things as it already is for anyone outside law enforcement to tap your telephone. In the case of law enforcement agencies, they may have legitimate reasons to trace your GPS records, but, as is the case with phone taps, they should have probable cause and a warrant to do so.

The bill would allow the same kind of tap-first, get-warrant-afterward for emergencies that are now allowed for phone tap warrants. And it would also allow police to track you through your GPS devices if they have reason to believe you are injured, lost or otherwise in need of assistance.

The bill is exactly the kind of thing that Congress should be about, updating laws to make them conform at once to changing technologies and eternal standards of privacy and individual rights.

The Oregonian

## Protecting the Privacy of Those Whose Cellphones are Tracking - June 19th, 2011

It's only been 25 or so years that the U.S. government granted civilian access to U.S. Air Force satellites supporting what was then a science-fiction technology known as global positioning. Americans were learning brave new things like personal computing and the use of email, but global positioning technology started to come of age, too, with the result today that email is quaint and GPS guides us to destinations with voiced driving instructions, speeds parcel delivery to our homes via trackable trucks, and even helps hikers, bikers and golfers decide their next best moves.

Geolocation technology also lurks within many of our cellphones, iPhones, high-end Blackberries and other devices so enmeshed in everyday life. It can do wondrous things, among them pinpoint a caller's location to emergency crews in the event 9-1-1 is dialed -- or help police bypass gumshoe ploddings and go straight to the suspect. Unless GPS is actively turned off – in some devices not a practical possibility – it tracks its keeper 24/7 just as it would another delivery truck.

Oregon Senator Ron Wyden, joined by Utah Rep. Jason Chaffetz, stands back to ask: Just who gets to know where everybody is?

It's a simple but vexing question. And he and Chaffetz are dead right to worry about such a thing, because it cuts straight to the core of civil liberty in a democracy that increasingly depends upon it.

While the information generated by geolocation technology bounces off publicly owned satellites and is recorded by the computers of service providers along the way, it is, like the content of a telephone call, private. In the absence of a search warrant, an electronic record showing that a person stopped at a city park and a Safeway on the way to work on a Friday morning should no more be the government's property than it is open to purchase by a business or a spy.

But right now the rules governing the uses and protections of geolocation information are a blur, if they exist at all.

Wyden and Chaffetz this week floated legislation that would require any law enforcement agency seeking to track an individual first obtain a search warrant showing probable cause of a crime exists. By persuasively linking the need for such information to a case, the agency would clear the same bar now in place for tapping a citizen's telephone.

The Oregonian

*(Continued)*

That's precisely as it should be. Our zoomy and emerging technologies, compelling and life-enhancing in so many ways, have shot beyond our ability to manage their first consequence of use: the electronic pileup of personal information. And we've shown ourselves in recent years to be better at excitedly adopting new technologies than in adapting, or even understanding, their legal, cultural and political consequences.

We're still learning when it comes to the near-antique telephone, which saw runaway and unauthorized tapping in the wake of the World Trade Center terrorist attacks. Yet the ground rules on telephone taps continue to be debated in such a way that pits national security interests against personal privacy.

Global positioning technology and the record left by it needn't suffer as contentious a fate.

The Wyden and Chaffetz measure, long in the making and headed for hearings, could help to protect everyone's privacy while leaving open legal approaches for selective tracking of individuals. Meanwhile it would require that commercial service providers obtain a customer's permission before releasing their geolocation information, and hackers and stalkers found to be tracking a person's movements would see swift punishment.

With such wise protections in place, there's no reason not to enjoy the next cool geolocating device – whether you can turn it off or not.

**House Committee on the Judiciary**

**Subcommittee on Crime, Terrorism, and Homeland Security**

**Hearing on the Geolocation Privacy and Surveillance (GPS) Act**

**Statement for the Record of**

**Professor Matt Blaze**

**May 17, 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.

Let me preface my remarks by pointing out an important – and essential - feature of H.R. 2168: it does not limit its coverage to one specific type of location tracking technology. 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 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. HR 2168 accomplishes this by defining "geolocation information" sufficiently broadly to encompass the range of high-precision location technologies likely to be relevant in the foreseeable future.

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 285 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 LET 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, there are more than three times as many cellular base stations today as there were ten years ago. Indeed, this trend has been accelerating in recent years, with the deployment of the latest generation of smaller and smaller-scale cellular base stations (called, variously, "microcells", "picocells" and "femtocells") designed to serve very small areas, such as particular floors of buildings or even individual homes and offices.

The effect of this trend toward smaller 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. But as even more precise location information becomes available, these 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 precise the sector identity 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 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.

As the precision provided by cellular network-based location techniques approaches that of GPS-based tracking technology, cellular location tracking can have 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, quietly and automatically calculated by the network, without triggering any unusual or overt behavior that might be detected by the subject. And the "tracking device" is now a benign object that is deliberately carried by the target -- his or her telephone, computer, or tablet.

**Updating The Electronic Communications Privacy Act of 1986**

***Overarching goal and guiding principle:*** *To simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce laws, respond to emergency circumstances and protect the public. These principles would not change, and are subject to, the current definitions, exceptions, immunities and permissions in ECPA.*

1. A governmental entity may require an entity covered by ECPA (a provider of wire or electronic communication service or a provider of remote computing service) to disclose communications that are not readily accessible to the public only with a search warrant issued based on a showing of probable cause, regardless of the age of the communications, the means or status of their storage or the provider's access to or use of the communications in its normal business operations.

2. A governmental entity may access, or may require a covered entity to provide, prospectively or retrospectively, location information regarding a mobile communications device only with a warrant issued based on a showing of probable cause.

3. A governmental entity may access, or may require a covered entity to provide, prospectively or in real time, dialed number information, email to and from information or other data currently covered by the authority for pen registers and trap and trace devices only after judicial review and a court finding that the governmental entity has made a showing at least as strong as the showing under 2703(d).

4. Where the Stored Communications Act authorizes a subpoena to acquire information, a governmental entity may use such subpoenas only for information related to a specified account(s) or individual(s). All non-particularized requests must be subject to judicial approval.

Adobe
Amazon.com
AOL
Apple
AT&T
CenturyLink
Data Foundry
Diaspora
Dropbox
eBay
Facebook
Google
Hattery Labs
Hewlett-Packard
IAC
IBM
Inflection
Integra Telecom
Intel
Intelius
Intuit
Linden Lab
LinkedIn
Loopt
Microsoft
Personal
Salesforce.com
Sonic.net
SpiderOak
TRUSTe
Twitter

American Booksellers Foundation for Free Expression
American Civil Liberties Union
American Library Association
Assoc. for Competitive Technology
Association of Research Libraries
Americans for Tax Reform
Bill of Rights Defense Committee
Business Software Alliance
Campaign for Liberty
Center for Democracy & Technology
Center for Financial Privacy and Human Rights
Citizens Against Government Waste
Common Sense Media
Competitive Enterprise Institute
Computer & Communications Industry Association
The Constitution Project
Consumer Action
Distributed Computing Industry Assoc.
EDUCAUSE
Electronic Frontier Foundation
Engine Advocacy
FreedomWorks
Future of Privacy Forum
Information Technology and Innovation Foundation
The Joint Center for Political and Economic Studies
Liberty Coalition
National Workrights Institute
NetCoalition
Newspaper Association of America
Software and Information Industry Association
TechAmerica
TechFreedom
Telecommunications Industry Assoc.

**May 15, 2012**

Mr. CHAFFETZ. The role of Congress is to protect and defend the United States Constitution and personal liberties provided to American citizens under the Fourth Amendment. Put simply, the government and law enforcement should not be able to track somebody indefinitely without their knowledge or consent or without obtaining a probable cause warrant from a judge. Just because it can be done doesn't mean it necessarily should be done.

With that in mind, I recently introduced the Geolocational Privacy and Surveillance Act. Companion legislation was also introduced in the United States Senate by Senator Ron Wyden of Oregon. I appreciate the bipartisan support of this bill, cosponsors in the Judiciary Committee include Chairman Sensenbrenner, Chairman Goodlatte, Chairman Coble, Representative Lofgren and Ranking Member Conyers. The bill creates a legal framework designed to give government agencies, commercial entities and private citizens clear guidelines for when and how geolocation information can be accessed and used.

In *Jones*, the recent Supreme Court case on the issue, the court ruled unanimously that physically attaching a GPS device to a vehicle constituted the search under the Fourth Amendment. Most law enforcement agencies have responded by requiring their officers to obtain probable cause warrants before placing GPS devices on vehicles. However, the court stopped short of requiring a warrant for all geolocation information, including that obtained from other devices or methods such as smartphones or, for instance, the OnStar System.

The Supreme Court has laid down the broad principle that location tracking without a warrant constitutes a search under the Fourth Amendment, it is now up to Congress to enact a comprehensive statute to fill in the details. In fact, Justice Alito specifically identified Congress appropriate place to resolve the difficult issues associated with the collision of new technologies and their impact on civil rights when he noted, "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes to draw detailed lines and to balance privacy and public safety in a comprehensive way."

I believe that Americans have a reasonable expectation of privacy. And I agree wholeheartedly with Justice Alito's notion that it is truly the Congress that should deal with it. I applaud the Chairman for holding this hearing. I thank the witnesses for attending and for their thoughtful testimony, and I yield back the balance of my time.

Mr. SENSENBRENNER. The Chair recognizes the gentleman from Virginia, Mr. Scott, for an opening statement.

Mr. SCOTT. Thank you, Mr. Chairman. Today we meet to discuss the Geolocational Privacy and Surveillance Act, a bill intended to clarify the standards of government access to certain types of personal location information. With greater conveniences that technology affords us, we also have new challenges to our privacy rights because of the types of information that is generated about us, how it is stored and by whom it can be accessed.

The Supreme Court's 1967 decision, *Katz v. The United States* continues to direct our privacy jurisprudence. In that case, a man

calls from a pay phone booth, were recorded by 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. That standard should continue to guide us today.

When you see something, when we go somewhere in public, you know that we may be seen by others, even if we do not want others to know where we are. The visual recognition by others is the risk that we take. What do not expect is a carrying of personal communication devices such as cell phones will be used by the government to track and record our every move. This is particularly the case of cell phone-based location information has become, in many cases, available and actually more accurate than GPS because of the proliferation of micro cells.

We have laws to make accommodations between privacy rights and sometimes urgent need of law enforcement to investigate crimes. For example, Congress has drafted several statutes to restrict government access to the content of an electronic communication, but provides less stringent standards for accessing non content records, merely reflecting that a communication took place. The Electronic Communications Privacy Act was enacted in 1986, but it did not contemplate every possible technological advance and it 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.

This bill addresses this gap by requiring the government to show probable cause and get a warrant in order to obtain a historical and prospective data about the location of our citizens. The bill includes an exception for emergency situations. Given our expectations of privacy, this bill should be a good starting point for our discussion on this issue. So I thank the gentleman from Utah for his work on the issue. And Mr. Chairman, I yield back the balance of my time.

Mr. SENSENBRENNER. Without objection, all Members' opening statements will be put in the record at this point. It is now my pleasure to introduce today's witnesses. John Ramsey is currently one of the national vice presidents of the Federal Law Enforcement Officers Association. And I right in calling it FLEOA?

Mr. RAMSEY. Yes, sir.

Mr. SENSENBRENNER. Okay. Mr. Ramsey was elected to this position in November of 2008, and serves as one of the ten elected board members representing 26,000 Federal law enforcement officers from nearly every Federal law enforcement agency.

Mr. Ramsey also a member of FLEOA'S national legal committee and serves as the national legal liaison director and chapter president for Mississippi. Mr. Ramsey is employed by the U.S. Department of Veterans Affairs Office of Inspector General in Jackson, Mississippi as the resident agent in charge. He has been with the VA OIG since 2000. He received a bachelor of science in criminal justice from Georgia State University and his Master's from George Washington University in forensics and criminology.

Mr. Joseph Cassilly is active with the Maryland State Attorneys Association having held several offices including two terms as president of the Association. He is the past president of the Na-

tional District Attorney's Association and is on the board of directors of NDAA. He was sworn in as assistant State's Attorney in October 1977, and in 1982, he was elected State's Attorney for Harford County, Maryland and has been reelected six times. He joined the U.S. Army in 19 and served with F company 75th Rangers, 25th infantry division. He was awarded a combat infantry badge, Purple Heart and Army commendation medal. He received a Bachelor of arts in psychology from University of Arizona in 1974, and his JD from the University of Baltimore Law School in 1977.

Edward Black has been president and CEO of the Computer and Communications Industry Association since 1995. He previously served for nearly a decade as CCIA's vice president and general counsel. He is past chairman of the State Department's Advisory Committee on International Communications and Information Policy and past president of the Washington International Trade Association and Foundation and chairman of the Pro Trade Group. He serves on the board of directors of the interoperability clearinghouse.

After serving as legislative director for Representative Louis Stokes in the early 1970's, Mr. Black served as congressional liaison for the State Department. He then served as chief of staff to Representative John LaFalce of New York before again returning to the executive branch as Deputy to the Assistant Secretary for Congressional affairs for the Secretary of Commerce. He subsequently practiced law in the private sector. He received his Bachelor of Arts degree from Muhlenberg College and his JD degree from the American University Washington College of Law.

Catherine Crump is a staff attorney with the ACLU, Speech Privacy and Technology Project. She is a non residential fellow at the Stanford Center for Internet and Security. Prior to joining the ACLU, she clerked for the Honorable M. Margaret McKeown of the U.S. Court of Appeals for the Ninth Circuit. She received her undergraduate degree from Stanford in 2000. Served as a Fulbright Fellow from 2000 to 2001, and received her JD degree from Stanford Law School in 2004.

The witnesses' written statements will be entered into the record in their entirety. I ask you to summarize your testimony in 5 minutes or less. To help you stay within the time limit you have got the red, yellow and green lights in front of you. The Chair has a reputation for banging the gavel when the red light goes on, and I now recognize Mr. Ramsey.

**TESTIMONY OF JOHN R. RAMSEY, NATIONAL VICE PRESIDENT, FEDERAL LAW ENFORCEMENT OFFICERS ASSOCIATION**

Mr. RAMSEY. Thank you, Chairman Sensenbrenner, Ranking Member Scott and other distinguished Members of the Committee. Thank you for the opportunity to testify today. On behalf of the 26,000 members of FLEOA, I am voicing our concerns with this proposed bill. The proposed legislation will impact all Federal law enforcement. Geolocational surveillance is an invaluable tool to combat domestic and international crime and terrorism in addition to rendering aid in exigent circumstances. As the proposed legislation stands, geolocational information has been given an overly broad definition and application. As written one could easily inter-

pret PIN registers, OnStar and even E-ZPasses as geolocational information.

These are not witch hunts that law enforcement officers are involved in. Information obtained with these court orders provides law enforcement with historical data as well as possible location information which becomes important when determine weather the need rises to the level of a court order or a warrant.

While conducting everyday ongoing criminal investigations, court orders issued to communication companies may provide law enforcement with geolocational information. This information can be critical when it comes to potentially unlocking evidence that may lead to the apprehension of a murderer or rapist, or even saving lives.

If law enforcement wants to know the content of a target's conversation, the most protected type of communication, we know that current Federal law and supreme court rulings require the issuance of a warrant as in the case with government-owned locational devices and Title III intercepts. The difference in this situation is that the government does not own nor are they attaching the locational device to a person.

Currently with a court order, law enforcement may request the possible location of a cellular device from a communication company via their cell tower or cell site information, which enables law enforcement to potentially infer a general area where a particular call originated, not necessarily a precise location. Cell site information only gives an approximate location versus a precise or exact location like GPS devices. Cell phones are not government-owned locational beacons, the government did not attach the GPS device to someone's personal cell phone unlike government-owned GPS devices attached to vehicles.

Seconds count when lives are at risk. Law enforcement should not be further hindered during their investigation of time sensitive cases that may involve the threat of serious bodily harm or death by imposing additional legal hurdles that may jeopardize the lives of countless innocent Americans. The Supreme Court did not extend *Jones* decision to cell phones, law enforcement is not seeking the content of conversations, nor are we trying to step on someone's expectation of privacy. We are simply looking at corporate records just like financial records to which a legally-authorized subpoena or court order would suffice.

While our membership respects the constitutional rights of all citizens, we do not want to see the United States adopt unnecessary legislation. If our country's laws allow for the disclosure of corporate records pursuant to legally authorized court orders or subpoenas, the same standard should apply to all corporate records to include communication companies.

Geolocation communication information should be treated no differently. We hope your Committee understands our concerns with the proposed legislation and respects our position. I would like to thank the Committee Members for your continued support of law enforcement and an opportunity to testify today.

Mr. SENSENBRENNER. Thank you.

[The prepared statement of Mr. Ramsey follows:]

**Prepared Statement of John R. Ramsey, National Vice President, Federal Law Enforcement Officers Association**

Chairman Sensenbrenner, Vice-Chairman Gohmert, and distinguished Members of the Committee:

I would like to thank you for the opportunity to testify today. I appear before you today in my official capacity as the National Vice President of the Federal Law Enforcement Officers Association (FLEOA). On behalf of the 26,000 members of the FLEOA, I am voicing our concerns with H.R. 2168. The proposed legislation will impact all Federal law enforcement. Geolocational surveillance is an invaluable tool to combat domestic and international crime and terrorism, in addition to rendering aide in exigent circumstances, such as child exploitation cases.

Geolocational communication services focuses on historical information and potential real-time information. This issue should not be confused with real-time conversations and/or Title III intercepts. However, as the proposed legislation stands, geolocational information has been given an overly broad definition and application. As written, one could easily interpret pen registers, On-Star, and EZ–Passes as "geolocational information." What we are focused on in this situation is wireless communication information currently obtained through a court order signed by a United States Judge. These are not witch hunts as some may allude to. Information obtained with these court orders provides law enforcement with historical data, as well as possible location information, which becomes important when determining whether the need rises to the level of a court order or a warrant.

While conducting everyday on-going criminal investigations, court orders issued to communication companies may provide law enforcement with geolocation information. This information can be critical when it comes to potentially unlocking the evidence that may lead to the apprehension of a murderer or rapist. If law enforcement wants to know the "content" of a target's conversation, the most protected type of communication, we know that current Federal law and Supreme Court rulings require the issuance of a warrant, as in the case with Government-owned location devices and Title III intercepts. The difference in this situation is that the Government does not own nor are they attaching the locational device to a person. With the current exceptions built into the proposed legislation, at least law enforcement has some leeway with regards to abductions and other exigent circumstances.

In order to better understand the intricacies of this issue, we need to take a closer look at "geolocational information," With a court order, law enforcement may have the opportunity at seeing who a killer or rapist called, in the past, by requesting historical data/records from a communication company. With a court order, pen registers may provide law enforcement with phone numbers, including the area codes, which may identify where a call was placed from, such as a specific state and/or city, similar to cell-tower information. With a court order, law enforcement may be able to see where the killer or rapist bought gas or used an ATM, by requesting historical information from a financial institution. Currently, with a court order, law enforcement may request the possible location of a cellular device from a communication company via cell-tower or cell-site information, which enables law enforcement to potentially infer a general area where a particular call originated, not a precise location. Cell-site information only gives an approximate location at best, versus a precise or exact location like GPS devices. Cell phones are not Government-owned locational beacons. The Government did not attach a GPS device to someone's personal cellular phone, unlike Government-owned GPS devices attached to vehicles. I would like to stress that all of these scenarios, information gathered does not contain the "content" of a conversation.

Law enforcement is permitted to gather information using court orders, a legal document or proclamation signed by a United States Judge in which the court orders a person to perform a specific act, or in some circumstances, prohibits them from performing a specific act. What is the next step? Are we going to do away with grand jury subpoenas and move to the issuance of search warrants for companies to disclose corporate and financial records? Law enforcement can request a subpoena and obtain employment records, medical records, and other personal and private information of individuals that are targets of criminal investigations. Who are we protecting with this legislation? The innocent or the criminals? FLEOA takes the position that the innocent were and are not targets of criminal investigations. FLEOA is also not suggesting that criminals, or those suspected of criminal wrong doing, have less constitutional rights than a law abiding citizen. But do we really want to slow down the apprehension of murderers and rapists so they can build their trophy wall by increasing the amount of legal documents necessary to gather information? Law enforcement should not be further hindered during their investigation of time sensitive cases that involve the threat of serious bodily harm or

death by imposing additional legal hurdles may very well jeopardize the lives of countless innocent Americans.

This legislation is a pale attempt to build on the 2012 *Jones* decision rendered by the U.S. Supreme Court. The Supreme Court did not extend the *Jones* decision to cellular phones. Law enforcement is not seeking the "content" of a conversation, nor are we trying to step on someone's expectation of privacy. We are simply looking at corporate records, just like financial records, to which a legally authorized subpoena or court order will suffice. When a person places a phone call, the "content" of the call is protected, not the parking lot, sidewalk or location from which it was placed. The proposed legislation would, under Rule 41 of the Federal Rules of Criminal Procedure, make "content" and "geolocational information," such as cell-site and EZ–Pass, rise to the same standard. FLEOA would opine that these two types of information do not enjoy the same level of expectation of privacy.

While our membership respects the constitutional rights of all citizens, we do not want to see the United States adopt unnecessary legislation. If our country's laws allow for the disclosure of corporate records pursuant to legally authorized court orders or subpoenas, the same standard should apply to all corporate records, to include communication companies. Geolocation communication information/records should be treated no differently. We hope your committee understands FLEOA's concern with the proposed legislation and respects our position.

I would like to thank the Committee Members for your continued support of law enforcement and its mission and for this opportunity to testify today. I will be happy to answer any questions that you may have at this time.

---

Mr. SENSENBRENNER. Mr. Cassilly.

## TESTIMONY OF JOSEPH I. CASSILLY, PAST-PRESIDENT, NATIONAL DISTRICT ATTORNEYS ASSOCIATION

Mr. CASSILLY. Thank you, Chairman Sensenbrenner Ranking Member Scott, Members of the Committee. The National District Attorney's Association is the oldest and largest organization representing State and local prosecutors in the United States.

Obtaining geolocation information is not a search, but even if it were a search, obtaining a warrant is not required for a lawful search when the circumstances of getting the warrant would be unreasonable or frustrate the lawful purposes of the government. Thus, there are legal searches that are recognized by the court that do not require probable cause. NDAA has serious concerns that H.R. 2168 would unreasonably frustrate State or local law enforcement's ability to effectively protect the citizens we serve.

NDAA believes it is necessary to distinguish between historical data compiled from cell tower hits and real-time GPS ping information. The overwhelming majority request for geolocation data in my jurisdiction are for historical data. These requests are often made to confirm or rebut information which does not meet the probable cause standard. For example, in a gang shooting in my jurisdiction, an anonymous caller who states they fear gang retaliation gives the police the identity of two gang members who committed the murder; the police get information about the suspects' cell phones from prior arrest reports. The cell site historical information for the time of the killing shows that those two cell phones were hitting off the same tower at the same time in the area of the murder. Even without this information, the police do not have probable cause to arrest, but they have at least allowed the ability to focus their investigation.

Gangs are domestic terrorists. Denying law enforcement the ability to use this critical tool is to decide to refuse to protect those communities. Section 2602(d) of the law, exception for consent, al-

lows for a parent or guardian to consent to a child's device location, but is silent as to whether such consent is available with those with mental handicaps, developmental disability, dementia or who may be on medication. And further, if a child is reported missing by their peers but the parents can not be located, do the police waste precious seconds hunting for the parents or use those seconds to hunt for the child?

The bill is confusing, 2602(f), exception for emergency information, has a different standard for law enforcement officer to access information when—than does 2604 emergency situation exception, including the fact that one requires a subsequent order while the other does not. The emergency exceptions are vague on what information can be legally obtained.

Do these exceptions allow, for example, in a kidnapping case for law enforcement attract the kidnappers' phone or only the victim's phone? It is important to note that the ability to gather GPS information lasts only so long as the battery continues to power the device. Any unreasonable delay may result in a bad dead battery and frustrate the effort to use geolocation.

Given that the proposed law subjects electronic communication service providers to possible criminal and civil liability if they cooperate with an officer, the laws should provide a course of action that would enable rapid transfer when needed, and possibility penalties for service providers who are intentionally slow to respond in providing critical law enforcement information.

State statutes and court rules impose additional burdens on the use of warrants that may be unintended or unforeseen by this Committee. For example, in Maryland, law enforcement officers are required to deliver a copy of the warrants to the person being searched at the execution of the warrant. Is the person being searched the person carrying the phone? If so, we would have to locate them before we locate them in order to serve the warrant and give them the opportunity to turn off the device and flee.

Maryland law enforcement are also required to deliver the statement of probable cause to the person searched at least 60 days after the warrant is issued. Generally these warrants are used at the end of an investigation, but often this information is needed at the beginning of the investigation.

These are some examples of the unintended consequences from only one State, and imagine them compounded them in 50 States. We assert that this legislation is a solution in search of a problem, and is the true defenders of the public freedoms and rights, America's prosecutors believe that the current system of police discretion and judicial oversight is working. For if it were not, the evidence would be found in court cases challenging the conduct of the police.

Thank you for the opportunity to testify before the Committee on this important legislation.

Mr. SENSENBRENNER. Thank you.

[The prepared statement of Mr. Cassilly follows:]

**National District Attorneys Association**
44 Canal Center Plaza, Suite 110, Alexandria, VA 22314
703.549.9222 (o) • 703.836.3195 (f)
www.ndaa.org

**Written Testimony of**

**The Honorable Joseph I. Cassilly**
**State's Attorney for Harford County, Maryland**
**and**
**Past President, National District Attorneys Association**

**Hearing on H.R. 2168, the "Geolocational Privacy and Surveillance Act"**

**House Judiciary Committee**
**Subcommittee on Crime, Terrorism, and Homeland Security**
**United States House of Representatives**

**May 17, 2012**

Chairman Sensenbrenner, Ranking Member Scott, members of the Subcommittee, thank you for inviting me to testify today on behalf of the National District Attorneys Association (NDAA), the oldest and largest organization representing over 39,000 district attorneys, State's attorneys, attorneys general and county and city prosecutors with responsibility for prosecuting 95% of criminal violations in every state and territory of the United States.

As an Army Ranger who served in Viet Nam and a State's Attorney for over thirty-three years I have pledged my honor and life to defending the Constitution and the rights of my fellow citizens.

The Founders of our Country in adopting the Fourth Amendment wanted to protect its citizens from unreasonable searches. Obtaining geolocation information from a third party has been determined not to be a search; although the U. S. Supreme Court may weigh in on that decision. Even if it is a search obtaining a warrant is not required for a lawful search when the circumstances of getting the warrant would be unreasonable or frustrate the lawful purposes of the government; ie. Search incident to arrest, search resulting from exigent circumstances or "hot pursuit", search of a vehicle, among other recognized exceptions to the warrant requirement.

NDAA has serious concerns with the potential impact that H.R. 2168, the Geolocational Privacy and Surveillance Act (GPS Act), would have on State or local law enforcement's ability to most effectively and efficiently protect the citizens we serve. The GPS Act, as currently written, has been drafted so broadly that the bill would require a search warrant to gather many forms of information that can currently be obtained by subpoena. The new standards set through the GPS Act would hamper law enforcement's ability to quickly obtain important information that could be used to save lives. NDAA feels that any legal reforms to the current system should be implemented to *shorten* the investigative timeline instead of lengthening it, which we feel would be an unintentional consequence of the GPS Act. NDAA believes that any bill that hinders law enforcement from doing its job most effectively would lead to serious consequences for crime victims and public safety. Because so many cases are time sensitive in nature - including child abductions, other forms of kidnapping and organized criminal and/or terrorist activities - law enforcement must be able to work these cases without unnecessary administrative delay.

NDAA believes it is imperative to distinguish between historical data compiled from cell tower hits, referred to as cell-site information and real time GPS ping information. The overwhelming majority of the requests for geolocation data in my jurisdiction are for the historical data. These requests are often made to confirm or rebut information which does not meet the probable cause standard. For example, in a gang shooting in my jurisdiction an anonymous caller who states they fear gang retaliation if their identity is known gives the police the identity of two gang members who committed the murder. The police receive cell phone information regarding these individuals from prior arrest reports. The cell-site historical information for the time of the killing shows that those two cell phones were hitting off the same tower at the same time in the area of the murder. Even with this information, the police do not have probable cause to arrest but to require probable cause to access historical records would have deprived the officers of this vital information. Gang crimes are domestic terrorism which rules with fear, silences witnesses and deprives whole communities of life and liberty. Denying law enforcement the ability to use this critical tool is to decide to refuse to allow America's communities to protect themselves from the scourge of gangs.

In section 2602 (d) "Exception for Consent" allows for a parent or guardian to consent to a child's device location but it is silent as to whether such consent is available for those with mental handicaps, developmental disabilities, dementia or who may be on medication. Also, what if a child is reported missing by their peers but parents or guardians cannot be located? Do the police waste precious seconds hunting for the parents or use those seconds to hunt for the child?

Evidence of the confusion this bill will cause is obvious from the fact that section 2602 (f) "Exception for Emergency Information" sets a different standard for a law enforcement officer to access geolocation information than does section 2604(a)(1)(A) "Emergency Situation Exception", including the fact that one section does not require a subsequent order while the other does. While NDAA does appreciate the "Emergency Situation Exception" contained in section 2064(a) of the GPS Act, we also feel the bill as currently written leaves too much of a grey area on what geolocational information can be legally obtained by law enforcement in such emergency situations. For example, the exception allows for interception of geolocation information when "such officer reasonably determines that an emergency situation exists that --- involves—immediate danger of death or serious physical injury to any person;" It is unclear, however, whether this exception would permit interception of geolocation information relating to others – such as the perpetrator of a crime - or only information relating to the person whose life or safety is threatened. Take a kidnapping case, for example; it is currently unclear whether law enforcement could use this exception to track the kidnapper's phone or only the victim's phone or other electronic devices belonging to the victim. It is also important to point out that the ability to gather GPS information lasts only so long as the battery continues to power the device. Stopping to investigate to gather information or draft a warrant or find a judge may exhaust the battery and frustrate the effort to use geolocation.

It may not be clear at first whether a missing person is in danger or just out of touch and yet frantic relatives often demand that law enforcement use every opportunity to locate that person. Given that the proposed law subjects electronic communication service providers' employees to possible criminal and civil liability if they cooperate with an officer, as well as loss of their job if

the employer wishes to separate itself from an employee's decision, the employee might challenge the officer's determination that an exception to the warrant requirement exists.

If Congress chooses to elevate the standard for location evidence to probable cause, law enforcement will be forced to adapt to these changes and such changes would extend the investigative timeline and decrease the number of leads law enforcement can pursue in a given time period. Additionally, with deep cuts in federal spending to important State and local law enforcement programs over the past several years – including to COPS, Byrne-JAG, Byrne Competitive and cuts to information sharing programs like the Regional Information Sharing System (RISS) - law enforcement has been forced to do more with less; the GPS Act would seem to present yet another burdensome obstacle for State and local law enforcement to overcome in order to effectively protect and serve.

State statutes and court rules impose additional burdens on the use of warrants. For example in Maryland, law enforcement officers are required to deliver a copy of the warrant to the person being searched at the execution of the warrant. Is the person being searched the person carrying the phone? This means that the target of the investigation would be alerted to the investigation and afforded an opportunity to intimidate witnesses, destroy evidence, turn off the wireless communication device and flee. In addition Maryland law enforcement is required to deliver the statement of probable to the person searched at least sixty days after the warrant is executed; therefore, warrants in Maryland generally come at the conclusion of the investigation, but most law enforcement needs geolocation information at the beginning of the investigation. Additionally, on weekends, holidays and evenings law enforcement may use hours trying to

locate a judge and another hour driving to their location with the warrant. These are just some examples from one of fifty states and several territories of how the Federal requirement of a warrant translated to the States will result in uncounted obstacles and frustrate or destroy law enforcement efforts.

Whatever level of investigative process is deemed appropriate by the Congress, NDAA urges the Committee to take steps to guarantee that law enforcement is able to access the required communications records – including location information – once that process is implemented. The emergency exceptions outlined in section 2602(f) of the GPS Act may provide the necessary recourse but if there is no statutory mandate for a service provider to turn over the records, and no time frame for compliance, law enforcement may effectively be denied the information we need despite being in accordance with the legal process. The law should provide a course of action that will enable the rapid transfer of information when needed and possibly provide penalties for service providers who are intentionally slow to respond in providing critical location information.

NDAA appreciates the privacy concerns of America's citizens and strives for all of America's State and local prosecutors to minimize unnecessary intrusions into citizen's privacy. While there are countless articles expressing concern about the amount of location evidence obtained by law enforcement and private companies, not a lot has been publicized about the good that has come from the proper use of location evidence by law enforcement to solve crimes and to save lives. There are literally thousands of instances where the proper gathering and use of this important evidence has led to the rescue of abducted children, the identification and prosecution

of sexual predators, and the apprehension and conviction of a terrorist looking to harm innocent Americans. We assert that this legislation is a solution in search of a problem and as the true defenders of the public's freedom and rights America's prosecutors believe that the current system of police discretion and judicial oversight is working; for if it were not the evidence would be found in cases challenging the conduct of the police in the Courts.

Chairman Sensenbrenner, Ranking Member Scott, members of the Subcommittee, I appreciate the opportunity to testify before you on this important legislation and will answer any questions which you may have.

Mr. SENSENBRENNER. Mr. Black.

**TESTIMONY OF EDWARD J. BLACK, PRESIDENT AND CEO, COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION**

Mr. BLACK. Mr. Chairman, Members of the Committee, thank you for the opportunity to testify today on the GPS Act. CCIA is an international trade association dedicated to innovation and dynamic open competition with members in many technology sectors. Our members employ half a million workers with annual revenues of a quarter of a trillion dollars. CCIA is also a founding member of the Digital Due Process coalition formed to update ECPA.

The GPS Act addresses one key coalition recommendation for updating ECPA. Extending Fourth Amendment protections to reflect the realities of the digital age is an important goal for our industry. Regardless of motivation, the new found—the recent Supreme Court decision in *Jones* called into question whether pervasive new technology received Fourth Amendment protection. *Jones* did not reach the question of protection for personal location information generated by mobile devices. Despite unanimous discomfort among the judges over warrantless tracking of individuals, *Jones* failed to include devices owned by over 95 percent of the U.S. population. Thus, authorities may now choose to replace physical tracking devices with pervasive and unchecked monitoring of our whereabouts via either private cell phone networks or GPS information built into our phones.

Representative Goodlatte and Chaffetz's GPS Act is an important step toward closing the 21st century loophole in ECPA. Requiring probable cause to justify intrusive surveillance may make the life of law enforcement agents slightly more difficult, but that was the explicit purpose of our Founders when they expressly limited the government's powers under the Fourth Amendment.

Mobile technologies are transforming and benefiting our economy. The mobile industry contributed 195 billion to our GDP, and 3.8 million jobs in 2011 alone. Trust is essential to this dynamic part of our economy, particularly where data is concerned, this is why the GPS Act is so vital.

Your location privacy says a great deal about you. It says where you work and sleep, your religious preferences, doctor visits and political affiliations. All are personal information with a legitimate claim to privacy. Current warrant protection against location information does not clearly apply to all GPS or cell site information. There is uncertainty in the business community about what the law is, for each type of data and what privacy assurances can be made to users. This uncertainty itself hampers innovation and the growth of companies and the Internet platform and cloud services sectors.

Problems of trust are exacerbated because there is rarely consent from the cell phone user when the government demands information from companies. In this nascent marketplace, we need a clarifying law requiring a warrant before law enforcement may demand personal location information from the electronic service providers. The GPS Act creates a uniform warrant standard for government demands of location data. It gives assurances to all users that the location information will be reasonably protected under the law.

This is vitally important as many new applications such as Yelp and Four Square incorporate real-time user information. This bill does not make this information off limits to government entities which would simply need to obtain a warrant, justas it must be done to access many other types of evidence under law and the Constitution.

This bill also recognizes that there are circumstances in which obtaining a warrant may be too time consuming or inappropriate. This bill would not keep law enforcement from doing its job.

In summary, we believe that the changes made by the GPS Act are vital to the privacy and civil liberties of Americans, and for the positive effects it would have on an exciting and booming sector of our economy. Thank you for the opportunity to testify today. I look forward to your questions.

Mr. SENSENBRENNER. Thank you, Mr. Black.

[The prepared statement of Mr. Black follows:]

*Before the*

Subcommittee on Crime, Terrorism, and Homeland Security
U.S. House of Representatives Committee on the Judiciary

*Regarding*

**Geolocation Privacy and Surveillance Act**
May 17, 2012

**Testimony of Edward J. Black**
President & CEO
Computer & Communications Industry Association (CCIA)

Mr. Chairman, Ranking Member, and Members of the Subcommittee:

Thank you for the invitation to testify before you today on the important issue of geolocation privacy. CCIA is an international non-profit trade association dedicated to open markets, open systems, and open networks. CCIA members participate in many sectors of the computer, information technology, and telecommunications industries and range in size from small entrepreneurial firms to some of the largest in the industry. In particular, we have a number of members involved in the mobile industry. Our members employ nearly half a million workers and generate approximately a quarter of a trillion dollars in annual revenue.[1]

Our industry occupies a unique position in the global marketplace. More than any other industry, it connects and empowers users. It helps educate, entertain, and erase distance. It serves as a powerful force for good in the global marketplace. At the same time, information generated by communication services can be misused by governments. In addition to posing a grave threat to civil liberties, this misuse will impair adoption and growth of ICT services. Thus, our constitutional values and our economic interests align, and point inexorably to the conclusion that a judicial warrant, founded upon probable cause, must accompany any law enforcement demands for private individuals' location information.

[1] For a complete listing of CCIA members see http://www.ccianet.org/members.

My testimony makes five points: First, geolocation privacy is a civil liberties imperative. The privacy concerns and Constitutional beliefs of the nation strongly support warrant protection for location information. Where a person is located in relation to society – their interactions, their associations, their sense of being a free citizen – this information is the very essence of personhood. To cede to government the unchecked power to track you wherever you are is to lay the cornerstone of the surveillance state. As the D.C. Circuit noted in its opinion in *United States v. Maynard*, location data reveals information about a person that would shock the average American, and it can do it for numerous surveillance targets, from the comfort of an air conditioned office. There can be no question that, as the court in *Maynard* decided, Americans have a reasonable expectation of privacy in their whereabouts.[2] The law should close the loophole in ECPA that was inadvertently created by new geolocation technology. Otherwise the intent of the original law as well as this reasonable expectation of privacy in one's whereabouts will be undermined.

Second, there is also an important business interest in location privacy. Mobile telephony and mobile Internet access are some of the fastest growing sectors in our national economy. Mobile penetration itself has grown at an incredible rate, and smartphones in particular continue to grab new users all the time. Mobile technology promises to improve lives in many ways and geolocation-aware devices and apps in particular offer a renaissance for users.

Third, many constituencies, from low-income and minority users, to many professionals, increasingly depend on mobile technology. For many, mobile devices are either the only means of accessing the Internet, or an indispensable tool in the workplace.

Finally, decreasing the trust that people have in the devices they use will have a meaningful impact on how those people interact in society and in business in the future. Trust is the most essential question when looking at the uptake of a new technology, particularly where data is concerned. This is why the GPS Act as introduced by Representatives Goodlatte and Chaffetz is so vital. Today, many users are aware that their smartphones have the capability to track their movements and, thanks to press surrounding the U.S. v. Jones case from last year, know that, at least for the time being,

[2] *United States v. Maynard*, 615 F.3d 544, 563-64 (DC Cir. 2010).

cell-site location data may not have the protection of a warrant. That knowledge impedes trust, and the GPS Act would send a clear signal that geolocation information collected through the use of cell phones will be respected and protected against government intrusion at the highest level.

**I. Civil liberties of Americans demand the protection of location data.**

Basic Fourth Amendment considerations call for the protection of location data just as we protect the content of letters and files within the home. The prevailing test for protection under the Constitution leads to the conclusion that the movement of people over time is information that the average American views as private data. To the extent that the courts have not embraced that rationale, Congress can and should step in to preserve location privacy rights.

The question of Fourth Amendment privacy rights in location information was raised most recently in a case that arose in Washington, DC. Police placed a GPS tracking device on the car of a suspected drug dealer without following proper warrant procedures, and the data gathered was challenged at trial.[3] The DC Circuit Court of Appeals issued a thoughtful opinion that came to the conclusion that people have a reasonable expectation of privacy in the collected history of their location information.[4] It can reveal intimate information about a person, including religion, political affiliation, health issues, and a host of other private details.[5] CCIA wholly agrees with this analysis.

The Supreme Court took a much narrower view when they heard the case, however. While they upheld the ruling, the majority opinion's theory was focused on the trespass that occurred when police placed the GPS receiver on the suspect's car.[6] This ruling certainly answered the question before the court, but left many other questions unanswered. It was not decided, for example, whether cell-site location information is similarly protected.

These questions are all the more unsettling because the government may misuse its powers in the name of preventing crime. The framers knew this reality well, and it is

---

[3] *Id.* at 549.
[4] *Id.* at 563-64.
[5] *Id.* at 562.
[6] *United States v. Jones*, 565 U.S. ___, slip op. at 4 (2012).

the genesis of the Fourth Amendment. Congress also appreciated the concern when it passed the Electronic Communications Privacy Act in 1986. It is now past time to clarify ECPA standards in response to new technology in several areas and geolocation information is one of them. CCIA agrees with the DC Circuit that the Fourth Amendment properly read protects all location data, but people's civil liberties need not wait on the courts. Congress has the ability to make sure that fundamental rights are not trampled on by a well-meaning but overreaching law enforcement, and the GPS Act would go a long way toward achieving that goal.

**II. Economic considerations demand protecting location data.**

*A. Mobile technology is revolutionizing our economy.*

Over the past decade mobile technologies have proven to be one of the most transformative of the information age. Their effects have been felt in everything from local emergency response to the fall of dictatorships.[7] Studies have linked mobile penetration to growth in GDP, particularly noting the network effects that increase GDP growth when penetration grows above 25%.[8]

The economic benefits of mobile access are hard to argue with. The mobile industry accounted for $195.5 billion in contribution to GDP and 3.8 million jobs in 2011 alone.[9] These numbers don't take into account the monetary benefits to mobile users who are better able to find what they're looking for, conduct business when traveling, and who gain numerous other advantages.

Nor do these studies address the non-monetary impact of mobile technologies. There are plenty of non-quantifiable, yet nonetheless important, benefits to mobile users. From family members quickly and easily able to let everyone know about a birth in the family, to checking the lyrics of that song you've had stuck in your head all day, all the way to being able to meet up with friends at the State Fair, mobile phones enable a host of desirable effects.

---

[7] Jamila Boughelaf, *Mobile phones, social media, and the Arab Spring*, April 2011. Tim Large, *Cell phones and radios help save lives after Haiti earthquake*, Reuters, Jan. 25, 2010.
[8] Kathuria *et al.*, 2009.
[9] Press Release, Wireless Industry A Catalyst For U.S. Economic Growth, Supporting 3.8 Million Jobs And Adding $195.5 Billion To GDP In 2011, *at* http://www.prnewswire.com/news-releases/wireless-industry-a-catalyst-for-us-economic-growth-supporting-38-million-jobs-and-adding-1955-billion-to-gdp-in-2011-149649095.html

In the past few years, the effects of the mobile revolution have been compounded by the rise of smartphones, giving access to computational power that only would have been available in a desktop computer just few years ago, in a form factor that fits in a pocket. Access to the Internet at the push of a button has changed how we communicate but also how we work, shop, travel, and play. This market has shown its power, shipping 144.9 million smartphones in the first quarter of 2012, and proving to be a bright spot in an otherwise somber economic outlook.[10]

In addition to being a booming business of its own, mobile and smartphones enable other businesses. The marketplace for smartphone apps has exploded in the past few years, for example. The small applications that run on smartphones can be useful, such as maps or educational tools, or amusements to kill time, such as music players, games, and social networking. In any case, they are often simpler to program than their equivalents on computers, and an industry of small businesses and independent developers has risen to create this new marketplace.

*B. Geolocation is an important piece of this marketplace.*

One particularly appealing piece of the smartphone market is the potential for geolocation-enabled apps. Through a number of different means, including the use of global positioning satellites (GPS) and cell-site location information, smartphones are able to determine their own location with considerable accuracy.

The device's ability to know its own precise location enables a wide variety of exciting services. Turn-by-turn directions are an obvious usage, but the possibilities go far beyond that. Apps can provide reviews of and coupons for nearby establishments, let you know when friends are nearby, and more. Despite their usefulness, however, only 6% of Americans use geolocation aware apps, and 70% of users are completely unaware that they exist.[11]

---

[10] IDC Press Release, *Worldwide Smartphone Market Continues to Soar, Carrying Samsung Into the Top Position in Total Mobile Phone and Smartphone Shipments, According to IDC*, May 1, 2012, *at* http://www.idc.com/getdoc.jsp?containerId=prUS23455612

[11] Liz Gannes, *Checking in From the Cutting Edge: Only Six Percent Use Geolocation Apps*, Dec. 6, 2011, http://allthingsd.com/20111206/checking-in-from-the-cutting-edge-only-6-percent-use-geolocation-apps/

Users also often express uncertainty, however, regarding the privacy of their geolocation information when asked about location-aware apps.[12] Location privacy is of the utmost importance, because of the depth of details about a person that can revealed. A trace of a person's comings and goings over the course of a week can show not just where they work and sleep, but also religious preferences, doctor visits, political affiliations, and many other pieces of personal information.[13]

The potential for abuse that comes with this information means that the trust of the user is of the utmost importance if this market is to grow and reach its fullest potential. CCIA believes that companies must treat geolocation information with the highest respect when it is gathered from users. Companies, however, can only control their own data practices. The same problems of trust in the platform arise when it is the government demanding information. This is why it is so important to this nascent marketplace that Congress pass a law requiring a warrant based on probable cause before law enforcement may demand location information about a person.

**III. Several constituencies depend heavily upon mobile technologies.**

The issues surrounding trust in location information are exacerbated by the fact that for many minorities, low-income individuals, rural populations, and professionals, smartphones may be the primary (and in some cases only) means of accessing the Internet and the great possibilities and opportunities that exist online. Unfortunately, these groups are also precisely the ones with the least trust of government. The possibility is very real that knowledge of the ease with which the government can obtain location information is deterring some of these groups from accessing the Internet via smartphones.

Broadband access in the United States is expensive and slow as compared to the rest of the world.[14] In many rural areas, in fact, landline broadband Internet is still not available at any price.[15] For those who cannot afford or access landline broadband,

---

[12] Louise Barkuus and Anind Day, *Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns*, July 2003.
[13] *United States v. Maynard*, 615 F.3d 544, 562 (DC Cir. 2010).
[14] Saul Hansell, *The Broadband Gap: Why is Theirs Faster?*, N.Y. Times, Mar. 10, 2009.
[15] FCC, High-Speed Services for Internet Access: Status as of December 31, 2008 (2010), *at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-296239A1.pdf

smartphones have become the only available means of reaching the Internet. While it is excellent that smartphones provide this service to those who would otherwise not have a means of Internet access, this limitation also presents problems with government surveillance.

The problem arises because those very groups that benefit in this way from smartphones have long standing reasons to be suspicious of government surveillance. These anxieties, valid or not, will affect the uptake of smartphones. This effect is likely to particularly affect potential smartphone users because the idea that a phone can carry geolocation information is much more obvious in a *smart*phone (as opposed to a feature phone, which can be located by cell-site data just as easily, but which is not transparent about the fact). It is likely that the perception of a lack of privacy against government intrusion affects the trust that potential smartphone users will place in the platform. If they perceive that the device will make it easier for the police to track their movements, they will forego using the device. Unfortunately, in many cases that also means they they will forego access to the Internet entirely, along with the economic and social benefits that come with access.

For many professionals, including members of Congress and their staff, a mobile device is necessity of life. In many other cases as well, the modern technology-enabled workplace demands its use. Thus, even those who might forfeit the empowering technology of mobile communications to escape an umbrella of perpetual surveillance cannot do so because of the demands of their job.

**IV. Trust is fundamental for growth and the current law undermines it.**

The situations described above hold true across the nation. As businesses across the Internet industry know, the trust of users is essential when collecting information from them, and geolocation information is no different. New geolocation services have the challenge of convincing potential users that they will treat information about their location with respect. In short, they must convince the users to trust them.

There are many things that companies can do to enhance that trust. Among other practices, they can and should be transparent with their users about the information they gather and how it will be used, give those users as much control as possible over whether

and when the information is collected, and protect the information once it is in their hands. It is vital for the health of their business to make this effort, and it is industry best practice.

The one thing a company that collects location data cannot promise, however, is that they will protect that information against warrantless snooping by the government. The current state of Fourth Amendment law gives warrant protection against location information collected through a physical trespass (i.e., placing a device on a suspect's car), but not through cell-site information or information collected directly from a device's GPS receiver.[16] There is therefore quite a bit of uncertainty amongst companies about what the law is for each type of data, and what promises they can make to their users.

That uncertainty itself hampers innovation and the expansion of businesses. Any company seeking start-up funding for a business plan that involves location information faces an uphill battle trying to overcome the stigma of legal uncertainty in a related area. The same is true when trying to form business partnerships or trying to sell a business that has achieved some success.

The same uncertainty has an even more important effect on user trust. Users who are nervous about the privacy of their information will be turned off by finding out that the company collecting that data either cannot say for certain when they will have to turn it over to law enforcement or will affirmatively do so even when the government does not have a warrant.

**V. The GPS Act can solve these problems.**

The bill proposed by Representatives Goodlatte and Chaffetz would solve these problems by applying a uniform standard for government demands of location data. By making that standard a warrant, it gives assurances to all users that their location information will be protected at the highest level under the law. This simple change would eliminate the uncertainty that exists in the location services industry and increase the trust that users place in the companies in that industry.

---

[16] *United States v. Jones*, 565 U.S. ___, slip op. at 11 (2012).

The GPS Act is a straightforward piece of legislation. While the Electronic Communications Privacy Act is itself complex and in need of reform in a broader sense, this bill would make some simple additions that ensure that the government must show a judge probable cause before it may demand either the present or past location of a suspect. This bill does not render this information completely off limits to government. Law enforcement would simply need to obtain a warrant, just as it must do to access many other types of evidentiary personal information under the law and the Constitution.

The bill is also balanced. It recognizes that there are circumstances in which obtaining a warrant may be too time consuming or inappropriate. Exceptions are provided for cases of emergency, the consent of the user, and instances of foreign intelligence gathering. In this way the proposal does not attempt to put law enforcement in a straitjacket that prohibits the government from doing its job.

We believe that the changes made by the GPS Act are vital both for the privacy and civil liberties of Americans and for the positive effects it would have on an exciting and booming sector of our economy. I thank you for the opportunity to testify today, and I look forward to answering your questions.

Mr. SENSENBRENNER. Ms. Crump.

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

Ms. CRUMP. 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. The ACLU supports passage of H.R. 2168, the Geolocational Privacy and Surveillance Act. Requiring law enforcement agents to obtain a warrant based upon probable cause before obtaining geolocational information would allow legitimate law enforcement investigations to proceed, while ensuring that innocent Americans do not have their privacy intruded upon.

As Congressman Chaffetz has already pointed out, passing the GPS Act would fulfill Congress's duty to ensure that the safeguards provided by the Fourth Amendment of our Constitution are respected.

Geolocational information 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 and others would not and indeed in the name simply could not secretly monitor and catalogue every single movement of an individual's car for a very long period.

The D.C. Circuit Court of Appeals expanded upon this point. A person who knows all of another's movements can deduce whether he is a weekly churchgoer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or groups and not just one such facts, but all such facts.

Attaching a GPS device to a vehicle is one way of obtaining location information. In the recent Supreme Court case *United States v. Jones*, the police tracked a defendant's movement continuously for 28 days with an accuracy of 50 to 100 feet. While some cell phones can also be tracked using GPS, all cell phone generate a continuous stream of location information because they register their location with cell phone networks several times a minute. Due to the proliferation of cell phone towers and advances in technology, it is the case that, as Professor Matt Blaze has pointed out to Congress in previous testimony and again today, it is becoming increasingly precise, and in some cases, cell site information is approaching the precision of GPS.

While the Supreme Court held in *Jones* that affixing a GPS device to monitor the movements of a car implicates the Fourth Amendment, it did not reach the question of whether that is a search that requires a warrant based upon probable cause. It will likely take years for this question to reach the Supreme Court once again. Congress should not stand by while law enforcement faces unclear standards for geolocation tracking and innocent Americans' privacy is invaded.

The warrant and probable cause requirement are essential components of the Fourth Amendment. The probable cause requirement is not high. Law enforcement merely has to have a good reason to believe that a search will turn up evidence of wrongdoing.

These requirements are especially important today given the tremendous technological developments of the past 10 years. Moreover, major telecommunication companies and Internet companies support a warrant and probable cause requirement.

Last August in an unprecedented effort to penetrate the secrecy surrounding cell phone tracking, 35 ACLU affiliates in 32 States filed over 380 Public Records Act requests to understand the policies procedures and practices of local law enforcement agencies for tracking cell phones. What we learned was disturbing. While over 200 of the agencies—while virtually all of the 200 agencies that responded indicated that they track cell phones, only a tiny handful indicated they had obtained warrants to do so. And many only comply with a lesser standard, such as a subpoena. The law governing location tracking policy should be clear, uniform, and protective of privacy, but unfortunately it is in a state of chaos with agencies in different towns following different rules, and in some cases, no clear rules at all.

The ACLU supports passage of the GPS Act because it would ensure that law enforcement agents obtain a warrant based upon probable cause in order to track—obtain geolocational information. The Act also includes perfectly reasonable and limited exceptions. Under the Act, for example, the police would be able to obtain location information when they had a good reason to believe that it would turn up evidence of wrongdoing, or where they have a good faith to believe that someone's life or safety was in jeopardy.

We urge the Committee to support H.R. 2168 and report it favorably from the Committee. Thank you.

[The prepared statement of Ms. Crump follows:]

Statement of Catherine Crump, Staff Attorney

American Civil Liberties Union

On

The Geolocational Privacy and Surveillance Act

Before the House Judiciary Subcommittee on Crime, Terrorism, and

Homeland Security

May 17, 2012

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

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

## I. Introduction

GPS and cell site technology provide law enforcement agents with powerful and inexpensive methods of tracking individuals over an extensive period of time and an unlimited expanse of space as they traverse public and private areas. In many parts of the country, the police have been tracking people for days, weeks, or months at a time, without ever having to demonstrate to a magistrate that they have a good reason to believe that tracking will turn up evidence of wrongdoing. Today, individuals' movements can be subject to remote monitoring and permanent recording without any judicial oversight. Innocent Americans can never be confident that they are free from round-the-clock surveillance by law enforcement of their activities. As Justice Sonya Sotomayor recently wrote, "The net result is that GPS monitoring--by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track--may alter the relationship between citizen and government in a way that is inimical to democratic society."[1]

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

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

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

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

### A. Tracking Cell Phones

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

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

The precision of cell site location information depends, in part, on the size of the coverage area of each cell tower. This means that as the number of cell towers has increased and the coverage area for each cell tower has shrunk, cell site location information has become more precise.

---

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

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

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

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

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

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

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

---

[5] *Hearing on Electronic Communications Privacy Act Reform and the Revolution in Location Based Technologies and Services Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on Judiciary*, 111th Cong. (2010) (statement of Professor Matt Blaze at 5), *available at* http://judiciary.house.gov/hearings/pdf/Blaze100624.pdf; Thomas Farely & Ken Schmidt, Cellular Telephone Basics: Basic Theory and Operation (2006), http://www.privateline.com/mt_cellbasics/iv_basic_theory_and_operation/

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

[7] *Id.* at 13.

[8] *Id.* at 10.

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

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

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

### B. Tracking Vehicles

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

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

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

Location tracking enables law enforcement to capture details of someone's movements for months on end, unconstrained by the normal barriers of cost and officer resources. *See United States v. Pineda-Moreno*, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, J, dissenting from denial of rehearing en banc) ("The modern devices used in Pineda-Moreno's case can record the car's movements without human intervention—quietly, invisibly, with uncanny precision. A small law enforcement team can deploy a dozen, a hundred, a thousand such devices and keep track of their various movements by computer, with far less effort than was previously needed to follow a single vehicle.").

---

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

In *United States v. Jones*, 132 S. Ct. 945, 954 (2012), the Supreme Court held that a Fourth Amendment search occurred when the government placed a GPS tracking device on the defendant's car and monitored his whereabouts nonstop for 28 days. *Id.* at 954. A majority of the Justices also stated that "the use of longer term GPS monitoring . . . impinges on expectations of privacy" in the location data downloaded from that tracker. *Id.* at 953-64 (Sotomayor, J., concurring); *see also id.* at 964 (Alito, J., concurring). As Justice Alito explained, "[s]ociety's expectation has been that law enforcement agents and others would not -- and indeed, in the main, simply could not -- secretly monitor and catalog every single movement of an individual's car, for a very long period." *Id.* at 964 (Alito, J., concurring).

Justice Sotomayor emphasized the intimate nature of the information that might be collected by the GPS surveillance, including "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *Id.* at 955 (quoting *People v. Weaver*, 12 N.Y.3d 433, 442 (N.Y. 2009)). While even the limited collection of geolocation information can reveal intimate and detailed facts about a person, the privacy invasion is multiplied many times over when law enforcement agents obtain geolocation information for prolonged periods of time. As the D.C. Circuit Court of Appeals has observed, "[a] person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts." *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd sub nom. United States v. Jones*, 132 S. Ct. 945 (2012).

There have always been facets of American life that have been uniquely safeguarded from the intrusive interference and observation of government. Geolocational surveillance threatens to make even those aspects of life an open book to government. As Justice Sotomayor pointed out in *Jones*, "Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse." *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (quotations omitted).

While privacy rights are often conceptualized as belonging to individuals, they are also important because they ensure a specifically calibrated balance between the power of individuals on the one hand and the state on the other. When the sphere of life in which individuals enjoy privacy shrinks, the state becomes all the more powerful:

> The net result is that GPS monitoring--by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track--may alter the relationship between citizen and government in a way that is inimical to democratic society.

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

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

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

Furthermore, while the government routinely argues that records of a person's prior movements deserve less privacy protection than records of where a person travels in real time, this is a meaningless distinction. As one judge has noted, "[t]he picture of [a person]'s life the government seeks to obtain is no less intimate simply because it has already been painted." *In re Application of the U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827, 840 (S.D.Tex. 2010) (citation omitted). A contrary conclusion would eliminate privacy protections even in real-time data, because police officers would be free to use GPS devices to record vehicles' travels so long as they waited some minutes before accessing those records, thereby rendering them "historical."

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

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

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

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

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

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

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

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

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

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

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

In August 2011, 35 ACLU affiliates submitted public records requests with state and local law enforcement agencies around the nation seeking information about their policies, procedures, and practices for tracking cell phones.[13] The ACLU received over

---

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

---

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

[16] 132 S. Ct. at 964.

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

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

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

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

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

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

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

**Conclusion**

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

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

Mr. SENSENBRENNER. Thank you very much, and I want to thank all of the witnesses for making their statements within the time limit, that is not what usually happens around here. The Chair will defer asking questions and will begin by recognizing the author of this bill, the gentleman from Utah, Mr. Chaffetz.

Mr. CHAFFETZ. I thank you Mr. Chairman. And thank you to all the witnesses, I appreciate your perspective and the passion you bring behind those perspectives. I find it fascinating that there are now more wireless accounts in this country than there are people in this country. To say that the technology is not pervasive would be inaccurate, it is very pervasive and can be helpful in many ways, but it can also be confusing as we try to find and test the limits of where privacy starts, where it ends, and what law enforcement can do about this.

I also want to note, this bill is not intended to be solely focused on just law enforcement. What I am also worried about is somebody tracking and following somebody else in a surreptitious manner. The idea that somebody could take a spurned lover and put a GPS device or figure out how to track that person surreptitiously needs clarification of law. So this bill is not just about law enforcement, that has been the discussion thus far, but it is also about how do we as individuals track and follow other individuals without our own permission, and I want to make that clear.

I also want to highlight a comment, actually, from Jason Weinstein, a Department of Justice deputy assistant Attorney General who was called on Congress to clarify a law in this area, "There really is no fairness when the law applies differently to different people depending on which courtroom you are standing in."

In addition, the top FBI lawyer, Andrew Weissmann, has stated, "FBI agents in the field need clear rules." And it is telling agents who are in doubt, "Obtain a warrant to protect your investigation." I know through the work of the ACLU that the police in Lincoln, Nebraska obtained GPS location data on telephones without demonstrating probable cause, but in close proximity in Wichita, Kansas, they do demonstrate probable cause in order to obtain this information. And my understanding is since at least since 2007, the Department of Justice has recommended that U.S. attorneys obtain a warrant based on probable cause prior to engaging in these forms of cell phone tracking.

I guess my initial question here, and I also highlight a quote I used earlier from Justice Alito who was quoted as saying a legislative body is well-situated to gauge changing of public attitudes, to draw detailed lines and to balance privacy and public safety in a comprehensive way. I don't believe we can just leave this to the court and hope that 5 years from now, something percolates up to the top of the food chain.

I think that Congress has a proactive responsibility, and I am pleasantly surprised by the support we have from industry, they don't want people to be afraid of their mobile phones and they don't want people to be afraid of their automobiles and whatnot.

My question, first, to Mr. Ramsey here, you would have to agree, don't you, that there is great inconsistency and confusion, not only in light of just the *Jones* case, but from law enforcement agencies,

from prosecutors, where are the lines? Doesn't this need clarification one way or the other?

Mr. RAMSEY. FLEOA would agree that there does need to be clarification, but we feel that the way it is written is overly broad and we need to narrow that focus down to where it doesn't hinder law enforcement. As you said, this bill isn't targeting law enforcement; however, there are parts of it that might, for example, prevent apprehension of suspects.

Mr. CHAFFETZ. Understood, and I appreciate it. The point I guess I am trying to make, the need for legislation to move on this. Mr. Cassilly, would you agree with that? You actually, in your testimony, argued that the court should deal with this and that Congress shouldn't do.

Mr. CASSILLY. No, I didn't say that. What I said was that you can't show any evidence from court cases out there that seems to indicate a pervasive abuse by law enforcement of this ability. I think there are a couple of concerns. First of all, I think probable cause is a high standard, okay? My real case——

Mr. CHAFFETZ. My time is so short, I am already on to the yellow light here. There is a need to be consistent, you would agree with that? And would you also agree that there is great inconsistency? Even between Lincoln, Nebraska and Wichita, Kansas, between different courts and between what the FBI is saying, and what the Department of Justice is saying, there is great uncertainty and there is not a point of clarification thus far, correct?

Mr. CASSILLY. I agree that we need to come up with some general uniform rules, just in order to help the industry be able to respond and know whether——

Mr. CHAFFETZ. But you don't think law enforcement and the prosecutors and the courts needs some clarification as well? This is a 9-to-nothing case in the *Jones* case.

Mr. CASSILLY. I think we do, but I don't think we need to go as far as this bill goes. I think this bill would seriously prevent us from lawfully acquiring——

Mr. CHAFFETZ. So you may disagree with the standard, but you would agree that there is a need for a standard, correct?

Mr. CASSILLY. Yes.

Mr. CHAFFETZ. With that, I yield back, Mr. Chairman.

Mr. SENSENBRENNER. The witness should answer the question. Do you agree there should be a standard?

Mr. CASSILLY. I think there should be a standard. I don't think that the probable cause standard as set out in this bill is appropriate. There was a hypothetical, the actual case I gave you regarding the gang shooting, and the information we got in the gang shooting, that doesn't rise to probable cause standard. That is an anonymous informant, which everybody who deals with probable cause will know that that is not enough to allow us to proceed to get a warrant with an anonymous, untested informant. But it would be enough to allow us to establish a reasonable basis under other court decisions to request that sort of information.

Mr. SENSENBRENNER. Thank you. The gentleman from Virginia, Mr. Scott.

Mr. SCOTT. Thank you, Mr. Chairman. Mr. Black, if the police had five unsolved rapes using what essentially looks like the same

MO, and wanted cell phone information to ascertain if one cell phone had been at each of the sites at the appropriate time, would that be something that would be—should be allowed? And follow up on that, if there is a robbery on Times Square on New Year's Eve, would getting the cell phone information from everyone on Times Square that night also be available, or is there a difference?

Mr. BLACK. Maybe I will start with the second provision, I think that identifies the fact that when we are asking for information, location information, we are not asking a question of who is not there, we are asking a question where are people. So you are finding out a lot of information which, in some cases, is considered very private by the person who is being the subject of inquiry. And we do feel that a probable cause standard is not that high a standard, but it is an important—it a standard higher enough to protect some vital privacy rights.

In any specific example we can come up with, we would like the exceptions, scrutinized and I think worked with.

Mr. SCOTT. In the case of five different sites, five different times, is that targeted enough to satisfy probable cause?

Mr. BLACK. If there is a robbery in Time Square in a certain time frame, and you want to find everyone who was in Times Square at that point, I guess I would probably have some problem with that.

Mr. SCOTT. What about the five different rapes, five different times where it is unlikely that any more than one person would satisfy that search?

Mr. BLACK. I think there are adequate tools. I do not think that the information of that—that sounds pretty persuasive to me. We have legal precedents and maybe some other who has spent some time in criminal law. I think there will always be borderline cases. By and large, I really think the vast majority of law enforcement needs are not super time sensitive and can be met by a probable cause standard. What you are suggesting is a state of facts that make it pretty logical to want to get that information. To me, that gets close to probable cause.

Mr. SCOTT. Okay. Ms. Crump, should it make a difference whether or not the device is attached or the search is done without a physical attachment, say, to a car? Should that make a difference?

Ms. CRUMP. Thank you for the question. No, I don't believe that should make a difference. I think the Supreme Court decision, Justice Alito stated it well when he pinpointed the intrusion that occurs through tracking is the monitoring of someone's movements, particularly over an extended period of time. You can accomplish that by attaching a GPS device to someone's car, but you can obtain the same type of intimate private information by tracking someone through their cell phone. And because the relevant factor is a degree of privacy invasion, the physical attachment of the device is not the operative thing here.

Mr. SCOTT. Now people have used the term "warrant with probable cause." Is there such a thing as a "warrant without probable cause"?

Ms. CRUMP. Not generally, no.

Mr. SCOTT. Okay. Should—if you have a warrant, should the person being surveilled be notified the same way they are notified in any other warrant?

Ms. CRUMP. I think it depends on the context. In general, there are exception for notification when warrants are served. So for example, if it would interfere with an ongoing law enforcement investigation. I think that one could certainly make an argument that if you were tracking someone for the purposes of a criminal investigation and notifying them of the tracking would interfere with that investigation, that there is a strong argument to be made that as in, for example, Historic Communications Act, there would be a good reason to have a provision that upon a good cause showing you would be exempt of that requirement. I think you can accommodate the privacy interest here while also making reasonable accommodations such as that for compelling law enforcement interests.

Mr. SCOTT. Does the bill have an exemption for searches done under FISA?

Ms. CRUMP. Yes, the bill has that exemption which would allow for important national security investigations to go forward. That is one a number of reasonable and limited exemptions including for consent, for monitoring minor children when their parents wish it to be done, and for various emergency circumstances, such as, for example, when someone is in danger of their life or serious bodily harm.

Mr. SENSENBRENNER. The other gentleman from Virginia, Mr. Goodlatte.

Mr. GOODLATTE. Thank you, Mr. Chairman. I very much appreciate your holding this hearing on legislation and this important evolving technology. And I want to thank and commend the gentleman from Utah, Mr. Chaffetz, for introducing the legislation which I am pleased to cosponsor.

I would like to start by asking all for of you, and I will start with the representatives of law enforcement first. In examining practices of State and local law enforcement, what has the experience been in those jurisdictions which require a probable cause warrant standard for the attachment of these devices?

Mr. RAMSEY. I would probably have to defer to Mr. Cassilly here on the State and local law enforcement aspect of that nature.

Mr. CASSILLY. I am sorry, Congressman, I can't answer that because I am not aware of—other than until I heard about Wichita, I am not aware of a jurisdiction that did—does require probable cause for access. Most of the jurisdictions that I am aware of use a reasonable basis standard.

Mr. GOODLATTE. Mr. Black or Ms. Crump.

Mr. BLACK. Well, we don't collect that information on law enforcement, but I can tell you that a warrant clearly provides a clear message that a private sector company can feel much more confident responding to without running the risk of violating their customers' rights. It is a clear legal standard that response to that warrant has been established. I think it provides a level of protection to the private sector as well as for the customer and citizen.

Mr. GOODLATTE. Ms. Crump, maybe you know of some jurisdictions that impose that standard?

Ms. CRUMP. Thank you for the question. When we conducted our 35—our 32-State survey, we uncovered a small number of jurisdictions that do require a warrant based on probable cause to track

even cell phones. So, for example, the County of Hawaii, Wichita and Lexington, Kentucky all reported to us that they require a warrant based on probable cause. I do not believe that those jurisdictions would willfully put their citizens in danger in order to impose this requirement. I think it is a more reasonable conclusion to believe that they can accommodate legitimate law enforcement interests while also accommodating the warrant requirement, and that is a reason the requirement set out in the GPS Act are reasonable ones.

Mr. GOODLATTE. Although the court concluded that the government's action in *Jones* was a search, none expressly required that police get a warrant in future GPS tracking cases. The government effectively forfeited that argument. Further, there is no clear indication of the level of suspicion, probable cause, reasonable suspicion or something less that is required to attach a GPS unit and monitor the target's movement.

So let me ask you each of you what level of suspicion, probable cause, reasonable suspicion or something less should be required to attach a GPS unit and monitor a target's movements or monitor a target via a cell phone. We will start with you, Mr. Ramsey.

Mr. RAMSEY. The way I understand the question is you are asking for at what level?

Mr. GOODLATTE. Finish the work the court, they punt it over to us and help us find the best way to set a standard that protects the privacy rights of individuals and particular innocent citizens. Our bill, as you know, requires probable cause as a standard, but if you are troubled by that, make a case for another standard.

Mr. RAMSEY. A lot of times these geolocational devices are used as building evidence, it is the building blocks in some of these investigations, working up to a probable cause warrant for an arrest of an individual. So if you start at the building block level, you are actually near the reasonable suspicion level.

Mr. GOODLATTE. I am running out of time so I am going to jump over to Ms. Crump, too, and if we have time, we will come back to Mr. Cassilly.

Ms. CRUMP. In our view the reasonable suspicion requirement is too low. The warrant requirement—the probable cause requirement is the basic default of under our constitutional system when there is a search. Law enforcement often mentions that it would be useful to track GPS and develop probable cause. However, there are a wide range of useful law enforcement techniques that law enforcement is not allowed to conduct without probable cause because they are simply too invasive. It would surely be useful for law enforcement agents to be able to search someone's phone without having to get a warrant. But we don't allow that under our system because we recognize that that is a grave intrusion.

When you talk about the type of information that is available through GPS tracking, for instance, being able to tell where someone gets medical treatment or whether they are an unfaithful husband, or who their friends and associates are. That is similarly sensitive and should be similarly protected.

Mr. GOODLATTE. Thank you, Mr. Chairman.

Mr. SENSENBRENNER. The gentleman's time has expired. The gentleman from Colorado, Mr. Polis.

Mr. POLIS. Thank you for holding this hearing, Mr. Chairman. I was considering joining as cosponsor of this bill, and based on what I am hearing today, I plan on doing so after this hearing. It has been very informative and appreciate it.

One question I had, and am not sure who can help me on the panel is how the process works with regard to identity list suspects, or John Does or people that, of course, and I would think if somebody is a serious criminal, they would have no identity attached to their cell phone, it would simply be an anonymous cell phone. Is there a procedure under law enforcement, and perhaps Mr. Cassilly or Mr. Ramsey would know that allows for a warrant for a John Doe in terms of following them on GPS or tracking their cell phone.

Mr. CASSILLY. Often we do get phone numbers. For example, if a victim called and lured to a specific location and the victim has the suspect's phone number on their phone, we would do a petition check. We use court order, so we would do a petition for a court order, and cite the cell phone, the number, information on that specific number.

Mr. POLIS. This bill would not impact that process; is that correct?

Mr. CASSILLY. It would if it requires a probable cause warrant.

Mr. POLIS. Well, it would insofar as it does it the same way if you have their identity, but it doesn't do it separately. There would still be a way of doing it based on the cell phone number with probable cause.

I tend to agree with what Ms. Crump said, if you are talking about somebody's home, somebody's private conversations and where they are, these are very intimate matters and deserve all of our privacy protections. And obviously, we are focusing a lot on the violation of privacy for criminal investigation side, but I want to open this up a little bit about some of the positive applications from a consumer perspective with regard to GPS, and some of the potential lifesaving technologies. And I want to ask Mr. Black whether he thinks this bill will in any way stand in the way of lifesaving services or ambulances or other fire-reduction services that are going after people who are on cell phones and have GPS. Does this interfere with some of the positive side of this at all?

Mr. BLACK. Thank you for the question. I think, to the extent that lifesaving situations involve maybe law enforcement as well, clearly the exceptions, I think, are sufficient to cover those circumstances. I would suggest that people value their privacy enough that there will be times if, in fact, easy access to their location information transpires, turning off your phone becomes a customer consumer reaction which we don't want. We don't want people feeling they don't want to be followed so they are going to start turning off their phones, and then get in an accident or critical situation and that is not available.

So I think given a degree of security and trust that you will not be casually surveilled is actually helpful in making sure people use all the benefits of their cell phone, including their location identity information.

Mr. POLIS. So people would be more likely to keep their cell phones during potential emergency situations if they have privacy

assurances there as well. And I assume many of the privacy specifics can be dealt with in user agreements with cell phone providers as well. Many people may choose to, in fact, allow for emergency purposes, their provider to know where they are, they might have some kind of biometric feedback if they need their heart rate monitored and ascribe to privacy to that. And again, I would think, in general, people are more likely to do these kinds of lifesaving activities if they are assured that this information will not be used for ulterior reasons or by "the government" or by anybody else. It would just be a private arrangement with their medical care provider.

And again, there is tremendous promise of the biometric feedback of saving lives, whether it is simply monitoring insulin level or it is heart rate or a number of other conditions. And to the extent we can increase confidence in these by reassuring privacy, I think we can save lives through this law. So I plan on joining as a cosponsor and I thank the Chair for the hearing and I thank the witnesses for coming forward.

Mr. SENSENBRENNER. The gentleman's time has expired. The gentleman from South Carolina, Mr. Gowdy.

Mr. GOWDY. Thank you, Mr. Chairman. Ms. Crump, it has been a while since I studied Constitutional law or search and seizure. What is the standard required for physical surveillance if law enforcement just wants to follow someone?

Ms. CRUMP. The Supreme Court has set different standards for physical surveillance and electronic surveillance. Physical surveillance, the Supreme Court has not required a warrant based on probable cause to carry it out.

Mr. GOWDY. That is what I thought. So you can follow someone in their car without meeting any standard of proof?

Ms. CRUMP. That is right, and I think——

Mr. GOWDY. What about air space surveillance?

Ms. CRUMP. I think that is a similar rule. The line that Justice Alito——

Mr. GOWDY. I am not going there yet, we are not there yet. I am just asking you about physical surveillance, both on land and air. And there is no probable cause requirement for either.

Ms. CRUMP. That is certainly correct.

Mr. GOWDY. What about grand jury subpoenas, what is the standard required to issue a grand jury subpoena?

Ms. CRUMP. Generally it would be relevance.

Mr. GOWDY. Right. So could a Federal prosecutor send a grand jury subpoena to a service provider and get their passive GPS historical GPS information?

Ms. CRUMP. I don't believe so.

Mr. GOWDY. Why not?

Ms. CRUMP. Because of the current restrictions of the Historic Communications Act which already sets a standard for tracking location.

Mr. GOWDY. So what would a prosecutor have to do to get that?

Ms. CRUMP. To obtain cell site location information under the Historic Communications Act. Right now, prosecutors have to show that the information is relevant and material to an ongoing investigation.

Mr. GOWDY. That is my point it is not probable cause, it is a relevance standard, so that is what I asked. Right?

Ms. CRUMP. I misunderstood then.

Mr. GOWDY. No, more likely, I misphrased my question. What about folks on probation, what is the standard, if any, for GPS monitoring of folks on probation?

Ms. CRUMP. Probationers have generally been recognized have fewer Fourth Amendment rights.

Mr. GOWDY. Right, because they have already been convicted. How about folks who are on bond and are still presumed innocent, what is the requirement for GPS tracking of folks on bond?

Ms. CRUMP. It is similar.

Mr. GOWDY. Similar in that it is not probable cause?

Ms. CRUMP. That is right.

Mr. GOWDY. All right. Orders of protection for women who have been battered and go to a court, and one of the conditions of the order of protection is GPS monitoring. What is the standard there?

Ms. CRUMP. You have reached one actually that I am not particularly familiar with that area of law, so I am afraid I cannot answer.

Mr. GOWDY. It is not probable cause.

Mr. District Attorney, Jason Chaffetz and Chairman Goodlatte are two of the most reasonable people in Congress. Period, new paragraph.

Mr. SENSENBRENNER. Without objection, so ordered.

Mr. GOWDY. My——

Mr. CASSILLY. Mr. Goodlatte left, he didn't hear that.

Mr. GOWDY. Well, I am sure the transcript will reflect that I meant that with a lot of earnestness, because I did. I am biased toward law enforcement and prosecutors. So how can you get together with Mr. Goodlatte and Mr. Chaffetz and come up with something that meets their legitimate privacy in Constitutional privacy expectations and still doesn't hamper law enforcement's ability to investigate cases for which probable cause has not been developed yet?

Mr. CASSILLY. I would be very glad to do that. I still assert that a reasonable basis standard which is used, recognized by the United States Supreme Court and used throughout law enforcement for many, many decisions would be a proper protection.

As far as protecting the industry from knowing whether or not the request is legitimate or not, using a court order without requiring that the court order be a warrant. Once you change the word "court order" to "warrant," you complicate the situation because warrants require a lot of service and notice, as opposed to a court order, which is used for things like wiretaps and other types of electronic surveillance.

Mr. GOWDY. But you are happy to sit down on behalf of District Attorneys and work with Mr. Chaffetz and Mr. Goodlatte?

Mr. CASSILLY. I would be happy to do that.

Mr. GOWDY. Thank you, Mr. Chairman.

Mr. SENSENBRENNER. Gentleman's time expired. The gentlewoman from California, Ms. Chu.

Ms. CHU. Thank you, Mr. Chair. Mr. Black, in your testimony you provided some very interesting statistics in regard to smartphone users; you said that only 6 percent of Americans use

geolocation or apps, and that 70 percent of users are completely unaware that they exist. So I would like to ask you and Ms. Crump, some out there might argue that cell phone users voluntarily make their locations known because they carry a cell phone by choice. How would you respond to that statement?

Mr. BLACK. I think certainly making it available to a particular user, or for a particular purpose, is not making it available to the world for all purposes and not making it available to all other third parties. So yet, people may, in fact, say I am willing to have this in order to have an entity communicate with me, but that does not mean I want to be followed everywhere and my location known by a variety of people who I do not choose to have given access to.

Ms. CHU. Ms. Crump.

Ms. CRUMP. I agree with everything Mr. Black just said. Today it is difficult to function in our society without having a cell phone. I think it is a mistake to equate a decision to carry a cell phone with a decision that you do not mind being tracked 24 hours a day, 7 days a week. I think that in our society, there is a lot of information we might, for example, choose to release to someone for a limited time, or for a limited purpose, but that does not mean we would want everyone to have access to the same information, or that we would feel comfortable being tracked by law enforcement. So I think there is a meaningful distinction between disclosing location information to a cell phone company and disclosing it to everyone.

Ms. CHU. Thank you.

And, Mr. Black, you also said that companies should treat geolocation information with the highest respect when it is gathered from users. How far could potential abuse go in terms of the private information obtained?

And Ms. Crump, too.

Ms. CRUMP. I am sorry, the question was how far could——

Ms. CHU. How far—to what extent could private information be obtained? How far could it go?

Ms. CRUMP. It could actually go quite far. We have much personal and sensitive information in the hands of third parties today simply by the way that our devices function. It is not simply that we store all of our location information with our cell phone companies; we store all of our emails with third-party companies such as Google.

And so if we don't establish firm guidelines to indicate that our private information is still private, even in our increasingly digital and interconnected age, Americans will end up forfeiting rights that we have held dear for a long time.

Mr. BLACK. I would agree. The fact is, modern digital technology has great benefits, but it does open up the potential for great access into people's private affairs.And that is what we are trying to do. We are trying to—the level of intrusion, unwarranted and unconsented intrusion into people's private affairs—their location, their sensitive data, a variety—is something that we need to guard against.

I love my industry, I love our technology, and it does great things, but there is a potential dark side. And what we are trying

to do is make sure that we have sufficient safeguards to make sure that the very fundamental, vital privacy protections are preserved.

Ms. CHU. Well, in fact, you write that, by having location privacy access, that you could show not just where people work and sleep but also religious preferences, doctor visits, political affiliations.

Mr. BLACK. Exactly. I mean, the amount—what you learn by being able to monitor precisely someone's location over a period of time can reveal all kinds of sensitive things. It is not just illegal behavior; it is all kinds of personal, private information—health care.

I mean, not everyone can do it everyplace, but technology clearly exists. And I think Matt Blaze's testimony says, not only can you identify where they are in a building but what floor in a building, so what doctor offices, what specialty they are in.

I mean, you are talking about a surveillance, monitoring capability which can be very detailed, very intrusive. And the longer you can do it, the more complete you do it, the more you can find out the most intimate facts about an individual.

Ms. CHU. And is it possible that smartphone users might be hesitant to use their device because they fear that the government will invade their privacy?

Mr. BLACK. I am sorry, I didn't hear the whole question.

Ms. CHU. Well, you refer in your testimony to smartphone users not wanting to use their devices because of privacy invasions.

Mr. BLACK. I am sorry, my hearing.

Mr. SENSENBRENNER. The witness will answer——

Ms. CHU. Well, thank you.

Mr. SENSENBRENNER [continuing]. The question.

Ms. CHU. I yield back.

Mr. SENSENBRENNER. Okay, she yields back.

The gentleman from California, Mr. Lungren.

Mr. LUNGREN. Thank you very much, Mr. Chairman.

I am sorry I wasn't here for your formal presentations, but I will continue to look at this.

Here is the dilemma I find. We have several generations of Americans who utilize devices today to tell everybody in the world who they are and what they are and, you know, Facebook and so forth, where they are revealing so much about themselves and, at the same time, they somehow have an expectation of privacy, even though they have given information to the very intimate thing called the Facebook. And sometimes it is difficult in conversation with folks to say, well, you have exposed all of this to the world, and now you have this expectation of privacy. And so we have almost different perspectives now on what the reasonable expectation of privacy is.

As an elected official, I find my privacy invaded by something called trackers today. I mean, you walk out of a building here, and someone is in your face with a smartphone asking you a question equivalent to, "When are you going to stop beating your wife?", and if you don't answer it, it looks like you are running away from it. One of the great techniques people have figured out on that is to pull out their own cell phone and to start talking with their spouse.

And so, as Mr. Gowdy was saying, what is required for law enforcement to have somebody follow somebody? And is there an es-

sential difference between, you know, a human tracking and electronic tracking from a law enforcement standpoint, and how would you articulate that? And I would ask that to you, Ms. Crump.

Because I am struggling with this. I am trying to figure out what would be reasonable. Having been on the law enforcement side, I understand the necessity of gathering information. And the general rule is, if it is somehow publicly available, you don't have that expectation of privacy.

And so, how should we analyze this in terms of the—if I, in law enforcement, have an unlimited number of police officers, men and women, I could pretty well follow you. I can't go into the house, but I could wait outside wherever you go. I could know your location by making sure I have enough cops on the street. I don't think I have to go to a court to do that.

What is the essential difference, from an analytical standpoint, between having an unlimited number of cops available to do that and being able to track you by the device that you might have? And once we establish what that analytical difference is, what standard should be used, if any, to limit what law enforcement might do? Can you help me with that?

Ms. CRUMP. I think that is one of the most interesting and complicated questions in this area. And you are getting at the difference between physically following someone on the one hand and tracking them electronically on the other.

In a word, the difference is resources. Physically tracking someone requires a significant expenditure of resources on behalf of law enforcement, and that imposes a natural limit on the degree to which this intrusive form of surveillance can be carried out.

What has happened with the development of electronic tracking is, that natural limit has fallen away. So today is it possible for a law enforcement agency to track someone's movement in the comfort of the stationhouse simply by tracking the location of their cell phone. And I think——

Mr. LUNGREN. So what is the analytical application there? I mean, we don't define privacy standards by budgets, I presume, or by the comfort or discomfort of the law enforcement officer. So what should we be looking at to help us to come up with legislation that is appropriate?

Ms. CRUMP. Thank you.

I think the relevant factor is the degree of privacy invasion. And I think what motivated the Supreme Court's unanimous decision in *Jones* was the view by many of the Justices that tracking someone electronically for 24 hours a day, 7 days a week is simply a totally different animal than doing that the old-fashioned way by foot.

And because the technology has changed, we need to recalibrate the relevant legal standards. And I think the GPS Act does that quite well.

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

The gentleman from Georgia, Mr. Johnson.

Mr. JOHNSON. Yes, I was going to ask a similar question. My question would have been, if an automobile is situated in a public place and then law enforcement attaches a GPS device surreptitiously, what is the difference between that kind of surveillance and also just a physical surveillance, you put a tail on someone and

follow them around for 28 days or so? You could certainly follow someone around in a car—one car or two cars could follow someone for 28 days, and there would be no issue as far as privacy is concerned. Is that correct?

Ms. Crump?

Ms. CRUMP. Yes, thank you. I think——

Mr. JOHNSON. You could even follow someone from the air in a helicopter, you know, or perhaps even a drone. If you are following someone with a drone that just hovers overhead and tracks their movements without a GPS on the automobile, you could do that legally, could you not?

Ms. CRUMP. I think I would distinguish between the physical surveillance examples on the one hand and the drone and GPS tracking——

Mr. JOHNSON. Well, how about a helicopter?

Ms. CRUMP. And I think the helicopter is more like physical surveillance. You know, I think the salient difference is the ease with which this surveillance can be carried out. When——

Mr. JOHNSON. If it is easier than physical surveillance—well, if it is easier than physical surveillance on the ground, versus in the air, what are the implications?

Ms. CRUMP. I think to some degree an economic analogy is useful. People simply buy more of something that is cheaper. And when you reduce the cost of engaging in surveillance, the odds that someone will engage in surveillance where is it not necessary or doesn't serve a strong law enforcement purpose increases. And, therefore, it is a greater threat to privacy, and a higher standard is warranted.

Mr. JOHNSON. Well, Darrell Issa may come up with a device that interferes with the GPS signal from a car, and—I mean, the marketplace has something to do with this also.

Mr. Black?

Mr. BLACK. Well, I want to, I think, reiterate what my industry has done—and I love it—it has made it so easy to access this tremendous amount of private information. The resources, if you will, the prioritization of resources has acted as a certain natural check and balance on the overuse of extensive surveillance. What technology has done is made that cost de minimis, and will, frankly, make it even less so in the future. It gets smaller and smaller. So instead, not one person sitting in a police station watching one car; one person watching a thousand people that they now decided to follow.

So the ease of doing it is why we are saying that we need to recalibrate what the threshold is.

Mr. JOHNSON. Uh-huh. So that is—this is a very difficult situation that—I feel like yielding to Mr. Lungren.

Mr. LUNGREN. Yeah, will the gentleman yield?

One of the things that strikes me is, we see in a lot of cities now, they have a lot of cameras set up all over. And it has been controversial, but it is going on. Is there an essential difference between the ubiquitousness of cameras and being able to track somebody that way and this kind of a device? And is that difference that somehow you are invading the person's property interest—in other words, you are actually reaching out and touching them in order

to be able to follow them? Or you are receiving something from something which is actually touching them? Is that a—could I ask that question?

Mr. JOHNSON. Sure.

Ms. CRUMP. I think there are a few ways to distinguish the camera example from GPS tracking. The physical attachment is one of them. Some people recognize an indignity to having their own object be turned into a device which is essentially spying on them.

But also, today, cameras, generally speaking, capture one person at one point in time. They are not engaging in a type of continuous tracking. That may not be true in the future when all of these camera networks are, you know, networked together and can be easily be analyzed. But for right now, I think, where the technology is, there is a meaningful distinction.

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

The gentleman from Pennsylvania, Mr. Marino.

Mr. MARINO. Thank you, Chairman.

You raised the question, or you made the statement concerning the *Supreme Court v. Jones*, but you did not delineate their reasoning, to a certain extent. And when the Supreme Court stated that affixing a GPS monitor to track a car for weeks is within the meaning of the Fourth Amendment, it didn't address the search issue.

So how would you interpret the search issue? Would you put—ma'am, would you put a 2-week limit on the search issue? Or is it a search issue? Could you please respond to that?

Ms. CRUMP. Thank you for the question.

Law enforcement agencies have actually objected to the idea of establishing different criteria based on the length of search. And they have done that because they argue that that would be unmanageable, because how do you know how long, you know, a search is? If you track someone for a week and then wait another week and then track for a week, where does it categorize?

So, for that reason, I think it makes the most sense to establish a uniform and clear standard that will be easy to follow, and that should be a warrant, probable cause standard for all location tracking.

But you are certainly correct in how you characterize the *Jones* decision. That case involved 28 days of geolocation tracking——

Mr. MARINO. That is right.

Ms. CRUMP [continuing]. And Justice Alito specifically said that we are not reaching the question of how long tracking has to occur for it to be a search, but surely 28 days crosses any reasonable line.

Mr. MARINO. So do you draw a distinction between any type of potential crime or any type of investigation compared to—let's use a drug investigation. We want to monitor, but we don't want to tip off the drug dealer that we are monitoring. And I say "we" because I was in law enforcement for 19 years. So it would tip that individual off, in most cases, that he or she was being followed.

But let's take it to the next level. Let's take it to the level of a child being abducted, a child being taken by—we are not quite sure who the individual is per se, but we do have some reasonable information based on, say, a partial license plate, make and model of the vehicle, and to monitor that. Do you see a distinction there?

Ms. CRUMP. I think we all share the common intuition that some crimes are more serious than others, and a petty theft versus a child abduction should potentially be treated differently.

I think the GPS Act, as currently drafted, responds to that by, for example, including an emergency situation. So if a child is abducted and someone has a good-faith belief that the child is in danger, law enforcement would be able to engage in tracking in that case, even without meeting the warrant requirement. Similarly, in the bill there is an exception for national security investigations.

Mr. MARINO. So who makes that determination? You are going to allow law enforcement to make that determination on a case-by-case basis?

Ms. CRUMP. I think that this body is actually the appropriate one to make that determination. I think the current draft bill allows law enforcement appropriate flexibility, indicating the types of situations in which law enforcement should be able to track even where they don't meet the warrant requirement, while generally holding a warrant requirement in the vast majority of the investigations where the police have time to go to a judge and prove their case to a neutral magistrate.

Mr. MARINO. Okay, thank you.

I don't know what my time is, but does anyone else on the panel have a comment pursuant to those statements or questions?

Sir, please.

Mr. CASSILLY. Yes, I think one of the issues becomes the responsiveness of the service provider. I mean, as the Congressman asked the question, who determines when you fall under the exception, I think the issue becomes, do the police run in to a disagreement with the service provider? Well, you know, we think their lives are at stake, and the service provider's response is, well, you know, we don't think so; you know, we are too busy right now. And I think one of the parts of this discussion should be, you know, what are the standards for the service providers to respond, the time limits that they have to respond.

And I do agree that part of the good thing that comes out of this is that there is some sort of a standard instrument that comes out of this discussion—court order or a certain subpoena—with a basis that industry can rely on and say, okay, this is a reasonable request, we are required to respond to this, and we do so in good faith.

Mr. MARINO. Good. Thank you.

I think my time has long expired. Thank you.

Mr. CHAFFETZ. [Presiding.] The gentleman yields back.

We will now recognize the gentlewoman from Texas for 5 minutes.

Ms. JACKSON LEE. I thank the Chairman very much.

And this is a very vital discussion. I offered some legislation just a while back dealing with privacy issues as a Member of the Homeland Security Committee, an opportunity for Federal agencies to talk together, or either the Department of Homeland Security to talk with Justice and another department. And, certainly, the issue of privacy was raised, and the amendment was challenged on that basis, even though I thought that I had adequately put in privacy provisions.

And so I would like to pose my questions from a perspective of someone who has seen the challenge of privacy head-on and values my commitment to privacy and would make the argument that, in the instance of the particular amendment that had to do a lot with terrorism and issues of that sort, that it was misunderstood.

But keeping that in mind, I vigorously believe that privacy is something that we should hold on to and deserves the ultimate standard of respect, while we recognize the challenges of law enforcement or those who are engaged in counterterrorism.

So I would like to ask Mr. Cassilly, just aside from all the discussions you have had with other Members and that you may have repeated this or said this before, from the law enforcement perspective—and I am going to ask you to wear a prosecutor's hat and police hat only because you are dealing with receiving information from law enforcement—what would be, in your mind, a sufficient privacy or structure of protection for getting information such as the data that says, "I was standing in a place today at a certain time," that is, phone data, making a phone call, or I was moving around, going toward another place, which is the information I understand that can be secured? What would be, in your mind, the privacy protection that law enforcement should adhere to or should consent to or should put in place?

Mr. CASSILLY. I think you are asking, just if I can clarify the question, what is the standard that we would use in being allowed to go forward to seek this information?

Ms. JACKSON LEE. Your clarification I think is a good interpretation of what I thought, you know, was clear, which is, what would you believe were satisfactory privacy parameters as you pursue getting this information?

Mr. CASSILLY. Well, I think that the proper standard, which is of course what the Supreme Court has said, with respect to law enforcement being able to go up and stop people on the street and to question them about crimes would be a reasonable basis. Do they have a reasonable basis, a reasonable suspicion, to make that inquiry, to stop someone on the street, if we are using that analogy? To detain them on the street, to require them to produce identification on the street, that requires a reasonable basis standard. And I think that would be——

Ms. JACKSON LEE. A reasonable basis of suspicion.

Mr. CASSILLY. Reasonable basis—reasonable suspicion of criminal activity. And I think that is the same standard that would work under these circumstances, to require law enforcement to be able to show a reasonable basis.

And they could show that either to the prosecutor in issuing a subpoena or through a petition to the court for a court order, as long as that was the requirement for the showing.

Ms. JACKSON LEE. With that in mind, let me—thank you, Mr. Cassilly.

Let me go to Ms. Crump. And in a calm Judiciary Committee room, that sounds reasonable, but I would say to you, since I am not a fan of stop-and-frisk, which I understand has taken over in epidemic proportions in areas like New York, I would be concerned, having issued probable cause warrants as a member of the judiciary, as a city court judge, and looking the officer face-to-face in

whatever disguise they were in, because I would get them 11:00, 12:00, early morning hours, because they were just coming off the street and get the warrant based upon their presentation in the courthouse.

Tell me your concerns about just that standard. Because what I see is potential, not purposeful havoc and not mean-spirited havoc, but I see havoc. And tell me what the basic corners of the concern would be. I just see tracking going on.

Ms. CRUMP. Thank you for the question.

I think one of the aspects of this debate that your comments highlighted was the importance of a judge being interposed between a citizen and the police. We have a tradition in this country of interposing magistrate judges between the citizen and the police, and it is not because we don't trust law enforcement agents, but it is because we believe, as the Supreme Court has said, that often there is a need for an objective mind to weigh the evidence at hand. And I think that it is important when location tracking is at issue for there to be that interposition between the citizen and police.

Ms. JACKSON LEE. Say that——

Mr. CHAFFETZ. Thank you——

Ms. JACKSON LEE. Could I just have her repeat? Objective mind——

Ms. CRUMP. It is important to have an objective mind interposed between the citizens and the police.

Mr. CHAFFETZ. Thank you——

Ms. JACKSON LEE. Well, let me thank you very much. I yield back.

Mr. Chairman, may I just inquire to you directly and just indicate that, as I am looking at the legislation, H.R. 2168, if I might inquire, you think the legislation has an objective mind interposed in between the decision?

Mr. CHAFFETZ. Yes, I do. Yes, I do.

Ms. JACKSON LEE. All right. I thank the Chairman. I yield back.

Mr. CHAFFETZ. Thank you.

Now we will start a second round of questioning, and I will recognize myself for 5 minutes.

There are a number of exceptions that are put in here. Mr. Ramsey and Mr. Cassilly, is there anything that you would add or subtract to those list of exceptions as you have been able to look at the bill?

Mr. CASSILLY. Well, as I pointed out in my testimony, I think that the exception with respect to consent needs to be expanded to not only cover children's phones but to cover phones of persons who may be mentally limited or who may be ill.

We recently had a case in Maryland where an individual who was going into a diabetic episode was not able to respond to 911 operators to tell them where he was. Under those circumstances, either it is an emergency situation, if it doesn't fall under the life-threatening exception, there certainly should be some way of just asking a relative, "Okay, is it okay if we locate his phone?", something like that.

But usually for someone who may be mentally limited, they are not going to—you know, they may function fine, they just may not be there.

Mr. CHAFFETZ. Okay.

Mr. CASSILLY. So we think that ought to be a thing. I think you have two emergency exceptions in the statute; I think they need to come together. And I think that the emergency needs to be a little broader than just, you know, serious injury and death. That is a——

Mr. CHAFFETZ. Let me do this in the essence of time. Perhaps if you could respond and give us any adaptations that you would like to see to the bill in general, but specifically to the exceptions.

I would offer that to all of you, as well.

Much of this is based on the wiretap statute. Is there anything that you don't like about the wiretap statute that you would also—you would change in this bill but you would also change in the wiretap statute?

Mr. Ramsey?

Mr. RAMSEY. We wouldn't have an opinion on any changes to the Title III wiretap statute.

Mr. SENSENBRENNER. Mr. Cassilly?

Mr. CASSILLY. Well, I mean, I wouldn't want to see any changes reflected on Title III. But when you look at Title III, Title III requires a probable cause finding. And when you end up saying that there you actually get the contents of the communication, whereas here you are only getting, you know, a location of a cell phone, that if you are looking at it from a perspective of the degree of intrusion, that would say to me that then you would only require under these circumstances a reasonable, articulable suspicion.

Mr. CHAFFETZ. Okay.

Ms. Crump, Mr. Cassilly contends in his written statement that his organization believes, quote, "It is imperative to distinguish between historical data compiled from cell tower hits and realtime GPS ping information." Could you comment on that?

Ms. CRUMP. Thank you for the question.

I don't think the distinction between historical and realtime data is a meaningful one. As one court has remarked, the story of your life doesn't become any less sensitive because it has already been written.

Today, cell phone companies store historical information about us for very lengthy periods of time. Some cell phone companies keep records of where we have been for over a year. And I think, in light of that, many Americans believe that where they have been for the past 60 or 90 days is at least as sensitive as where they are going in realtime.

Mr. CHAFFETZ. Let me also ask you, Mr. Ramsey contends that there should be a lower standard of law enforcement to access geolocation information from smartphones and other mobile devices than the standard for attaching tracking devices to cars, because in the case of smartphones, quote, "the government doesn't own nor are they attaching the locational device to the person," as was obviously the case in the *Jones* case.

Can you comment on that?

Ms. CRUMP. My instinct on this is the same as Justice Alito, that the relevant privacy invasion is the tracking of someone, not the property invasion. And, therefore, I think the distinction between physically attaching a GPS device to a car and obtaining equivalent

information from a cell phone company or an OnStar navigation system is not one that the law should reflect.

Mr. CHAFFETZ. And, finally, in the essence of time here, again, we focused all on law enforcement; my intention with this legislation was also to make this applicable to non-law-enforcement entities.

Is there anything in the bill that troubles you in terms of, is it civilians or average citizens out there tracking or following other individuals? Because right now they are not precluded from doing so, in many of these cases. Is there anything that bothers you outside of the scope of law enforcement that you would change?

Mr. Ramsey or Mr. Cassilly?

Mr. CASSILLY. I think there is some concern over the industry, the folks who work for the industry being intimidated somewhat by complying with a legitimate law enforcement request by the fear of becoming criminally or civilly liable. And I think that needs to be clarified, as well as more specifics on what sort of cooperation law enforcement can expect back from the industry, when we can expect to receive information and that sort of thing.

Mr. BLACK. If I could respond, yes, certainly I think industry very much wants a clearer standard. And one of the reasons we want a reasonably high standard is because being deluged with tens of thousands of requests at a lower standard frankly becomes quite burdensome and requires decision-making at a much different level.

First of all, keep in mind, we have a wide range of companies who may get involved here. We are not just talking big Internet platforms. We are talking a lot of companies that may be much smaller, do not have legal counsel, do not have a range of capability and structure to deal with that.

So, particularly, there was some reference to, I think in testimony, to a mandatory response time situation. Any fixed time would be very harmful. The DMCA uses the word "expeditiously" in terms of response—I think any legislation talking about industry response needs that flexibility because of the diversity of providers that exist.

Mr. CHAFFETZ. Thank you.

I now recognize the Ranking Member, Mr. Scott, for 5 minutes.

Mr. SCOTT. Thank you.

There are a number of exceptions in the bill. Mr. Black, should there be an exception if the evidence is getting away—that if you delay and get a warrant, the person will escape and you won't know where they are?

Mr. BLACK. Your question is with regard to the exception relating to——

Mr. SCOTT. Where there are life and death exceptions, people's lives are in danger. Do you have that exception?

Mr. BLACK. Well, certainly——

Mr. SCOTT. What about, the bank just got robbed and the people are getting away, and if you can get the information right then, you might be able to catch the person, and if you wait 45 minutes, they would have gotten away. Is that an exception?

Mr. BLACK. I think we start out with the assumption that the exceptions that we see provide for most emergency situations, and

that to the extent the exception needs to be broader, there is a great deal of privacy risk at stake. And I would like to see the law enforcement justification as to why the current exceptions really aren't adequate to cover specific——

Mr. SCOTT. Mr. Ramsey, would you want an exception for the evidence that is getting away?

Mr. RAMSEY. I think that would be appropriate for all law enforcement——

Mr. SCOTT. And how do you cover that—is there an exception now with other warrants, that if you had a search warrant, you need to get the information right away or it may get away, and then you get an after-the-fact warrant?

Mr. RAMSEY. You have hot-pursuit exceptions that—you have exceptions to a warrantless arrest or situation.

Mr. SCOTT. Okay, so a hot-pursuit type of warrant would be an exception that would—Ms. Crump, what do you think about a hot-pursuit exception?

Ms. CRUMP. In the Fourth Amendment doctrine, that is well-recognized exception, and I could imagine a reasonably crafted exception here that encompassed the same idea.

Mr. SCOTT. Okay.

Who pays the costs of all of this? Mr. Black indicated a deluge of requests. That would obviously have cost implications to a phone company. Who pays the additional costs to responding to all of these requests?

Mr. BLACK. Under some existing statutes, there are cost referral situations, and companies do get some compensation. I think we have to—while companies are not anxious to incur the burden without compensation, on the other hand we want to make sure that this does not become a profit center for companies. We do not want them encouraging law enforcement to come undertake unnecessary and widespread surveillance in order to get revenue.

Mr. SCOTT. Thank you.

Do the different phone companies keep different data? Apparently, they can keep track of where you have been, because as you travel your phone pings the cell, so they can find out all the cells where you were. There are also business records of when and where you made a call.

Do different companies keep different data, Ms. Crump?

Ms. CRUMP. Yes, they do keep some different data, at least in terms of the length of time that they store the information.

So, for example, we were able to obtain through a Public Records Act request a one-sheet document from the Department of Justice in which it summarized how long different carriers kept different forms of location information. So, for example, Verizon stores the cell phone towers used by a mobile phone for 1 rolling year; T-Mobile keeps it for 4 to 6 months officially but, quote, "really a year or more"; and AT&T Cingular retains it from July 2008. So who your carrier is impacts——

Mr. SCOTT. Is that the fact that you made a call or where you were?

Ms. CRUMP. That is an excellent question that I would like to know the answer to.

Oh, I am sorry. Let me clarify that. That is where you were, but the precise nature of that information, how precise it is, is something that neither carriers nor law enforcement has disclosed.

Mr. SCOTT. Okay. But how long—if you made a call, how long is that kept? Is that a different list?

Ms. CRUMP. That is a different list.

Mr. SCOTT. Okay.

Ms. CRUMP. And it is also on this piece of paper, but I don't have it with me.

Mr. SCOTT. Okay.

Now, Ms. Crump, you said there was no difference between the historical record and realtime data, but should there be a different standard in getting information that you made a phone call from Times Square on New Year's Eve, yes or no? Should there be a different standard from realtime tracking?

Because, but for the privacy, electronic privacy records, a fact that you made a phone call would be a business record that you could scoop up on a relevance basis.

Ms. CRUMP. I agree with the general idea that as the information becomes more precise, it is more sensitive. However, the GPS Act provides a uniform standard, because law enforcement——

Mr. SCOTT. Even for getting a historic business record should be the same standard as realtime tracking?

Ms. CRUMP. I don't think it is fair to view cell phone location data as just another form of business record. Similarly, you know, our email is, in some sense, Google's business record if we have a Gmail account because it is all stored there. I think today it is more like, you know, a safe deposit box. We are entrusting something valuable about us to a third-party company, and that is different from it being just the business record of a bank.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. BLACK. If I would have a chance to comment, I would very much echo that. I think the technology in the email reference was on point. If we go to the concept that the data used by technology companies to perform their functions are just business records, then a massive amount of information about everyone becomes available under a lower standard.

Mr. CHAFFETZ. The gentleman's time has expired.

We will now recognize the gentleman from South Carolina, Mr. Gowdy, for 5 minutes.

Mr. GOWDY. Thank you, Chairman Chaffetz.

I will resist the temptation to ask about the expectation of privacy with emails that can be easily forwarded to the rest of the world. And I will instead ask Ms. Crump, you gave a quote to the gentlelady from Texas which I tried to write down but I missed it. It had something to do with a credible—something. Credible intermediary? Credible objective?

Ms. CRUMP. I am afraid that my memory is no better about what I may have said.

Mr. GOWDY. I think you were referring to, it is better to have a neutral, credible, detached——

Ms. CRUMP. Magistrate judge, yes.

Mr. GOWDY. Right. Which then got me wondering who that credible, neutral, detached magistrate is with the automobile exception to the Fourth Amendment.

Ms. CRUMP. There is an exception when there is——

Mr. GOWDY. Then there is no credible, neutral, detached intermediary, correct?

Ms. CRUMP. Although in general the Fourth Amendment requires you to go to a——

Mr. GOWDY. I wasn't asking in general. I was asking about one of the exceptions.

Ms. CRUMP. There are exceptions in the automobile——

Mr. GOWDY. How about exigent circumstances? Who is the credible, detached, neutral intermediary with the exigent circumstances exception?

Ms. CRUMP. Similarly, because the circumstances are exigent, there is no requirement that you go to a judge.

Mr. GOWDY. How about the public safety exception? Who is the credible, neutral, detached intermediary between law enforcement and private citizens with the public safety exception?

Ms. CRUMP. I think you are pointing to another extreme example where we all recognize that there is——

Mr. GOWDY. How about the plain field doctrine? Who is the credible, neutral, detached intermediary between the public and law enforcement with the plain feel doctrine?

Ms. CRUMP. Because the plain feel doctrine doesn't implicate the same privacy interests, there is no——

Mr. GOWDY. How about the plain view doctrine?

Ms. CRUMP. I would have the same answer to that.

Mr. GOWDY. Border exceptions?

Ms. CRUMP. It depends on the nature of the search at the border, but——

Mr. GOWDY. Search incidents to arrest?

Ms. CRUMP. I think what you are driving at is that there——

Mr. GOWDY. What I am driving at is, there are lots of exceptions.

Ms. CRUMP. That is right, but that doesn't mean there isn't a rule and that the rule isn't probable cause. And that there is a good reason——

Mr. GOWDY. Well, some would argue the rule has been swallowed by the exceptions. I would imagine your entity might argue from time to time that the rule has been swallowed by the exceptions, not to put words in your mouth, but—well, let me ask you this. Can you help me come up with all the instances in the criminal justice system where probable cause is not required?

Ms. CRUMP. I think you have come up with a pretty good list already——

Mr. GOWDY. Yeah, but you——

Ms. CRUMP [continuing]. But they have a common unifying theme, which is usually either a reduced expectation to privacy because the information sought isn't sensitive——

Mr. GOWDY. How about drug dogs? What is required to bring a drug dog and search a car?

Ms. CRUMP. A drug dog and a car? There is generally no requirement that there is probable cause.

Mr. GOWDY. Well, it is an articulable suspicion, right?

Ms. CRUMP. Well, the Supreme Court is reconsidering drug dogs sniffs right now, but currently the standard——

Mr. GOWDY. But now it is articulable suspicion. So we have—at one level, you don't have to have anything; you can just have a hunch. For instance, you can walk up to someone's house and do a knock-and-talk, and you don't have to have any basis to be able to do that. Police can stop and ask people questions, and they don't have to have any basis for doing that.

And then you can have an articulable suspicion, you can have a reasonable basis, and then you get to probable cause, which is the same standards you have to have to arrest someone. So you really want police to be able to make an arrest before they can get historical GPS information. You want the same standard to get the historical GPS information as you would have to have to make an arrest.

Ms. CRUMP. The arrest standard, like the house search and other standards, is a probable cause standard, and it is predicated on——

Mr. GOWDY. I am asking your opinion. You think that we should be able to make an arrest before we can get the historical GPS information.

Ms. CRUMP. Well, I don't think the standard for—no, I don't. And the reason is, to get probable cause for location information, you have to have a good reason to believe that a search will turn up evidence of a crime. So it is a different type of probable cause than actually physically arresting someone.

Mr. GOWDY. There is not a different definition for probable cause depending on whether it is an investigation or whether it is an arrest.

Ms. CRUMP. Well, when you are going to arrest someone, you have to have probable cause that they have committed a crime.

Mr. GOWDY. Right.

Ms. CRUMP. The only distinction I was drawing is that, to obtain geolocational information, you have to have probable cause to believe that a search will turn up evidence of a crime.

Mr. GOWDY. My time is up.

Mr. CHAFFETZ. The gentleman's time has expired. Yields back.

We now recognize the gentleman from Georgia for 5 minutes.

Mr. SCOTT. Thank you.

This is an area with unlimited implications, and so I appreciate all of the witnesses today for your diligence in responding to some difficult questions.

I will ask one, though, and it may not be too difficult, but—I understand that when you walk into a grocery store that there are things in the grocery store that connect with your cell phone and they can track you walking around in the store and then send a message to a screen, where you might happen to be pondering whether or not you should do what you always do at the store, and that is get that cherry pie even though you are on a diet and everything. And them, boom, they start flashing out to you, "Cherry pie, 50 percent off," you know, "Get one now," you know.

Is that a violation of—would that be a violation of this proposed legislation?

Mr. BLACK. I suppose I ought to try that. No, we have a consent—we have users, basically, you have—the owner of the cell

phone has a choice as to those kinds of services being made available or not.

Mr. SCOTT. Well, I mean, a lot of people have cell phones and then we come up with new technology——

Mr. BLACK. That is right.

Mr. SCOTT [continuing]. And there was never a consent given in the agreement for the cell phone.

Mr. BLACK. I think it is important to point out that our industry has found a great deal of sensitivity in the public to privacy. Facebook has made some changes, and there have been outcries. Google merely consolidated existing privacy policies, and there was wild outcry. There is an FTC oversight that has taken actions in a number of places. Consumer boycotts exist in many instances.

The empowerment of the user community out there is very, very real. And I think you have a lot of free market operation to balance and control with, if you will, abusive practices. People may exceed what somebody might find comfortable, but there really are mechanisms in that world to push back.

Mr. SCOTT. So you are suggesting——

Mr. BLACK. That is different than somebody knowing and being able to use that in an adversarial proceeding, which I think is what the bill is largely focused at.

Mr. SCOTT. Well, if there was a crime committed with the DNA from a discarded paper plate with the residue of cherry pie on it, and law enforcement subpoenaed the records of the Harris Teeter store to see whether or not you purchased a cherry pie on a particular day shortly before the——

Mr. BLACK. If there was only one cherry pie sold in the city and somebody bought it, maybe you could build a probable cause standard.

Mr. SCOTT. Yeah, I mean, but I still need to get an answer for my question. Does this kind of scenario, the store or whoever it is in control of capturing the data while you are walking around in the store, would that be an illegal act under this legislation that is proposed? Can someone answer that?

Ms. CRUMP. I believe I can answer. And as I read the definition set out in the statute, that is not covered, because the definitions target the provider of an electronic or remote computing service or the provider of a geolocation information service. And because the store itself is not one of those services, I don't believe, at least under the current draft, that it is covered.

Mr. SCOTT. Well, then, would it cover law enforcement?

Ms. CRUMP. To take your cherry pie DNA example, I think in that case it wouldn't be covered, because this bill deals exclusively with tracking people through electronic devices. You know, if law enforcement was trying to track someone, you know, the cherry-pie eater's movement after the fact, the bill would cover it if they did so through their cell phone or GPS. But it wouldn't cover the precise scenario you mentioned.

If you don't mind, I will also mention that your initial hypothetical was quite realistic. There was a mall that actually tried tracking people's movements through their cell phones. And when the public found out about it, their outrage was so great that the mall quickly announced it had discontinued the practice. And I

think that is a good example of how location information is still considered to be quite sensitive even in this digital age and why this act is so important.

Mr. CHAFFETZ. Thank you. The gentleman's time has expired.

We will now recognize the gentlewoman from Texas for 5 minutes.

Ms. JACKSON LEE. First, I want to acknowledge I think this hearing is enormously important, and I think the work that is being done by law enforcement is equally important.

Mr. Ramsey, I did not mention that local law enforcement is also involved in counterterrorism, to the extent that individuals spread out into our respective communities—and as I indicated, I am on Homeland Security.

But as I listened to my good friend from South Carolina lay out a litany of exceptions, I would make the argument that there is a framework upon which you can work with. And I just want to ask a simple question. Law enforcement is not interested in extinguishing privacy rights of citizens, is—I am asking you, Mr. Ramsey.

Mr. RAMSEY. You are asking me——

Ms. JACKSON LEE. Yeah, that is not your mission, to eliminate privacy rights of citizens.

Mr. RAMSEY. No, it is not. No.

Ms. JACKSON LEE. All right. So I just wanted to say that because I want to move on to other questions. And, as I said, this is a week where we are honoring police officers, and having been a former city court judge, I have dealt with officers a lot.

But I want to focus on Mr. Black and Ms. Crump. As I have said, as I listen to the long litany of exceptions, I become more comforted that we need to ensure that we have the right standards in this legislation that I am very interested in, H.R. 2168, but we do have, I think, a need to balance both rights. Because in the course of the stop-and-frisk—I am just on a metaphor statement here—in the course of the stop-and-frisk, innocent people are stopped and frisked. And that is the physical act of stopping and frisking individuals. And we know that, in the course of that that is under the label of law enforcement, there are individuals being stopped for no reasons whatsoever. And I think we have to protect against that.

So I just want to ask the question to Mr. Black. In these companies, generally, as you represent them, do they have a direct-dial number? Is there a number that law enforcement is assigned to? Or is it a random, pick up the phone, speaking to someone trying to get information?

Mr. BLACK. Well, certainly, in larger companies, there are well-established procedures to integrate with entities.

Ms. JACKSON LEE. Right.

Mr. BLACK. However, having said that, first of all, a lot of small companies are not able to do that. And even the largest companies, we are not dealing with just the Department of Justice or just even the State police; we are talking about jurisdictions of State, local, county, many, many different jurisdictions that may choose to try to contact companies in a variety of ways and different people.

So it is not clear that there is an easy channel always, even if both sides want it. The diversity—some, you know, a district attor-

ney, a sheriff in a variety of places—I mean, many, many requests come in.

And that is one of the problems I think we see, is that the—knowing this information is potentially—is there, the incentive to want it even when the need isn't that great, when, "Gee, it might be nice to know that," will geometrically expand the requests, increase the burden, and increase the amount of privacy intrusion that may not really be highly justified.

Ms. JACKSON LEE. And I wanted to get that on the record, because you all fall sometimes in the category of too big to fail or too big to be big, and so it looks as if you should be able to handle everything. But I think privacy is as important for the larger companies with larger portfolios of customers as it might be for the small guys.

The other point I want to make is that, if I am correct, I believe that there is certainly the right of police when it is a child victim involved to pursue this information and be insistent. I think under the legislation, if I am not mistaken, that children provide the cover for getting information quickly.

My next question would be, is there a sense of intimidation? If you are talking about different size companies, law enforcement calls up, is there a sense of intimidation or a sense of the urgency without seeking protections because you have law enforcement? Which means—it is the nexus to my point, that we need some parameters.

Mr. BLACK. Let me say first of all, I think my companies can be expected to be good citizens. We have numerous instances of receiving awards, some from law enforcement entities, for the rapid response in that situation.

Ms. JACKSON LEE. And that is good.

Mr. BLACK. Willing to do that. The difficulty, as I say, you start creating fixed rules that become very difficult to operate for different kind of companies in different kind of settings. But, clearly, an expeditious type standard—yes, we want to respond. There is no desire to do anything but respond in emergency-type situations.

I think, frankly, the availability of the exceptions in the legislation help underline the importance of the basic standard itself. The more we see good flexibility in the exceptions, the more necessary and desirable and dependable it is to have the probable cause standard.

Mr. CHAFFETZ. Thank you——

Ms. JACKSON LEE. I ask the Chairman for an additional 1 minute, just unanimous consent. I just need to follow up with Ms. Crump, just for a moment, please.

Mr. CHAFFETZ. Without objection, so ordered.

Ms. JACKSON LEE. I thank you.

Ms. Crump, with the litany of exceptions that, I must say, that you handled very well as you repeatedly were being posed a series of criminal exceptions that we understand here, doesn't that give you the sense that although we want to adequately equip our law enforcement, that there are sufficient exceptions that we should be very keenly pointed toward the privacy issues, and that the opportunity to track where you are going, where you have been, the op-

portunity to mislabel someone and misidentify, is crucial for us getting in front of this new technology instead of behind it?

Ms. CRUMP. Thank you for the question, and I couldn't agree more with what you said. There are numerous exceptions already to the Fourth Amendment, but that doesn't change the fact that the benchmark is a warrant and probable cause and that that serves a valuable function when law enforcement wishes to access deeply sensitive information about all of us.

The Fourth Amendment we often bemoan as having been eroded away too far, but there is a reason it was written into the Constitution. It is because the Founders intended there to be a balance between law enforcement interests and privacy interests. And this bill would help restore that balance.

Ms. JACKSON LEE. Let me thank the Chairman, and I yield back my time.

Mr. CHAFFETZ. Thank you.

I would like to thank all of our witnesses for your time and your testimony and your expertise and making the time and effort to be here.

Without objection, all Members will have 5 legislative days to submit to the Chair additional written questions for the witnesses, which we will forward and ask the witnesses to respond as promptly as they can so the answers to these questions can be made part of the record.

Also, without objection, all Members will have 5 legislative days to submit any additional materials for inclusion in the record.

Hearing no objection, so ordered.

With that, again, I would like to thank the witnesses.

The hearing is now adjourned.

[Whereupon, at 11:52 a.m., the Subcommittee was adjourned.]

# APPENDIX

---

MATERIAL SUBMITTED FOR THE HEARING RECORD

epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Statement for the Record of
The Electronic Privacy Information Center (EPIC)

Marc Rotenberg, EPIC President
Ginger McCall, EPIC Open Government Project Director
David Jacobs, EPIC Consumer Protection Fellow
Alan Butler, EPIC Appellate Advocacy Fellow

Hearing on H.R. 2168, the "Geolocational Privacy and Surveillance Act"

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

May 17, 2012
2141 Rayburn House Office Building,
Washington, DC 20515

Thank you, Mr. Chairman, for the invitation to submit this statement for the record for this hearing on H.R. 2168, the "Geolocational Privacy and Surveillance Act" ("GPS Act") to be held on May 17, 2012 before the House Subcommittee on Crime, Terrorism, and Homeland Security. We ask that this statement be included in the hearing record.

EPIC thanks you, Representatives Chaffetz and Goodlatte, and the members of the Subcommittee, for your attention to this important issue. As communications technologies evolve, new forms of personal information are generated that require new legal safeguards. Your decision to hold this hearing will help protect important privacy rights.

The Electronic Privacy Information Center ("EPIC") is a non-partisan public interest research organization established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC fully supports the Committee's examination of the Electronic Communications Privacy Act of 1986 ("ECPA")[1] and location information. Mobile devices have become ubiquitous in modern society, and service providers now routinely record and transmit users' locations. In many instances, this can provide significant benefits to users of new communications services. But in some circumstances, this also poses real risks to privacy and security.

In light of these developments, it is important to establish clear standards to protect the privacy of users by ensuring that locational data is not misused. In this statement, we outline several steps that the Subcommittee can take to strengthen the privacy protection of US customers whose data is collected and used by companies around the world.

## I. EPIC has a Longstanding Interest in the Privacy of Location Data

In 1999, Congress amended the Communications Act of 1934 with the Wireless Communication and Public Safety Act of 1999.[2] The Act required wireless carriers to implement 911 emergency calling and added location privacy provisions to the Telecommunications Act. After the Act was passed, the Federal Communications Commission ("FCC") considered a rulemaking to develop guidelines governing the collection and use of location data generated by wireless communications systems.

EPIC filed comments in April 2001 encouraging the FCC to follow through on the rulemaking process because "location privacy is one of the most significant issues facing American consumers and the expeditious establishment of comprehensive, technologically neutral privacy protections would serve the public interest."[3] EPIC encouraged the FCC to enact rules that would give consumers "meaningful control over the collection and use of location

[1] Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. § 2510 et seq.).
[2] Pub. L. No. 106-81, 113 Stat. 1286 (1999).
[3] EPIC, Comments to the F.C.C. on Commission Public Notice, DA 01-696 (Apr. 6, 2001), *available at* http://www.epic.org/privacy/wireless/epic_comments.pdf. *See also,* Marc Rotenberg, *Communication Privacy: Implications for Network Design*, 36 Comm. ACM 61 (Aug, 1993).

data."[4] In later reply comments, EPIC encouraged the FCC to "carefully constrict the circumstances under which implied consent could be utilized, if at all"[5] and to clarify the meaning of several key terms—including "location information"—that are used in the Act. EPIC recommended a number of other rules, including a rule that would require consent to be specific as to the third party that can receive the information and the purpose for which that information will be used by that party, and a rule that would require carriers to keep a record of consent for as long as the permission is valid.[6] With all of these steps, EPIC sought to give users greater control over their location information by requiring opt-in consent for location tracking.

EPIC has previously submitted statements before the House Committee on the Judiciary on the importance of providing safeguards for location privacy. In a June 2010 statement, EPIC offered several steps that could be taken to strengthen the privacy protection of US customers.[7] EPIC recommended that users be fully informed of type of location data being collected and the purpose of the collection.[8] EPIC also recommended that location data not be collected or shared without affirmative consent, and that companies provide users with a simple and free means to refuse the processing of location data for a specific connection or transmission.[9]

More recently, EPIC submitted amicus briefs in several federal court cases involving location privacy. In *United States v. Jones*, the Supreme Court considered whether the government's warrantless installation and use of a GPS device to track a private vehicle implicated the Fourth Amendment.[10] EPIC filed an amicus brief in *Jones*, arguing that the warrantless use of GPS tracking devices could enable pervasive, suspicionless surveillance of Americans with no judicial supervision.[11] Ultimately, the Supreme Court unanimously ruled that the warrantless use of a GPS tracking device by the police violated the Fourth Amendment. The Court said that a search occurs where "the Government physically occupie[s] private property," like a car, "for the purpose of obtaining information."[12] Concurring opinions by Justices

---

[4] *Id.*
[5] EPIC, Reply Comments to the F.C.C. on Commission Public Notice, DA 01-696 (Apr. 24, 2001), *available at* http://www.epic.org/privacy/wireless/epic_reply.pdf.
[6] *Id.*
[7] *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the H. Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 109 (2010) (statement of the Electronic Privacy Information Center), *available at* https://epic.org/privacy/ECPA_Statement_2010-06-24.pdf.
[8] *Id.* at 7.
[9] *Id.*
[10] *United States v. Jones*, 132 S. Ct. 945 (2012).
[11] Brief of Amici Curiae Electronic Privacy Information Center (EPIC) and Legal Scholars in Support of Respondent, *United States v. Jones*, 132 S. Ct. 945 (2012) (No. 10-1259), *available at* https://epic.org/amicus/jones/EPIC_Jones_amicus_final.pdf.
[12] *Jones*, 132 S. Ct. at 949.

Sotomayor and Alito argued that the use of a GPS tracking device would also violate an individual's reasonable expectation of privacy under a traditional *Katz* analysis.[13]

Following *Jones*, EPIC submitted two amicus briefs in cases involving warrantless access to cell phone location records. In *State v. Earls*,[14] EPIC argued that the New Jersey Supreme Court should overturn a lower court decision holding that an individual has no legitimate expectation of privacy in the location of their cell phone.[15] The cell phone tracking techniques in the case, EPIC argued, "[are] more invasive than the GPS tracking in Jones."[16] Similarly, EPIC filed a brief in the Fifth Circuit urging the court to uphold a lower court ruling that the disclosure of historical cell phone location records without a warrant would violate the Fourth Amendment.[17] EPIC argued that this opinion should be upheld, in light of the Supreme Court's recent decision in *Jones*, because cell phone location records are collected without the knowledge or consent of users.[18] The records in the case, EPIC argued, provide a "comprehensive map of an individual's movements, activities, and relationships, . . . precisely the type of information that individuals reasonably and justifiably believe will remain private."[19]

These activities, which EPIC has pursued for more than a decade, indicate the growing importance of locational data for personal privacy.

## II. Location Privacy Concerns Are Substantial and Growing More Acute

Location privacy issues are becoming more substantial as the number of mobile devices increases and location methods become more precise. The number of mobile phone users in the United States increases every year. The Pew Research Center found that 77% of all adults had a cell phone or other mobile device in 2008.[20] By 2012, that figure had risen to 88%.[21]

---

[13] *Jones*, 132 S. Ct. at 954-58 (Sotomayor, J., concurring); *Jones*, 132 S. Ct. at 958-64 (Alito, J., concurring in the judgment).
[14] 22 A.3d 114 (Sup. Ct. N.J. 2011), *cert. granted*, 209 N.J. 97 (2011).
[15] Elec. Privacy Info. Ctr., *State v. Earls* https://epic.org/amicus/location/earls/ (last visited May 16, 2012).
[16] Brief of Amicus Curiae Electronic Privacy Information Center, *State v. Earls*, 209 N.J. 97 (2011) (No. 68,765), *available at* https://epic.org/amicus/location/earls/EPIC-Earls-Amicus-NJ-SCt.pdf.
[17] Elec. Privacy Info. Ctr., *In re Historic Cell-Site Location Information* (last visited May 16, 2012) https://epic.org/amicus/location/cell-phone-tracking/.
[18] Brief of Amicus Curiae Electronic Privacy Information Center, *In re United States for Historical Cell Site Data*, 747 F. Supp. 2d 827 (S.D.Tx. 2010), *appeal docketed*, No. 11-20884 (5th Cir. Feb. 22, 2012), *available at* https://epic.org/amicus/location/cell-phone-tracking/EPIC-5th-Cir-Amicus.pdf.
[19] *Id.*
[20] Pew Research Center, Teens and Internet Over the Past Five Years: Pew Internet Looks Back (Aug. 19, 2009), *available at* http://www.pewinternet.org/Reports/2009/14--Teens-and-Mobile-Phones-Data-Memo.aspx.
[21] Aaron Smith, *46% of American Adults are Smartphone Owners*, Pew Research Center at 2 (Mar. 1, 2012), *available at* http://www.pewinternet.org/~/media//Files/Reports/2012/Smartphone%20ownership%202012.pdf.

American consumers carry their mobile devices everywhere, all day, every day. The location records created by these devices reveal aspects of consumers' social, political, professional, and educational lives. Every time an individual uses their mobile phone, a record is created.[22] The average individual sends or receives calls, text messages, or Internet data more than fifty times per day, generating a constant stream of location data. [23] For certain populations, mobile phone are even more ubiquitous. Young adults, for example, send an average 100 text messages per day.[24] All of these uses generate location data. The location records created provide a comprehensive map of people's movements, activities, and relationships over the course of many weeks and months—precisely the type of information that individuals reasonably and justifiably believe will remain private.

As technology improves, this location data will become more precise. Already, cell-site location data can be used to pinpoint an individual's location to the level of a room or floor in a building. Femtocells—low-power base stations used to route calls between consumers and the cellular network— have a range as small as ten meters.[25] Experts estimate that by 2016, femtocells will constitute 88% of all cell sites globally.[26] Some carriers even triangulate user location for emergency and other purposes.[27] Thus, as the technology develops further, cell phone companies will compile increasingly detailed location records of their users.

Mobile smart phones also contain built-in GPS functionality for location-based services. These devices enable consumers' location information to be collected not just by the carrier or platform developer, but by application developers and third-party advertisers. An examination of 101 popular iPhone and Android applications by the Wall Street Journal revealed that 56 applications either collected or transmitted location information to third parties.[28]

Other companies are also increasingly collecting the location information of consumers. Foursquare, with approximately 3 million users, is a service that lets users "check in" to a place, broadcast this fact to other individuals, and track the history of where they've been and with

---

[22] See Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 26 Berkeley Tech. L.J. (forthcoming 2012).

[23] Aaron Smith, *31% of Text Message Users Prefer Texting to Voice Calls, and Young Adults Stand Out In Their Use of Text Messaging*, Pew Research Center at 2 (Sept. 19, 2011), *available at* http://www.pewinternet.org/~/media//Files/Reports/2011/Americans%20and%20Text%20Messaging.pdf.

[24] *Id.*

[25] AT&T 3G Microcell—Wireless Signal Booster, AT&T, http://www.att.com/shop/wireless/devices/3gmicrocell.jsp (last visited May 16, 2012).

[26] Press Release, Informa Telecoms & Media, The Shape of Mobile Networks Starts to Change as Femtocells Outnumber Macrocells in US (Oct. 21, 2010), www.smallcellforum.org/pressreleases.php?id=269.

[27] Paul A Zandbergen, Accuracy of iPhone Locations: A Comparison of Assisted GPS, WiFi and Cellular Positioning, 13 Transactions GIS 5, 11 (2009).

[28] *What They Know-Mobile*, Wall St. J., http://blogs.wsj.com/wtk-mobile/ (last visited May 16, 2012).

whom.[29] Businesses are taking advantage of the service by offering discounts and coupons to individuals who "check in" to their location. Foursquare also has an API that allows developers to build on its platform. One recent smartphone application that provoked a particularly strong reaction, Girls Around Me, used information from Foursquare and Facebook to provide a map of women around a user's location.[30] As part of another program, Google collected MAC addresses (the unique device ID for Wi-Fi hotspots) and network SSIDs (the user-assigned network ID name) tied to location information for private wireless networks.[31] The "street view" vehicles also intercepted Wi-Fi "payload" data, which included emails, passwords, usernames and website URLs.[32] Advertisers and marketers also use location information in consumer data profiles, enabling them to track consumers through their daily journey and target them with advertisements based on their location.[33]

Perhaps because of the amount of information that can be derived from location data, this data is often considered sensitive or personally identifiable. For example, the Federal Trade Commission's amendments to the Children's Online Privacy Protection Act ("COPPA") Rule update the definition of Personally Identifiable Information in response to changes in technology, the increased use of mobile devices, and new business practices.[34] Under the new Rule, "personal information" includes "geolocation information."[35] The FTC's 2012 report considers location data to be "sensitive" information the collection of which requires the affirmative consent of consumers.[36]

Not surprisingly, consumers have significant concerns about the protection of location privacy. A recent survey found that 77% of cell phone users did not want to disclose their location to smartphone "Apps" or developers.[37] Consumers also strongly object when companies secretly enable location-tracking services. In May 2011, researchers discovered that an

---

[29] Foursquare, https://foursquare.com/ (last visited May 16, 2012).
[30] *See* Nick Bilton, *Girls Around Me: An App Takes Creepy to a New Level*, N.Y. Times – Bits (Mar. 30, 2012), http://bits.blogs.nytimes.com/2012/03/30/girls-around-me-ios-app-takes-creepy-to-a-new-level/
[31] Google, *Data Collected by Google Cars*, European Public Policy Blog (Apr. 27, 2010) http://googlepolicyeurope.blogspot.com/2010/04/data-collected-by-google-cars.html.
[32] *See* Elec. Privacy Info. Ctr., *Investigations of Google Street View*, https://epic.org/privacy/streetview/.
[33] *See generally* Ctr. for Digital Democracy, Google, Inc., *Request for Investigation and Imposition of Fines and Other Remedies for Violation of "Google Buzz" Consent Decree* (2012), *available at* http://www.centerfordigitaldemocracy.org/sites/default/files/CDDGoogleComplaint022212.pd (describing advances in Google's advertising ecosystem).
[34] Federal Trade Comm'n, *FTC Seeks Comment on Proposed Revisions to Children's Online Privacy Protection Rule* (Sept. 15, 2011), http://www.ftc.gov/opa/2011/09/coppa.shtm.
[35] Children's Online Privacy Protection Rule, 76 Fed. Reg. 59804, 59813 (proposed Sept. 27, 2011) (to be codified at 16 C.F.R. pt. 312), http://www.ftc.gov/os/2011/09/110915coppa.pdf.
[36] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change* 58 (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.
[37] Harris Interactive, Mobile Privacy: A User's Perspective (Mar. 4, 2011) *available at* http://www.scribd.com/doc/54220855/TRUSTe-Mobile-Privacy-Report.

unencrypted file on Apple iPhones stored a ten-month record of a user's location data.[38] During the 2011 holiday season, several malls decided to use shoppers' cell phones to track their movement from store to store.[39] In each case, consumers were outraged and members of Congress investigated the business practices.[40]

## III. The GPS Act Sets Out the Necessary Elements of an Effective Privacy Law

### A. The Act Establishes Appropriate Circumstances for the Collection of Location Data

The Act prohibits "[a]ny person" from intentionally intercepting or disclosing location data.[41] The Act also prohibits the use of location information by any person "knowing or having reason to know that the information was obtained through the interception of such information in violation of this [Act]."[42] Finally, the Act prohibits the disclosure of location information for the purposes of obstructing a criminal investigation.[43] These prohibitions mirror the protections found in ECPA, which also prohibits the interception, disclosure, and use of wire, oral, or electronic communications.

Like ECPA, however, the Act does not impose an absolute prohibition on the collection or use of location data. Information acquired in the normal course of business may be used or disclosed if doing so is "a necessary incident to the rendition of the service or to the protection of the rights or property of the provider of the service."[44] Location information may be intercepted through "any system that is configured so that such information is readily accessible to the general public."[45] The Act also allows individuals to consent to the interception of their location information, and parents are permitted to give consent on behalf of their children.[46] Location information may also be used in emergency situations or in situations involving the theft of the device sending geolocation information.[47] Finally, as discussed below, the Act contains an exception for information obtained pursuant to a warrant.

---

[38] Nick Bilton, *Tracking File Found in iPhones*, N.Y. Times, (Apr. 20, 2011) https://www.nytimes.com/2011/04/21/business/21data.html.
[39] Ken Wagstaff, *Will Your Mall Be Tracking Your Cellphone Today?*, Time, (Nov. 25, 2011), http://techland.time.com/2011/11/25/will-your-mall-be-tracking-your-cellphone-today/.
[40] *See* Letter from Al Franken, Chairman, Subcomm. on Privacy, Tech. and the Law, to Steve Jobs, CEO, Apple Corp. (Apr. 20, 2011), *available at* http://www.franken.senate.gov/files/letter/110420_Apple_Letter.pdf; *see also* Ashley Lutz, *Malls Cell-Phone Devices to Track Shoppers Halted After Complaints*, Bloomberg (Nov. 28, 2011), http://mobile.bloomberg.com/news/2011-11-28/cell-phone-technology-to-track-shoppers-halted-after-complaints.
[41] H.R. 2168, 112 Cong. §2602(a)(1)(A)-(B) (2012).
[42] *Id.* §2602(a)(1)(C).
[43] *Id.* §2602(a)(1)(D)(i).
[44] *Id.* §2602(b).
[45] *Id.* §2602(c).
[46] *Id.* §2602(d).
[47] *Id.* §2602(f).

B. The Act Establishes a Warrant Standard for Government Access to Location Data

Under the Act, a government entity may intercept location information "only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure."[48] Warrant requirements provide important checks against government abuse. As Justice Sotomayor stated in *Jones*, "the Fourth Amendment's goal [is] to curb arbitrary exercises of police power [] and prevent 'a too permeating police surveillance.'"[49] As the Supreme Court has long-recognized, a warrant requirement strikes a reasonable balance between the protection of privacy and the needs of law enforcement. "Although some added burden will be imposed upon the Attorney General, this inconvenience is justified in a free society to protect constitutional values."[50] Here, a warrant requirement enables legitimate access to location information by law enforcement while protecting the privacy of individuals.

Although the Act makes clear that Government interception of location information is unlawful absent a warrant, it also provide an exception for emergency situations, similar to the emergency exception in ECPA, 18 U.S.C. § 3125. While this exception includes broad language about "emergency situations" that involve "conspiratorial activities," it also makes clear that, even in an emergency, an officer intercepting location information must apply for a warrant within 48 hours of interception.[51] In the event that the warrant application is denied, the information "shall be treated as having been obtained in violation of this chapter and an inventory shall be served on the person named in the application."[52] This provides a strong deterrent to any officer intercepting location information without sufficient grounds for a warrant.

C. The GPS Act Establishes a Private Right of Action to Ensure Enforcement

Importantly, the Act applies to private parties as well as law enforcement. The Bill prohibits the interception and disclosure of location information by "any person," a term that includes private companies and individuals.[53] The Bill's civil damages provision provides that "any person whose geolocation information is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from a person, other than the United States, which engaged in that violation such relief as may be appropriate."[54] The Bill's damage provision allows plaintiffs to recover the greater of "actual damages suffered by the plaintiff and

---

[48] *Id.* §2602(h)(2).
[49] *United States v. Jones*, 132 S. Ct. 945, 956, (2012) (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)).
[50] *United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.*, 407 U.S. 297, 299 (1972).
[51] H.R. 2168, 112 Cong. § 2604(a) (2012).
[52] *Id.* § 2605(b) (2012).
[53] *Id.* §2602(a)(1).
[54] *Id.* §2605(a).

any profits made by the violator as a result of the violation" or "statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000."[55]

Private rights of action strengthen enforcement and allow individuals to seek remedies. They empower consumers to enforce the law themselves, create a strong disincentive for the irresponsible handling of consumer data, and provide a necessary backstop to the current enforcement scheme.

Statutory damage provisions ensure that individuals can seek compensation for and deter privacy violations. Harms suffered as a result of privacy violations are often difficult to quantify, and include intrusions upon individuals' autonomy, mental and emotional distress, loss of reputation and trust, and an increased risk of identity theft, financial loss, erroneous credit information, and even bodily harm. Thus, privacy laws frequently feature statutory damage provisions to ensure adequate enforcement of privacy interests.[56]

## IV. The European Commission Has Provided an Effective Model for the Protection of Location Privacy

Concerns regarding locational privacy are arising in other countries, as well. The approach of the European Commission, in particular, provide the United States with a possible model to protect the privacy of locational data. With Directive 2002/58 on Privacy and Electronic Communications, also known as E-Privacy Directive,[57] the European Commission has created an effective framework for the regulation of locational data.

The Directive requires that location data other than traffic data be processed anonymously or with the consent of the individual, and provides protections to ensure that this consent is meaningful.[58] Obtaining this consent requires informing the user of the type of data, the purpose of the collection, the duration of the collection and whether a third party will be doing the processing. Consent may be withdrawn at any time, and there must be a simple and free means for a user to refuse the processing of location data for a specific connection or transmission. Finally, the processing of data is restricted to what is necessary for providing the value-added service.

The Article 29 working party, an E.U. advisory group of experts on privacy and data

---

[55] *Id.* §2605(c).

[56] *See* Fair and Accurate Credit Transactions Act, 15 U.S.C. §§ 1681 *et seq.*; Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510 *et seq.*;Video Privacy Protection Act, 18 U.S.C. § 2710; Driver's Privacy Protection Act, 18 U.S.C. § 2724; Telephone Consumer Protection Act, 47 U.S.C. § 227; Cable Communications Privacy Act, 47 U.S.C. § 551.

[57] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *available at* http://europa.eu.int/eurlex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

[58] *Id.* Art. 9.

protection, has also issued an opinion on geolocation information.[59] The opinion states that "*prior informed consent* is also the main applicable ground for making data processing legitimate when it comes to the processing of the locations of a smart mobile device in the context of information society services."[60] Furthermore, if the purpose for which the data is being used changes in a material way, consent must be obtained again.[61] Finally, the opinion provides that individuals must be able to withdraw their consent without suffering negative consequences for the use of their device.[62]

The Transatlantic Consumer Dialogue (TACD) has also passed a resolution on mobile commerce that addresses privacy concerns of consumers.[63] The resolution states that the E.U. and U.S. governments should: "Protect consumer privacy in mobile commerce and prohibit use of any personal data (including purchase and location information) for purposes that consumers have not explicitly agreed to or that unfairly disadvantage them."

## V. EPIC's Recommendations

### A. There Should be Limitations on the Use of Location Data

As currently drafted, the bill regulates the interception of location data, but once consent is obtained, there are no limitations on use of this information. The bill should be modified so that location data is only used consistent with the context in which it was provided. Moreover, consumers should have the opportunity to access the location data that is collected and there should be limitations on the period of storage for location data.

In particular, a purpose-specification or "respect for context" principle is likely to play an important role in the protection of location privacy. In many cases, location information is already collected by companies. The privacy risk, therefore, comes not in the collection (or "interception") of location information, but in its use. For example, Verizon recently started using geolocation information for business, marketing, and advertising purposes after failing to give new customers meaningful notice of these changes.[64] Currently, the Bill only prohibits the "use" of location information if that information was obtained through interception, *i.e.*, illegally.[65] The application of a context- or purpose-specification principle would prohibit data use that violates contextual integrity, instead of only prohibiting data use that follows an illegal interception.

---

[59] Working Party 29 Opinion Geolocation services on smart mobile devices, 881/11/EN, May 2011, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf.
[60] *Id.* at 14.
[61] *Id.* at 15.
[62] *Id.* at 16.
[63] Transatlantic Consumer Dialogue, Resolution on Mobile Commerce, August 2005, http://www.tacd.org/cgibin/db.cgi?page=view&config=admin/docs.cfg&id=283.
[64] *See* Elec. Privacy Info. Ctr., *In re Verizon Wireless*, https://epic.org/privacy/ftc/in_re_verizon.html (last visited May 16, 2012).
[65] H.R. 2168, 112 Cong. §2602(a)(1)(C).

B, The Act's Consent and Public Information Exceptions Should Be Clarified

The Act provides an across-the-board prohibition on the interception, disclosure, and use of location information, subject to a few discrete exceptions.[66] This framework makes clear that location information is sensitive, protected, personal information that cannot be misused. However, in order for this prohibition to be effective the exceptions must be narrow and clear. The Act defines an exception allowing interception of location information "pertaining to another person if such other person has given prior consent,"[67] but it does not explain or imply what sort of consent is required. The Act also provides for an exception where location information is accessed "through any system that is configured so that such information is readily accessible to the general public,"[68] without reference to the source or use of such information. If these exceptions are not narrowly defined, they could provide an enormous loophole for third party collection and disclosure of sensitive location information.

The Act's consent exception is crucial. Section 2602(d) creates an exception for interceptions of location information "pertaining to another person if such other person has given prior consent to such interception."[69] Companies have often intercepted location data without the affirmative consent of consumers. When Verizon and OnStar announced the collection of location information, they obtained "consent" by requiring consumers to opt out of such collection. And when several malls announced that they would begin monitoring the paths that consumers traveled from store to store, the "consent" of consumers was obtained through a few lines of text attached to a mall directory. Arguably, announcing a practice and then requiring consumers to opt-out of that practice does not constitute "prior" consent as the statute requires, nor do inconspicuous notices provide a means of "giv[ing]" consent. However, the Bill's language is sufficiently unclear to allow for the interception of location information through hidden notices or on an opt-out basis. The approach recommended by the FTC, the Trans-Atlantic Consumer Dialog, and EPIC, is to ensure that consent is meaningful by requiring consumers to opt in to the use of their location data.

Section (e) of the Act outlines the exception for "public information," which specifies that it is not unlawful to access location information "through any system that is configured so that such information is readily accessible to the general public."[70] Similar language in the Wiretap Act has recently been a source of confusion and controversy in the case of Google's Street View program.[71] Section (e) is also likely to be a source of confusion, since it does not make clear whether configuring a system in such a way that "information is readily accessible" eliminates all protections for users of that system. It is also unclear whether accessing location

[66] *Id.* § 2602(a)(1).
[67] *Id.* § 2602(d)(1).
[68] *Id.* § 2602(e).
[69] *Id.* § 2602(d).
[70] *Id.* § 2602(e).
[71] *See* Elec. Privacy Info. Ctr., *Ben Joffe v. Google*, http://epic.org/amicus/google-street-view/ (last visited May 16, 2012).

information through such a system would allow downstream misuses that would otherwise be prohibited. More fundamentally, the Act does not provide a definition, or even an example, of "readily accessible" information.

Users may not know, or may not have control over, the configuration of a particular system that they use, like Foursquare or Facebook.[72] Some systems enable location sharing by default, without the users' explicit consent, and would thus broadcast location information in a way that could allow downstream misuse.[73] More importantly, privacy settings on social media sites typically allow different degrees of privateness.[74] Even when a person has control over the configuration of such a system, as in the case of a home Wi-Fi network, it is unclear why a configuration that allows "access" to location information should authorize collection of that data, except to the extent that it indicates consent under Section (d).[75] As currently drafted, Section (e) causes confusion, acts as a potentially large loophole for all online information collection, and provides no clear benefit over the consent-based exception.

C. The GPS Act Should Apply Fair Information Practices to Location Data Stored by Private Actors

Fair Information Practices (FIPs) can provide an effective solution to location privacy concerns. One recent formulation, the Consumer Privacy Bill of Rights contained in the Administration's listed the following principles:

- Individual Control: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
- Transparency: Consumers have a right to easily understandable and accessible information about privacy and security practices.
- Respect for Context: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
- Security: Consumers have a right to secure and responsible handling of personal data.

---

[72] *See* Julia Angwin & Jeremy Singer-Vine, *Selling You on Facebook*, WALL ST. J. (Apr. 7, 2012), at C1.
[73] This is especially clear in the case of recent apps that combine personal location information with other related information to provide a "mapping" service. *See* Nick Bilton, *Girls Around Me: An App Takes Creepy to a New Level*, N.Y. Times – Bits (Mar. 30, 2012), http://bits.blogs.nytimes.com/2012/03/30/girls-around-me-ios-app-takes-creepy-to-a-new-level/.
[74] *See* Naomi Gleit, *More Privacy Options*, Facebook Blog (Mar. 19, 2008), http://blog.facebook.com/blog.php?post=11519877130.
[75] It is important to note that one of the goals of Google's Street View program was to collect and map the location of private Wi-Fi networks, which it did by logging network data from "open" networks across the world. *See* Elec. Privacy Info. Ctr., *Investigations of Google Street View* , https://epic.org/privacy/streetview/ ((last visited May 16, 2012). Even Google recognized that such sweeping collection of personal information required some degree of consent, and they eventually allowed users to "opt out" of their program. Kevin J. O'Brien, *Google Makes Sweeping Concession on Data Collection*, N.Y. TIMES, Nov. 16, 2011.

- Access and Accuracy: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.
- Focused Collection: Consumers have a right to reasonable limits on the personal data that companies collect and retain.
- Accountability: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.[76]

FIPs are central to American privacy law, appearing most prominently in the Privacy Act of 1974.[77] Trans-Atlantic consumer groups have recommended similar principles in the context of location privacy, such as transparency, data minimization, purpose limitation, limitation of data retention periods and data security.[78] EPIC recommends that the Act apply FIPs to stored location data.

## VI. Conclusion

EPIC respectfully requests that the Subcommittee take the following steps outlined in this statement:

- In general, adopt FIPs to location data stored by private actors;
- Specifically, adopt purpose-specification and data limitation requirements;
- Clarify the consent exception to require that users affirmatively consent to data collection;
- Clarify the public information exception to prevent the creation of a loophole for online information collection.

Thank you for your consideration of our views. We would be pleased to provide any further information the Committee requests.

---

[76] White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy, Feb. 23, 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.
[77] *See* Privacy Act of 1974, 5 USC § 552a.
[78] Transatlantic Consumer Dialogue, Protecting Mobile Privacy in a Hyper-local World, May 2012.

International Association of Chiefs of Police
515 North Washington Street
Alexandria, VA 22314-2357
Phone: 703-836-6767; 1-800-THE IACP
Fax: 703-836-4543
Web: www.theiacp.org

**President**
Walter A. McNeil
Chief of Police
Quincy Police Department
Quincy, Florida

**Immediate Past President**
Mark A. Marshall
Sheriff
Isle of Wight County
Isle of Wight, VA

**First Vice President**
Craig T. Steckler
Chief of Police
Fremont Police Department
Fremont, CA

**Second Vice President**
Yousry "Yost" Zakhary
Director
Woodway Public Safety Department
Woodway, TX

**Third Vice President**
Richard Beary
Chief of Police
University of Central Florida
Orlando, FL

**Fourth Vice President**
Ronal W. Serpas
Superintendent of Police
New Orleans Police Department
New Orleans, LA

**Vice President at Large**
Patrick Foley
Chief of Police
Douglas Police Department
Douglas, MA

**Vice President at Large**
James Craze
Chief of Police
Greenbelt Police Department
Greenbelt, MD

**International Vice President**
Nelson Wertang Garcia
Chief, Community Policing & Human Rights Center
Policia Militar do Distrito Federal
Brasilia, Brazil

**Vice President-Treasurer**
Carl R. Wolf
Chief of Police
Hazelwood Police Department
Hazelwood, MO

**General Chair Division of State Associations of Chiefs of Police**
Kent Barker
Chief of Police
Tualatin Police Department
Tualatin, OR

**General Chair Division of State and Provincial Police**
John R. Batiste
Chief
Washington State Patrol
Olympia, Washington

**Parliamentarian**
David G. Walchak
IACP Past President
New Braunfels, TX

**Executive Director**
Bart R. Johnson
Alexandria, VA

**Deputy Executive Director**
Chief of Staff
James W. McMahon
Alexandria, VA

May 18, 2012

The Honorable Lamar Smith
Chairman
Committee on the Judiciary
United States House of Representatives
Washington, DC 20515

Dear Chairman Smith:

On behalf of the International Association of Chiefs of Police (IACP), I am writing you to voice our strong opposition to H.R. 2168, the Geolocational Privacy and Surveillance (GPS) Act. The provisions of H.R. 2168, as they relate to law enforcement's access rules when requesting a search warrant, would severely hinder our ability to properly serve the communities we are sworn to protect.

Requests for search warrants cannot adopt a "one size fits all" approach and must be evaluated on a case by case basis before a decision is made for the need to establish the level of probable cause. Access to fundamental data is a crucial law enforcement investigative tool and creates leads that could be used to bring focus on a specific individual who may be involved in criminal activity while eliminating persons who, while originally thought to be involved, are not. Without this basic information law enforcement would never be able to establish the probable cause and trace a criminal's "electronic footprint." Law enforcement's goal is to attain justice while avoiding wrongful arrests and convictions.

Thank you for your attention to this matter.

Respectfully,

Walter A. McNeil
President

Berkeley
[technology law journal]
117
Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact
Stephanie K. Pell & Christopher Soghoian
VOLUME 27
NUMBER 1
2012
UNIVERSITY OF CALIFORNIA, BERKELEY
SCHOOL OF LAW
BOALT HALL

# 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.

---

© 2012 Stephanie K. Pell & Christopher Soghoian.

† 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** ..... 119

II. **TECHNOLOGY** ..... 126

A. A BRIEF INTRODUCTION TO CELL PHONE TECHNOLOGY ..... 126
B. CELL SITE DATA ..... 128
C. GLOBAL POSITIONING SYSTEM ("GPS") ..... 128
D. WIFI ..... 129
E. PINGS ..... 131
F. TRENDS ..... 132

III. **THE LAW** ..... 133

A. LEGAL BACKGROUND FOR REAL-TIME OR "PROSPECTIVE" CELL SITE DATA ..... 134
1. *The DOJ's Interpretation of the Standard for Obtaining Prospective Cell Site Data* ..... 135
2. *Judicial Resistance to the Government's Use of Hybrid Orders* ..... 137
3. *Divergent Interpretations of the Standard for Requiring Disclosure of Prospective Cell Site Data Create Legal Uncertainty* ..... 139
B. LEGAL BACKGROUND FOR HISTORICAL CELL SITE DATA ..... 141
1. *The DOJ's Interpretation of the Standard for Obtaining Historical Cell Site Data* ..... 142
2. *Judicial Interpretation of the Standard for Obtaining Historical Cell Site Data* ..... 143
a) The Third Circuit Finds That Magistrate Judges Have the Discretion To Require Probable Cause ..... 143
b) The D.C. Circuit's "Mosaic Theory" ..... 145
3. *The* Jones *Decision* ..... 148
4. *The Importance of Legislative Clarity in the Face of Rapid Technological Change* ..... 150
C. QUESTIONS RAISED BY THE TWO EXISTING STANDARDS FOR COMPELLING DISCLOSURE OF LOCATION DATA ..... 151
1. *What Does a "D" Order Require the Government To Show?* ..... 151
2. *Probable Cause of What?* ..... 154

IV. **LESSONS LEARNED** ..... 157

A. ACQUIRING FACTS TO MAKE GOOD POLICY IS DIFFICULT ..... 157
B. THE SINGULAR ADVOCACY FOCUS ON LAW ENFORCEMENT STANDARDS HAS NARROWED A DISCUSSION THAT SHOULD INCLUDE MINIMIZATION AND OTHER "DOWNSTREAM" PRIVACY PROTECTIONS ..... 160

C. THE POLARIZED VIEWS OF LAW ENFORCEMENT AND PRIVACY ADVOCATES MAKE CONSENSUS BUILDING DIFFICULT ....161

V. **WHAT IS THE HARM, AND WHO CAN ADDRESS IT MOST EFFECTIVELY?** ....163

A. THE GOVERNMENT'S GAZE AND THE PANOPTIC EFFECT ....164

VI. **LEGISLATIVE PROPOSAL** ....174

A. OVERARCHING PRINCIPLES ....175
1. *Clear Rules* ....175
2. *Technology Neutrality* ....176
3. *Standards Alone Will Not Achieve the Appropriate Balance* ....176
4. *Insistence on a Single Location Standard Is "A Foolish Consistency"* ....177

B. HOW TO DEFINE LOCATION INFORMATION FOR PURPOSES OF AMENDING THE ECPA ....178

C. A STANDARD FOR LAW ENFORCEMENT COMPELLED DISCLOSURES OF HISTORICAL LOCATION DATA ....180

D. A STANDARD FOR LAW ENFORCEMENT COMPELLED DISCLOSURES OF PROSPECTIVE LOCATION DATA ....181

E. POST ACCESS RULES AND "DOWNSTREAM" PRIVACY PROTECTIONS ....183
1. *Minimization* ....184
2. *Notification* ....185
3. *Surveillance Statistics* ....188

VII. **CONCLUSION** ....193

## 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/IsojNy.

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.digitaldueprocess.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.digitaldueprocess.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 Comm'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/view?id=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. Gorden 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 *Knott*'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/IhMb7d.

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.

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.

May 16, 2012

The Honorable F. James Sensenbrenner
Chairman, Subcommittee on Crime, Terrorism, and Homeland Security
Committee on the Judiciary
United States House of Representatives
2138 Rayburn House Office Building
Washington, DC 20515

**RE: H.R. 2168, the Geolocational Privacy and Surveillance Act**

Dear Chairman Sensenbrenner,

We write on behalf of the thousands of law enforcement professionals our organizations represent to offer comments on H.R. 2168, the GPS Act. We have serious concerns about the potential impact that the GPS Act as written would have on our ability to protect the citizens we serve. Briefly, here are some of our concerns:

- the broadly written language would significantly lengthen the investigative timeline in a wide range of investigations by requiring a warrant to be issued where a subpoena or administrative process is currently sufficient;
- emergency provisions in the bill are not specific enough to prevent problems of access to critical evidence in times of highest need;
- in the absence of a demonstrated pattern of abuse or misuse of location evidence by law enforcement it is not clear what problem this bill addresses;
- the bill does not address the major issue of service provider responsiveness to legitimate law enforcement process requests;
- the Supreme Court clearly signaled in the Jones decision that it is likely to take up related cases, and until the Court more fully develops constitutional protections for location evidence we urge Congress to not act to restrict law enforcement access to such evidence.

We urge the committee to carefully consider the insights of the highly-trained practitioners who develop and utilize location evidence to solve crimes and save lives before acting on any legislation. If our ability to access and utilize this information on a timely basis is significantly limited, as we read the GPS Act to do, it may be some of the most vulnerable among us who will bear the cost.

We are always mindful of our responsibility as guardians of a free society to minimize unnecessary intrusions into citizens' privacy. One doesn't have to look very far these days to find articles expressing concern about the amount of location evidence obtained by law enforcement and private companies. Notably absent from the public discourse, however, has been any discussion of the countless cases where location evidence has been used to rescue abducted children, identify and prosecute sexual predators, and capture dangerous fugitives. Equally

absent is any indication of a pattern of abuse by the professionals who use this information on a regular basis. This compels us to ask: what problem is the Act meant to solve?

Location records constitute a critical source of evidence in an ever-expanding range of investigations. The present balance of judicial supervision and law enforcement efficiency is an appropriate one and has existed for some time. That balance should not be abandoned without a demonstrated need for an increase in privacy, and a demonstrated pattern of abuse — neither of which have been shown to exist. We believe the GPS Act is drafted so broadly that the bill could be read to require a search warrant to gather many forms of information that can currently be obtained by subpoena. Such a standard would hamper law enforcement's ability to quickly and efficiently obtain the information that could save lives. Law enforcement must be able to work critical investigations without undue delay; therefore, legal reforms should *contract* the investigative timeline at the same time they protect privacy and promote innovation. We believe the proposed GPS Act could lead to a *lengthening* of the investigative timeline, with adverse consequences for crime victims and public safety overall.

Location evidence is used to good effect in many instances where law enforcement may not have generated probable cause sufficient to satisfy the warrant requirement. Further, the time required to generate a search warrant and have it signed, even in cases where probable cause exists, may hamper law enforcement's efforts to move quickly in an investigation. This is particularly true in quickly-evolving, high-volume cases like child abductions, where every second counts and every possible lead must be explored. Of course, if Congress chooses to elevate the standard for location evidence to probable cause, law enforcement will adapt. Such a change would extend the investigative timeline and decrease the number of leads law enforcement can pursue in a given time period, however, and in some cases, prevent officers from obtaining records that would be helpful. The human cost of these changes should not be discounted.

Any discussion of law enforcement use of location evidence, and communications records generally, would be incomplete without some consideration of the practical obstacles that law enforcement currently faces in obtaining this evidence from service providers, irrespective of the legal standards. Whatever level of process is ultimately deemed appropriate, the undersigned organizations urge the Committee to take steps to guarantee that law enforcement is able to access the required communications records – including location information – once that process is obtained. The emergency exceptions outlined in §2602(f) of the GPS Act may seem to provide the necessary recourse, for example, but if there is no statutory mandate for a service provider to turn over the records, and no time frame for compliance, we may effectively be denied the information we need, whatever the level of legal process. The law should provide a framework that will enable the rapid transfer of information when needed, and properly incentivize service providers to respond rapidly to process calling for critical location information.

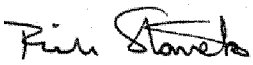
As a final point, we note that the United States Supreme Court has recently expressed a great deal of interest in defining the protections offered by the Constitution in this area. In particular, the recent Jones decision demonstrates a clear trend towards further delineation of privacy protections with respect to location evidence.

The undersigned organizations believe that the GPS Act's broad prohibition on law enforcement's use of location evidence without a warrant will significantly erode our access to location evidence and our efficiency in obtaining it. In the absence of any demonstrated problem with the current framework, and given the expectation that the Supreme Court will more fully develop constitutional protections for location evidence soon, we believe legislative action at this time would be premature. We urge the members of the Committee to consider the impact on law enforcement's ability conduct effective and efficient investigations carefully before making any adjustment to the existing law. What seems like an acceptable change in abstract discourse may seem less so when a child is missing, and every second counts.

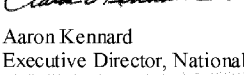
Thank you for your attention to our concerns. We look forward to working with you on this most important issue.

Sincerely,

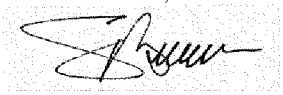
Ronald C. Sloan
President, Association of State Criminal Investigative Agencies (ASCIA)
Director, Colorado Bureau of Investigation



Richard W. Stanek
President, Major County Sheriffs' Association (MCSA)
Sheriff, Hennepin County (MN)



Aaron Kennard
Executive Director, National Sheriffs' Association (NSA)



Scott Burns
Executive Director, National District Attorneys' Association (NDAA)

Charles H. Ramsey
President, Major Cities Chiefs of Police Association (MCCA)
Commissioner, Philadelphia Police Department

**Federal Bureau of Investigation**
*Agents Association*

May 16, 2012

Honorable F. James Sensenbrenner
Chairman
Subcommittee on Crime, Terrorism, and Homeland Security
House Committee on the Judiciary
2138 Rayburn House Office Building
Washington, DC 20515

**Re: H.R. 2168, the *GPS Act***

Dear Chairman Sensenbrenner:

I am writing on behalf of the FBI Agents Association (FBIAA), a voluntary professional association currently representing over 12,000 active duty and retired FBI Special Agents. The FBIAA is concerned about the impact that restrictions on the use of geolocational data proposed in H.R. 2168, the *GPS Act*, could have on criminal investigations.

FBI Special Agents are committed to using developing technologies in a manner that respects individual privacy and constitutional requirements. Towards this end, Special Agents often use historical geolocational data from cell-towers and internet protocol addresses (IP) in the early stages of investigations to find approximate locations of persons of interest and enable more detailed investigations to proceed. Reasonable access to this data can be crucial to efforts to investigate complex criminal networks and ongoing criminal plots.

To date, courts have found historical and approximate information different from "real-time" tracking information, and have allowed law enforcement authorities to obtain such information without obtaining a warrant. This data, because it is historical and does not entail any potential trespass to a individual's property, is unlike the type of data discussed in cases such as the recent Supreme Court case of *United States v. Jones*, and does not implicate reasonable privacy expectations. Accordingly, law enforcement officials have been able to utilize this data at the early stages of investigations when obtaining a warrant is not practical.

Unfortunately, as drafted, H.R. 2168 could comprise the effectiveness of investigations using geolocational data. For example, the legislation would require a warrant in order to acquire geolocational information, and the definition of "geolocation information" in the bill treats historical and real-time data as equivalents in respect to privacy expectations. Requiring a warrant for all types of geolocational data in this manner would make it much more time-consuming and difficult for law enforcement to obtain access to historical geolocational data,

**Post Office Box 12650 • Arlington, Virginia 22219**
**A Non-Governmental Association**
**(703) 247-2173 Fax (703) 247-2175**
**E-mail: fbiaa@fbiaa.org www.fbiaa.org**

and such delays could jeopardize the often time-sensitive investigations that rely on such data.

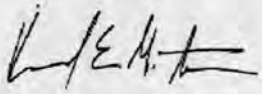
Additionally, the broad definition of geolocational information used in H.R. 2168 could result in application of the legislation's mandates to IP information. Requiring a warrant for all IP data could unnecessarily hinder the ability of law enforcement officials to expeditiously locate criminals, such as child pornographers and others, who use their computers in connection with criminal plots that threaten the safety of our country and its residents.

The FBIAA appreciates that efforts have been made to address law enforcement concerns by including a variety of exceptions in the legislation. However, the language of the exceptions is too narrow in some cases and too vague in others. For example, the consent exception does not make it clear who has to provide the consent (the property owner or the person receiving the property). Further, the exception for emergency situations requires an "immediate" threat of death or serious injury that could make it difficult to safely apply the exception to circumstances where the threat of death or serious injury is real but perhaps not immediate, such as kidnappings. Finally, the "emergency information" exception appears to only allow information related to the location of the person whose life is threatened, and not information related to the person causing the threat, which could make it difficult for the exception to be applied in kidnapping investigations. Given the significant civil and criminal penalties for violations of the mandates in H.R. 2168, these ambiguities create very real concerns for law enforcement officers.

For these reasons, the FBIAA is opposed to H.R. 2168 as currently drafted. The FBIAA appreciates your consideration of these concerns and hopes that you will continue working with the law enforcement community to address these issues.

Sincerely,

FBI Agents Association



Konrad Motyka, President

I

112TH CONGRESS
1ST SESSION

# H. R. 2168

To amend title 18, United States Code, to specify the circumstances in which a person may acquire geolocation information and for other purposes.

---

IN THE HOUSE OF REPRESENTATIVES

JUNE 14, 2011

Mr. CHAFFETZ (for himself and Mr. GOODLATTE) introduced the following bill; which was referred to the Committee on the Judiciary, and in addition to the Select Committee on Intelligence (Permanent Select), for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

# A BILL

To amend title 18, United States Code, to specify the circumstances in which a person may acquire geolocation information and for other purposes.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

**SECTION 1. SHORT TITLES.**

This Act may be cited as the "Geolocational Privacy and Surveillance Act" or the "GPS Act".

**SEC. 2. PROTECTION OF GEOLOCATION INFORMATION.**

(a) IN GENERAL.—Part 1 of title 18, United States Code, is amended by inserting after chapter 119 the following:

## "CHAPTER 120—GEOLOCATION INFORMATION

"Sec.
"2601. Definitions.
"2602. Interception and disclosure of geolocation information.
"2603. Prohibition of use as evidence of acquired geolocation information.
"2604. Emergency situation exception.
"2605. Recovery of civil damages authorized.

### "§ 2601. Definitions

"In this chapter:

"(1) ELECTRONIC COMMUNICATION SERVICE.—The term 'electronic communication service' has the meaning given that term in section 2510.

"(2) ELECTRONIC SURVEILLANCE.—The term 'electronic surveillance' has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

"(3) GEOLOCATION INFORMATION.—The term 'geolocation information' means, with respect to a person, any information that is not the content of a communication, concerning the location of a wireless communication device or tracking device (as that term is defined section 3117) that, in whole or in part, is generated by or derived from the operation

of that device and that could be used to determine or infer information regarding the location of the person.

"(4) GEOLOCATION INFORMATION SERVICE.—The term 'geolocation information service' means the provision of a global positioning service or other mapping, locational, or directional information service to the public, or to such class of users as to be effectively available to the public, by or through the operation of any wireless communication device, including any mobile telephone, global positioning system receiving device, mobile computer, or other similar or successor device.

"(5) INTERCEPT.—The term 'intercept' means the acquisition of geolocation information through the use of any electronic, mechanical, or other device.

"(6) INVESTIGATIVE OR LAW ENFORCEMENT OFFICER.—The term 'investigative or law enforcement officer' means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of, or to make arrests for, offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses.

"(7) PERSON.—The term 'person' means any employee or agent of the United States, or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.

"(8) REMOTE COMPUTING SERVICE.—The term 'remote computing service' has the meaning given that term in section 2711.

"(9) STATE.—The term 'State' means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

"(10) WIRELESS COMMUNICATION DEVICE.—The term 'wireless communication device' means any device that enables access to, or use of, an electronic communication system or service, remote computing service, or geolocation information service, if that device utilizes a radio or other wireless connection to access such system or service.

"(11) COVERED SERVICE.—The term 'covered services' means electronic communication service, remote computing service, or of geolocation information service.

**"§ 2602. Interception and disclosure of geolocation information**

"(a) IN GENERAL.—

"(1) PROHIBITION ON DISCLOSURE OR USE.—Except as otherwise specifically provided in this chapter, it shall be unlawful for any person to—

"(A) intentionally intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, geolocation information pertaining to another person;

"(B) intentionally disclose, or endeavor to disclose, to any other person geolocation information pertaining to another person, knowing or having reason to know that the information was obtained through the interception of such information in violation of this paragraph;

"(C) intentionally use, or endeavor to use, any geolocation information, knowing or having reason to know that the information was obtained through the interception of such information in violation of this paragraph; or

"(D)(i) intentionally disclose, or endeavor to disclose, to any other person the geolocation information pertaining to another person intercepted by means authorized by subsections (b)

through (h), except as provided in such subsections;

"(ii) knowing or having reason to know that the information was obtained through the interception of such information in connection with a criminal investigation;

"(iii) having obtained or received the information in connection with a criminal investigation; and

"(iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation.

"(2) PENALTY.—Any person who violates paragraph (1) shall be fined under this title, imprisoned not more than five years, or both.

"(b) EXCEPTION FOR INFORMATION ACQUIRED IN THE NORMAL COURSE OF BUSINESS.—It shall not be unlawful under this chapter for an officer, employee, or agent of a provider of covered services, whose facilities are used in the transmission of geolocation information, to intercept, disclose, or use that information in the normal course of the officer, employee, or agent's employment while engaged in any activity which is a necessary incident to the rendition of service or to the protection of the rights or property of the provider of that service, except that a pro-

1 vider of a geolocation information service to the public
2 shall not utilize service observing or random monitoring
3 except for mechanical or service quality control checks.

4 "(c) EXCEPTION FOR CONDUCTING FOREIGN INTEL-
5 LIGENCE SURVEILLANCE.—Notwithstanding any other
6 provision of this chapter, it shall not be unlawful for an
7 officer, employee, or agent of the United States in the nor-
8 mal course of the official duty of the officer, employee,
9 or agent to conduct electronic surveillance, as authorized
10 by the Foreign Intelligence Surveillance Act of 1978 (50
11 U.S.C. 1801 et seq.).

12 "(d) EXCEPTION FOR CONSENT.—

13 "(1) IN GENERAL.—It shall not be unlawful
14 under this chapter for a person to intercept
15 geolocation information pertaining to another person
16 if such other person has given prior consent to such
17 interception unless such information is intercepted
18 for the purpose of committing any criminal or
19 tortious act in violation of the Constitution or laws
20 of the United States or of any State.

21 "(2) CHILDREN.—The exception in paragraph
22 (1) permits a parent or legal guardian of a child to
23 intercept geolocation information pertaining to that
24 child or to give consent for another person to inter-
25 cept such information.

1 "(e) EXCEPTION FOR PUBLIC INFORMATION.—It
2 shall not be unlawful under this chapter for any person
3 to intercept or access geolocation information relating to
4 another person through any system that is configured so
5 that such information is readily accessible to the general
6 public.

7 "(f) EXCEPTION FOR EMERGENCY INFORMATION.—
8 It shall not be unlawful under this chapter for any inves-
9 tigative or law enforcement officer or other emergency re-
10 sponder to intercept or access geolocation information re-
11 lating to a person if such information is used—

12 "(1) to respond to a request made by such per-
13 son for assistance; or

14 "(2) in circumstances in which it is reasonable
15 to believe that the life or safety of the person is
16 threatened, to assist the person.

17 "(g) EXCEPTION FOR THEFT OR FRAUD.—It shall
18 not be unlawful under this chapter for a person acting
19 under color of law to intercept geolocation information
20 pertaining to the location of another person who has un-
21 lawfully taken the device sending the geolocation informa-
22 tion if—

23 "(1) the owner or operator of such device au-
24 thorizes the interception of the person's geolocation
25 information;

"(2) the person acting under color of law is lawfully engaged in an investigation; and

"(3) the person acting under color of law has reasonable grounds to believe that the geolocation information of the other person will be relevant to the investigation.

"(h) EXCEPTION FOR WARRANT.—

"(1) DEFINITIONS.—In this subsection:

"(A) COURT OF COMPETENT JURISDICTION.—The term 'court of competent jurisdiction' includes—

"(i) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that—

"(I) has jurisdiction over the offense being investigated;

"(II) is in or for a district in which the provider of a geolocation information service is located or in which the geolocation information is stored; or

"(III) is acting on a request for foreign assistance pursuant to section 3512 of this title; or

1 "(ii) a court of general criminal juris-
2 diction of a State authorized by the law of
3 that State to issue search warrants.
4 "(B) GOVERNMENTAL ENTITY.—The term
5 'governmental entity' means a department or
6 agency of the United States or any State or po-
7 litical subdivision thereof.
8 "(2) WARRANT.—A governmental entity may
9 intercept geolocation information or require the dis-
10 closure by a provider of covered services of
11 geolocation information only pursuant to a warrant
12 issued using the procedures described in the Federal
13 Rules of Criminal Procedure (or, in the case of a
14 State court, issued using State warrant procedures)
15 by a court of competent jurisdiction, or as otherwise
16 provided in this chapter or the Foreign Intelligence
17 Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).
18 "(i) PROHIBITION ON DIVULGING GEOLOCATION IN-
19 FORMATION.—
20 "(1) IN GENERAL.—Except as provided in para-
21 graph (2), a person providing covered services shall
22 not intentionally divulge geolocation information per-
23 taining to another person.
24 "(2) EXCEPTIONS.—A person providing covered
25 services may divulge geolocation information—

"(A) as otherwise authorized in subsections (b) through (h);

"(B) with the lawful consent of such other person;

"(C) to another person employed or authorized, or whose facilities are used, to forward such geolocation information to its destination; or

"(D) which was inadvertently obtained by the service provider and which appears to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

**"§ 2603. Prohibition of use as evidence of acquired geolocation information**

"Whenever any geolocation information has been acquired, no part of such information and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

**"§ 2604. Emergency situation exception**

"(a) EMERGENCY SITUATION EXCEPTION.—Notwithstanding any other provision of this chapter, any in-

1 vestigative or law enforcement officer, specially designated
2 by the Attorney General, the Deputy Attorney General,
3 the Associate Attorney General, or by the principal pros-
4 ecuting attorney of any State or subdivision thereof acting
5 pursuant to a statute of that State, may intercept
6 geolocation information if—
7 "(1) such officer reasonably determines that an
8 emergency situation exists that—
9 "(A) involves—
10 "(i) immediate danger of death or se-
11 rious physical injury to any person;
12 "(ii) conspiratorial activities threat-
13 ening the national security interest; or
14 "(iii) conspiratorial activities char-
15 acteristic of organized crime; and
16 "(B) requires geolocation information be
17 intercepted before an order authorizing such
18 interception can, with due diligence, be ob-
19 tained;
20 "(2) there are grounds upon which an order
21 could be entered to authorize such interception; and
22 "(3) an application for an order approving such
23 interception is made within 48 hours after the inter-
24 ception has occurred or begins to occur.
25 "(b) FAILURE TO OBTAIN COURT ORDER.—

"(1) TERMINATION OF ACQUISITION.—In the absence of an order, an interception of geolocation information carried out under subsection (a) shall immediately terminate when the information sought is obtained or when the application for the order is denied, whichever is earlier.

"(2) PROHIBITION ON USE AS EVIDENCE.—In the event such application for approval is denied, the geolocation information shall be treated as having been obtained in violation of this chapter and an inventory shall be served on the person named in the application.

**"§ 2605. Recovery of civil damages authorized**

"(a) IN GENERAL.—Any person whose geolocation information is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person, other than the United States, which engaged in that violation such relief as may be appropriate.

"(b) RELIEF.—In an action under this section, appropriate relief includes—

"(1) such preliminary and other equitable or declaratory relief as may be appropriate;

"(2) damages under subsection (c) and punitive damages in appropriate cases; and

1 "(3) a reasonable attorney's fee and other liti-
2 gation costs reasonably incurred.
3 "(c) COMPUTATION OF DAMAGES.—The court may
4 assess as damages under this section whichever is the
5 greater of—
6 "(1) the sum of the actual damages suffered by
7 the plaintiff and any profits made by the violator as
8 a result of the violation; or
9 "(2) statutory damages of whichever is the
10 greater of $100 a day for each day of violation or
11 $10,000.
12 "(d) DEFENSE.—It is a complete defense against any
13 civil or criminal action brought against an individual for
14 conduct in violation of this chapter if such individual acted
15 in a good faith reliance on—
16 "(1) a court warrant or order, a grand jury
17 subpoena, a legislative authorization, or a statutory
18 authorization;
19 "(2) a request of an investigative or law en-
20 forcement officer under section 2604; or
21 "(3) a good-faith determination that an excep-
22 tion under section 2602 permitted the conduct com-
23 plained of.
24 "(e) LIMITATION.—A civil action under this section
25 may not be commenced later than two years after the date

1 upon which the claimant first has a reasonable oppor-
2 tunity to discover the violation.

3 "(f) ADMINISTRATIVE DISCIPLINE.—If a court or ap-
4 propriate department or agency determines that the
5 United States or any of its departments or agencies has
6 violated any provision of this chapter, and the court or
7 appropriate department or agency finds that the cir-
8 cumstances surrounding the violation raise serious ques-
9 tions about whether or not an officer or employee of the
10 United States acted willfully or intentionally with respect
11 to the violation, the department or agency shall, upon re-
12 ceipt of a true and correct copy of the decision and find-
13 ings of the court or appropriate department or agency
14 promptly initiate a proceeding to determine whether dis-
15 ciplinary action against the officer or employee is war-
16 ranted. If the head of the department or agency involved
17 determines that disciplinary action is not warranted, such
18 head shall notify the Inspector General with jurisdiction
19 over the department or agency concerned and shall provide
20 the Inspector General with the reasons for such deter-
21 mination.

22 "(g) IMPROPER DISCLOSURE IS VIOLATION.—Any
23 willful disclosure or use by an investigative or law enforce-
24 ment officer or governmental entity of information beyond

the extent permitted by this chapter is a violation of this chapter for purposes of this section.".

(b) CLERICAL AMENDMENT.—The table of chapters for part 1 of title 18, United States Code, is amended by inserting after the item relating to chapter 119 the following:

"120. Geolocation information ..... 2601".

(c) CONFORMING AMENDMENTS.—Section 3512(a) of title 18, United States Code, is amended—

(1) in paragraph (2)—

(A) by redesignating subparagraphs (B), (C), and (D) as subparagraphs (C), (D), and (E), respectively; and

(B) by inserting after subparagraph (A) the following:

"(B) a warrant or order for geolocation information or records related thereto, as provided under section 2602 of this title;".

**SEC. 3. REQUIREMENT FOR SEARCH WARRANTS TO ACQUIRE GEOLOCATION INFORMATION.**

Rule 41(a) of the Federal Rules of Criminal Procedure is amended—

(1) in paragraph (2)(A), by striking the period at the end and inserting a comma and "including geolocation information."; and

(2) by adding at the end the following:

"(F) 'Geolocation information' has the meaning given that term in section 2601 of title 18, United States Code.".

**SEC. 4. FRAUD AND RELATED ACTIVITY IN CONNECTION WITH OBTAINING GEOLOCATION INFORMATION.**

(a) CRIMINAL VIOLATION.—Section 1039(h) of title 18, United States Code, is amended—

(1) in paragraph (2)—

(A) in subparagraph (A), by striking "and" at the end;

(B) in subparagraph (B), by striking the period at the end and inserting a semicolon and "and"; and

(C) by adding at the end the following new subparagraph:

"(C) includes any geolocation information service.";

(2) by redesignating paragraph (4) as paragraph (5); and

(3) by inserting after paragraph (3) the following:

"(4) GEOLOCATION INFORMATION SERVICE.—The term 'geolocation information service' has the meaning given that term in section 2601.".

(b) CONFORMING AMENDMENTS.—

(1) DEFINITION AMENDMENTS.—Section 1039(h)(1) of title 18, United States Code, is amended—

(A) in the paragraph heading, by inserting "OR GPS" after "PHONE"; and

(B) in the matter preceding subparagraph (A), by inserting "or GPS" after "phone".

(2) CONFORMING AMENDMENTS.—Section 1039 of title 18, United States Code, is amended—

(A) in the section heading by inserting "**or GPS**" after "**phone**";

(B) in subsection (a)—

(i) in the matter preceding paragraph (1), by inserting "or GPS" after "phone"; and

(ii) in paragraph (4), by inserting "or GPS" after "phone";

(C) in subsection (b)—

(i) in the subsection heading, by inserting "OR GPS" after "PHONE";

(ii) in paragraph (1), by inserting "or GPS" after "phone" both places that term appears; and

(iii) in paragraph (2), by inserting "or GPS" after "phone"; and

(D) in subsection (c)—

(i) in the subsection heading, by inserting "OR GPS" after "PHONE";

(ii) in paragraph (1), by inserting "or GPS" after "phone" both places that term appears; and

(iii) in paragraph (2), by inserting "or GPS" after "phone".

(3) CHAPTER ANALYSIS.—The table of sections for chapter 47 of title 18, United States Code, is amended by striking the item relating to section 1039 and inserting the following:

"1039. Fraud and related activity in connection with obtaining confidential phone or GPS records information of a covered entity.".

(c) SENTENCING GUIDELINES.—

(1) REVIEW AND AMENDMENT.—Not later than 180 days after the date of enactment of this Act, the United States Sentencing Commission, pursuant to its authority under section 994 of title 28, United States Code, and in accordance with this section, shall review and, if appropriate, amend the Federal sentencing guidelines and policy statements applicable to persons convicted of any offense under section

1039 of title 18, United States Code, as amended by this section.

(2) AUTHORIZATION.—The United States Sentencing Commission may amend the Federal sentencing guidelines in accordance with the procedures set forth in section 21(a) of the Sentencing Act of 1987 (28 U.S.C. 994 note) as though the authority under that section had not expired.

**SEC. 5. STATEMENT OF EXCLUSIVE MEANS OF ACQUIRING GEOLOCATION INFORMATION.**

(a) IN GENERAL.—No person may acquire the geolocation information of a person for protective activities or law enforcement or intelligence purposes except pursuant to a warrant issued pursuant to rule 41 of the Federal Rules of Criminal Procedure, as amended by section 3, or the amendments made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(b) GEOLOCATION INFORMATION DEFINED.—In this section, the term "geolocation information" has the meaning given that term in section 2601 of title 18, United States Code, as amended by section 2.

○



○