GEOLOCATION TECHNOLOGY AND PRIVACY

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

MARCH 2, 2016

Serial No. 114–107

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PUBLISHING OFFICE

23–406 PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing 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 OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
JIM JORDAN, Ohio
TIM WALBERG, Michigan
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
CYNTHIA M. LUMMIS, Wyoming
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
RON DESANTIS, Florida
MICK MULVANEY, South Carolina
KEN BUCK, Colorado
MARK WALKER, North Carolina
ROD BLUM, Iowa
JODY B. HICE, Georgia
STEVE RUSSELL, Oklahoma
EARL L. "BUDDY" CARTER, Georgia
GLENN GROTHMAN, Wisconsin
WILL HURD, Texas
GARY J. PALMER, Alabama

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MATT CARTWRIGHT, Pennsylvania
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
TED LIEU, California
BONNIE WATSON COLEMAN, New Jersey
STACEY E. PLASKETT, Virgin Islands
MARK DESAULNIER, California
BRENDAN F. BOYLE, Pennsylvania
PETER WELCH, Vermont
MICHELLE LUJAN GRISHAM, New Mexico

JENNIFER HEMINGWAY, *Staff Director*
DAVID RAPALLO, *Minority Staff Director*
TROY STOCK, *Subcommittee on Transportation and Public Assets Staff Director*
SEAN BREBBIA, *Counsel*
WILLIE MARX, *Clerk*

CONTENTS

GEOLOCATION TECHNOLOGY AND PRIVACY

Wednesday, March 2, 2016

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
WASHINGTON, D.C.

The committee met, pursuant to call, at 10:03 a.m., in Room 2154, Rayburn House Office Building, Hon. Jason Chaffetz [chairman of the committee] presiding.

Present: Representatives Chaffetz, Mica, Jordan, Walberg, Amash, DesJarlais, Massie, Meadows, DeSantis, Buck, Walker, Blum, Hice, Carter, Grothman, Hurd, Cummings, Lynch, Connolly, Cartwright, Duckworth, Kelly, Lieu, Plaskett, and Welch.

Chairman CHAFFETZ. The Committee on Oversight and Government Reform will come to order.

Without objection, the chair is authorized to declare a recess at any time.

Thank you all for being here. In today's modern age, this is a new phenomenon, new waters, new areas that we are chartering here. And these technological advances, particularly with smartphones, have made it easier to solve crimes and to take criminals off the streets, but it also makes it easier and less expensive for law enforcement to track people's movements over long periods of time. And keep in mind, as we address these issues with law enforcement, there are also issues that bleed over in how organized crime, how individuals can use these types of technologies in a very nefarious way as well.

But these advances make it possible to conduct either historical or real-time prolonged surveillance previously unachievable with traditional surveillance techniques. And prolonged surveillance of geolocation reveals intimate personal details far exceeding mere location.

As the D.C. Circuit noted, "A person who knows all of another's travels 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 political groups, and not just one such fact about a person but all such facts."

Geolocation is more than just a record of where we are or were; it is a window into who we are. Do you want your Uber trip records to have Fourth Amendment protection? What about your Fitbit data? What about your smartphone information?

The Department of Justice takes an interesting position on this. The Director of National Intelligence recently acknowledged that, "In the future, intelligence services might use the Internet of

Things for identification, surveillance, monitoring, location tracking, and targeting for recruitment or to gain access to networks or use credentials."

In plain English, he is saying that the government intends to appropriate the technology you buy and can strip the companies you entrust with your data to be the arms of the State to spy on you. It doesn't seem like too much to ask the executive branch that before prying into your life it at least convince a neutral judge they have probable cause for doing so.

Protection against unreasonable government searches is a cornerstone of our democracy. It is an expectation in our life. I do believe that each American has an expectation and a right to privacy. The Fourth Amendment provides "the right of people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated."

Think about what you keep on your smartphone, everything from banking information and personal health data, sensitive communications, family photos, and who knows what in the future. It sounds a lot like persons, houses, papers, and effects to me.

In April of 2014, the committee began an investigation into law enforcement's use of cell-site simulators after press reports allege widespread use of devices also known as stingrays to locate people, that using the word stingray in a generic term. There are lots of other brand names that are out there.

The committee discovered multiple executive branch agencies possessing these devices with the Department of Justice alone possessing hundreds of these devices. Even the IRS has a stingray, the IRS. What in the world are they doing with that machine? I do not trust Commissioner Koskinen and the IRS with this technology, especially after the agency targeted individuals for their political beliefs.

The committee's investigation confirmed, as many suspected, that law enforcement was using these devices without first obtaining a warrant. And the Supreme Court agrees. In Jones v. United States, the Supreme Court unanimously, unanimously rejected the government's warrantless use of a GPS device. In that case, Justice Alito remarked that Congress should solve these issues legislatively, and I happen to agree with that.

One of our witnesses here today worked with law enforcement and privacy advocates in the State of Virginia to update Virginia's laws post-Jones to ensure they adhere to the Fourth Amendment and gave law enforcement the legal tools necessary to catch and prosecute bad guys and women in this digital age. And my home State of Utah has done the same, as has California.

It is time for Congress to follow the lead. I happen to have introduced H.R. 491, the Geolocation Privacy and Surveillance Act, in a bipartisan way, in a bicameral way with good leadership there in the Senate in a bipartisan way as well. It provides law enforcement clear legal guidelines, when and how to use geolocation information, how it can be collected, addressed, and used. I intend to pursue all opportunities I can to make our fellow Members and the public aware of this type of technology and what it can mean in your life.

We are going to hear a lot today about government rules and protocols, but as Chief Justice John Roberts wrote in a case holding that police need a warrant to search a smartphone after arrest, the Founders did not fight a revolution to gain access to government rules and protocols. Just because it is easier in 2016 for law enforcement to track our location and learn intimate details about our lives, it doesn't mean those details are somehow less worthy of constitutional protection. I stand with the Founders; get a warrant.

We have a lot to talk about here. In this day and age, not only are we looking, as the Oversight Committee, into the past, but I think we also need to look into the future. And a lot of these tools can be used in a good way to make people's lives better, but we also have to make sure on what sort of privacy we are giving up in the name of security. We had a good hearing yesterday in Judiciary talking about it with the Director of the FBI, talking about a similar type of technologies and what we are going to do or not do with encryption. But dealing with geolocation is something that we want to explore here today and we have a good healthy panel for that.

Chairman CHAFFETZ. So I would now like to recognize our ranking member, Mr. Cummings of Maryland.

Mr. CUMMINGS. Thank you very much, Mr. Chairman. And I welcome all of our witnesses today.

Today's hearing provides an opportunity to discuss both the privacy concerns and law enforcement interests in obtaining geolocation information about our constituents. Geolocation information provides tracking capabilities with great accuracy making it a valuable law enforcement tool. This information can reveal intimate details of a person's life, which raises significant concern about whether the American people have a right to expect their private information be treated as such.

It is important that our law enforcement authorities have the ability to carry out their public safety duties, and it is also important that we protect the privacy rights of American citizens. Currently, Federal law enforcement officials use authority under the Stored Communications Act to obtain location records from wireless service providers. This law requires law enforcement authorities to provide "specific and articulable facts" demonstrating "reasonable grounds" to believe that the information they seek is "relevant and material to an ongoing criminal investigation."

Right now, there is a split among Federal courts. Some have held that the Americans have a reasonable expectation of privacy over this type of information. They require law enforcement to obtain a search warrant based on probable cause. Others have held that Americans do not have a reasonable expectation of privacy because they voluntarily use their cell phones in this manner. These courts require law enforcement to obtain a court order under the lower standard of reasonable suspicion.

This is a legitimate and challenging issue with reasonable voices on both sides. For example, on the one hand, the chairman has a bill that would create a uniform standard that recognize privacy interests and would require law enforcement to obtain warrants based upon probable cause. There are strong benefits to this ap-

proach, and it is supported by Senator Wyden, Ranking Member Conyers, and our own Congressman Welch.

There are also voices on the other side. For example, Congressman Gowdy has expressed concern that this approach could impair the efforts of law enforcement authorities to investigate and solve crimes.

Today, I welcome this debate because I want to make sure that we are striking the right balance. I look forward to hearing from all of our witnesses to help us continue to inform this debate and to ensure that we help our law enforcement authorities while protecting the privacy rights of our constituents.

And with that, I yield back.

Chairman CHAFFETZ. I thank the gentleman. I will hold the record open for 5 legislative days for any members who would like to submit a written statement.

And I will now recognize our panel of witnesses. We are pleased to welcome Mr. Richard Downing, Acting Assistant Attorney General in the Criminal Division at the United States Department of Justice. Mr. Michael Doucette is the Commonwealth's attorney in Lynchburg, Virginia. I appreciate your being here today. Mr. Paul Larkin, Jr., Senior Legal Research Fellow for the Edwin Meese III Center for Legal and Judicial Studies at the Heritage Foundation; and Ms. Neema Singh Guliani. Did I pronounce it right?

[Nonverbal response.]

Chairman CHAFFETZ. Guliani, Legislative Counsel for the American Civil Liberties Union. We do appreciate you all being here and your participation today.

So if you would please rise and raise your right hand. Pursuant to committee rules, all witnesses are to be sworn before they testify.

[Witnesses sworn.]

Chairman CHAFFETZ. Thank you. Let the record reflect that all witnesses answered in the affirmative.

In order to allow time for members to ask questions, we would appreciate your limiting any oral testimony to 5 minutes. Your entire written statement will be made part of the record.

Mr. Downing, you are now recognized for 5 minutes.

WITNESS STATEMENTS

STATEMENT OF RICHARD DOWNING

Mr. DOWNING. Thank you very much. Good morning, Chairman Chaffetz, Ranking Member Cummings, and members of the committee. Thank you for the opportunity to appear before you today.

I'd like to begin with the facts of a case based on public filings. The United States District Court judge in Jacksonville, Florida, was sitting in his living room one night, a shot from a high-powered rifle shattered his window. He was injured, but thankfully, the bullet did not hit him. The police had no eyewitnesses and a very large pool of suspects, including many litigants and defendants who had appeared before the judge.

So what did the investigators do? Among other things, they applied for court orders to obtain the cell tower records of the phones of some of the possible suspects. Those records provided a general

idea of the location of the phones. This information advanced the investigation and allowed agents to exclude certain innocent people and pursue leads that eventually led to the arrest of the alleged shooter. This case is just one example of the importance of location information to a wide variety of criminal investigations.

I should emphasize, however, that there is no single kind of geolocation information. Location information can differ in precision, everything from what country the phone is in to precise GPS measurements of latitude and longitude. Sometimes companies generate location information for their own business purposes, and other times, law enforcement may gather the information directly. Sometimes, it is generated continuously as the phone moves around. Other times, only when certain events happen like when a user places a call.

The Department recognizes the importance of considering individual privacy interests when obtaining different kinds of location information. At the same time, location information plays an important and sometimes pivotal role in our efforts to protect public safety and to seek justice. And it is important to recognize that different kinds of location information implicate different privacy concerns.

In the time that I have, it would be impossible to discuss in detail all of the various types of location information. And I would like to mention just two types: first, cell-site information; and second, information collected by cell-site simulators.

I recognize that these two types of information have confusingly similar names. Cell-site information is generated by cellular phone companies. A cell-site simulator is equipment operated directly by law enforcement officers. Cell-site information consists of business records that wireless carriers routinely collect and maintain as part of providing cellular service. These records identify the towers and sometimes the face of those towers handling communications with a particular device. While not providing pinpoint accuracy, the fact that a tower handled communications with a phone can give an idea of the location of the phone at the time that the communication occurred.

Providers collect and maintain cell-site records for their own business purposes such as to repair and improve their networks. This data is collected only periodically when calls and other communications occur, not continually, and courts have found that historical cell-site information may be obtained based on a court order under the Electronic Communications Privacy Act, as Congressman Cummings mentioned in his opening.

This provision requires the court to find that the government has provided specific and articulable facts showing that a substantial but not quite at the level of probable cause. Historical cell-site information can play a critical role at the outset of an investigation when there is not sufficient evidence yet to satisfy a probable cause standard such as in the shooting that I mentioned earlier.

I'd like to turn now to cell-site simulators, the equipment owned and operated by police officers. A cell-site simulator collects a limited set of signaling information, not the content of communications, from cellular devices in the vicinity of the simulator. It can be used to figure out the location of a suspect's phone.

The Department recognizes that the collection of precise location information in real time implicates different privacy interests than less precise information generated by a provider for its business purposes. That is why last September the Department issued a new policy governing the use of cell-site simulators in domestic criminal investigations. Under the policy, law enforcement agents now are generally required to obtain a search warrant supported by probable cause before using such a device.

In conclusion, I'd like to emphasize that the Department is dedicated to ensuring that its policies and practices comply with the law and promote the privacy and civil liberties of individuals while we fulfill our mission to protect the public and to seek justice.

Thank you, and I look forward to answering your questions.

[Prepared statement of Mr. Downing follows:]

Department of Justice

STATEMENT OF

RICHARD W. DOWNING
ACTING DEPUTY ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED

"GEOLOCATION TECHNOLOGY AND PRIVACY"

PRESENTED

MARCH 2, 2016

Richard W. Downing
Acting Deputy Assistant Attorney General
Department of Justice

Before the
Committee on Oversight and Government Reform
U.S. House of Representatives

At a Hearing Entitled
"Geolocation Technology and Privacy"

Presented
March 2, 2016

Good morning, Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee. Thank you for the opportunity to appear before you today to discuss the topic of geolocation information. The Department recognizes the importance of considering individual privacy interests when obtaining different types of geolocation information. At the same time, location information often plays an important and sometimes pivotal role in our efforts to protect public safety and seek justice. I will discuss some of the types of location information that Federal law enforcement investigators obtain, the types of legal authorization utilized to do so, and the standards that we must meet in order to obtain that legal authorization.

"Geolocation information" is not a single kind of information, nor is there one agreed-upon definition. Law enforcement uses a variety of different kinds of location information that provide some indication of the location of a particular person or thing. Depending on what type of location information is at issue, such information has different evidentiary significance, and how it is accessed implicates very different privacy concerns and legal provisions.

Location information can differ in how precisely the data can identify location, from the most general, such as the country in which someone or something is located, to the quite specific, such as measurements of latitude and longitude generated by a GPS system. Information concerning the location of a person or a thing is sometimes gathered directly by law enforcement officers, such as through the use of cell site simulators. In other circumstances, officers obtain location information from cell phone carriers and other commercial entities. These companies sometimes collect location information for their own business purposes, such as to improve their networks or target advertising, and at other times only in response to a warrant or order issued by a court. Some types of location information are collected continuously, while other types are collected only periodically or in connection with a specific transaction or event.

Let me provide some examples of how location information can be critical to solving crimes, protecting public safety, and seeking justice.

In one case, after a U.S. District Court judge in Jacksonville, Florida, was shot at with a high-powered rifle while he sat in his living room – and, thankfully, was not seriously harmed – investigating agents were faced with a very large pool of potential suspects, including many defendants and litigants who had appeared before that judge. Agents were able to use court orders issued under section 2703(d) of the Electronic Communications Privacy Act to obtain cell-site records that significantly narrowed the list of potential suspects. This advanced the investigation and conserved investigative resources by allowing agents to exclude certain potential suspects and pursue leads that eventually led to the arrest of the alleged shooter.

Another example concerns the fatal shooting of two students at the University of Southern California while they were parked in a vehicle near campus in 2012. The subjects stole the victims' cell phones. Ballistics evidence tied the shooting to another shooting earlier that year, causing investigators to focus on two suspects. The suspects' phone records, including historical cell-site information, were obtained with the State equivalent of a 2703(d) order. The location information showed that the suspects were in the vicinity of the crime scene at the time of the shooting, and they also showed that the suspects' phones were in the same vicinity as the victims' phones after the homicide. This information was critical to developing additional evidence supporting the murder prosecutions against the suspects. They were charged and convicted and are both serving sentences of life in prison without the possibility of parole.

Although it would be impossible to discuss in detail all of the varying types of location information, I would like to describe several categories of such information and the legal authority that typically is required to obtain that information. I will start with more precise location information carrying stronger privacy interests and which, because of constitutional or statutory requirements or Department policy, require a higher legal showing to obtain.

GPS and Similar Location Information from Wireless Carriers

Some carriers have the ability to determine the location of a user's wireless device by relying on the device's built-in GPS capability. Other carriers do not rely on GPS, but have similar capabilities to locate a device by measuring signals the device sends to multiple towers or other antennas. The FCC has mandated that all carriers have this capability so that emergency responders can find the device when the user dials 911. Using such techniques, a carrier can determine fairly precisely the phone's location and can do so nearly continuously. Such location information is generally only created when the user dials 911 or when the carrier receives legal process.

To obtain this information on a prospective basis from a wireless carrier, officers generally obtain a search warrant from a court based on probable cause. Exceptions to this rule include special situations such as where the phone user has consented or where there is a life-and-death emergency. Our experience has been that such information about the precise location of a device is not generally available on a historical basis from wireless carriers because such

companies do not maintain such information in the ordinary course of business and without specific court authorization requiring it.

Use of Cell-Site Simulators

Cell-site simulators are devices operated by law enforcement officers that can help determine the location of a known cellular device. The technology works by collecting a limited set of signaling information from cellular devices in the vicinity of the simulator in order to find the relative signal strength and general direction of a particular cellular telephone. Cell-site simulators used by the Department must be configured as pen registers, and may not be used to collect the contents of any communication.

In September 2015, the Department issued a new policy governing its use of cell-site simulators in domestic criminal investigations. The policy is intended to enhance transparency and accountability, improve training and supervision, establish a higher and more consistent legal standard, and increase privacy protections.

The policy adopts a consistent legal standard for the Department's use of cell-site simulators in domestic criminal investigations. While the Department has, in the past, obtained appropriate legal authorization to use cell-site simulators pursuant to orders under the Pen Register Statute, law enforcement agents now are required to obtain a search warrant supported by probable cause before using such a device. The policy recognizes that there are limited exceptions to the warrant requirement, such as exigent circumstances.

Tracking Devices

Another type of device operated by law enforcement that can provide information about the location of a person or object is a tracking device. In *United States v. Jones*, the Supreme Court held that the warrantless installation of a tracking device on a target's vehicle, and the use of that device to monitor the location of the vehicle over a 28-day period, constituted a search within the meaning of the Fourth Amendment. In light of the *Jones* decision, law enforcement agents now generally obtain a search warrant supported by probable cause before the installation and monitoring of a tracking device on a vehicle. There are, however, circumstances including long-standing exceptions to the warrant requirement, such as consent or exigent circumstances, where a warrant would not be required.

Cell-Site Information

Another category of location information is called cell-site (or cell tower) information. Cell-site information consists of business records that wireless carriers routinely collect and maintain as part of the service they provide to customers. This type of data generally provides less exact and less detailed information about a device's location than the GPS and similar information discussed above.

Cellular devices operate through radio communications with a carrier's cell towers. When a user places or receives a call, or sends or receives a text or data message, the device sends signals to a cell tower. Most towers divide their coverage area into three roughly pie-shaped "sectors", each of which corresponds to a separate antenna (or "face") that receives signals from wireless devices. Because each tower does not have unlimited range, the fact that a particular tower and sector handled some or all of a communication gives a rough idea of the location of the device at the time that the communication occurred. The service area of the tower can vary widely, depending on such factors as local topography, network traffic, and whether it serves a rural or urban area.

The records of the towers and sectors handling communications with a particular device are called cell-site information. Carriers have discretion over what types of cell-site information they choose to record and keep and how long they keep it. Carriers generally keep cell-site information related to phone calls; some also keep records related to text messages or certain data transfers. We are not aware of any carrier that keeps records of cell-site information for every signal sent between a device and towers. Carriers usually keep cell-site records for at least six months. Courts can compel the disclosure of historical cell-site information (*i.e.*, the tower/sector records made by the carrier regarding calls or text messages sent or received by the user in the past). They can also compel the disclosure of similar information on an ongoing basis.

Historical cell-site information by definition does not provide the location of the device in real-time. Providers, in their ordinary course of business, collect and maintain records of which towers devices use for their own purposes. Carriers use this information to repair and improve their networks so that, for instance, customers have fewer dropped calls and faster downloads. In addition to being generally less precise than GPS or similar information, this data is collected by the provider only periodically.

The Electronic Communications Privacy Act allows a government entity to compel disclosure of historical cell-site records via a court order issued on a finding of "specific and articulable facts" that the records sought are relevant and material to an ongoing criminal investigation. These orders, often called 2703(d) orders, provide more privacy protection than a standard subpoena by mandating prior judicial review and requiring a higher evidentiary threshold than the traditional relevance standard for subpoenas. Most Federal courts that have considered the issue – including three circuit courts and more than twenty district courts – have held that the wireless carriers' historical business records about network activity are properly obtained with a court order under section 2703(d) of the Electronic Communications Privacy Act.[1]

---

[1]A handful of lower courts have held that a search warrant was required to obtain historical cell-site records. A panel of the Court of Appeals for the Fourth Circuit had held that a

Prospective cell-site records are similar to historical cell-site records except that a provider discloses the records to law enforcement on an ongoing basis. In normal circumstances, for the Department to obtain this information, at a minimum a court must issue an order based on a finding that the request has satisfied both the requirements of the Pen Register Statute and the requirements for a court order under section 2703(d) of the Electronic Communications Privacy Act. Some courts have required a search warrant.

Other Business Records from Which Location May Be Inferred

Finally, there are a variety of other types of records from which investigators and fact-finders may infer the location of a person or a thing at a particular time. For example, when someone withdraws money from an ATM, uses a credit card at a store, or pays a bridge toll, businesses generate records that, among other things, suggest that the customer was at a specific place at a specific time. The customer voluntarily conveys to the business the identity of her card or device, and the business commonly makes a record of the information along with the location of the transaction. Such records are generally generated by the business only as often as the transaction occurs.

Many of these records of business activities do not include providing customers with communication services and therefore are not covered by the Electronic Communications Privacy Act, and some of them are not covered by any statute. In line with longstanding Supreme Court precedent governing how the Government may obtain third-party business records, the Department generally relies upon subpoenas to compel disclosure of such records.

Conclusion

Given the wide variety of different types of information that provide some indication of the location of a particular person or thing—as well as the different ways in which this information is generated and maintained, the different levels of precision it offers, the different ways that such information can be accessed, and the different privacy implications – it is appropriate that the law provide a variety of mechanisms for law enforcement to acquire such information. The Department is dedicated to ensuring that its policies and practices comply with those laws and enable law enforcement officers to seek justice and protect public safety while continuing to uphold the Department's long-standing commitment to promoting individuals' privacy and civil liberties. We are pleased to engage with the Committee in a discussion about this important issue.

---

search warrant is required to obtain historical cell-site location; however, that panel decision was vacated and will be heard by the full Court soon.

Chairman CHAFFETZ. Thank you, Mr. Downing. I appreciate it. Mr. Doucette, you are now recognized for 5 minutes.

STATEMENT OF MICHAEL R. DOUCETTE

Mr. DOUCETTE. Chairman Chaffetz, Ranking Member Cummings, members of the committee, my name is Mike Doucette. I'm the elected Commonwealth's attorney for the city of Lynchburg, Virginia. I'm also currently a board member of the National District Attorneys Association, the largest association representing the voice of prosecutors around the country. And I appreciate the opportunity to address you today, Virginia's perspective on the use of geolocation information and changes made after the decision in United States v. Jones.

In response to that decision, Governor Bob McDonnell back in 2012 convened a small group consisting of prosecutors, defense attorneys, and law enforcement to draft a bill to allow for a search warrant specifically for the use of a GPS device. One of the problems with which we had to deal with the use of a GPS device was how to satisfy the particularity requirement for a search warrant when the product of that proposed search is neither in a particular location, nor is a particular item.

And another problem we had to deal with was providing service of the warrant on the target of that warrant—GPS warrant without tipping him off that he is under surveillance. It would do no good to serve a warrant—a copy of a search warrant with its attached affidavit to the person who is to be surveilled and then tell that person to go about his usual suspected criminal activity.

Our key concern in drafting this bill was how to issue a search warrant in one particular jurisdiction but allow it to be valid in any other jurisdiction to which the object, usually an automobile, would travel in the future. For standard search warrants, a search warrant is issued in the jurisdiction in which there is probable cause to believe that the evidence or contraband sought will be located at that static point in time when the warrant is executed.

And so to address this issue, we defined "use of a tracking device" to include the installation, the maintenance, and the monitoring of that particular device. The search warrant is valid for 30 days from issuance. Additional 30-day extensions may only be issued by a circuit court. The installation of the tracking device must be completed within 15 days of the issuance of the warrant, and the device must be removed or disabled within 10 days after the use of the device has ended.

Upon issuance of the warrant, the warrant and the affidavit are automatically sealed by the circuit court. There is a process for unsealing at the end of the use of that particular GPS search warrant. Both the warrant and the affidavit must be served on the owner or possessor within 10 days after the end of that use of that tracking device. And again, 30-day extensions may be granted by the circuit court.

In 2014, we anticipated through legislation what we believed United States v. Jones might ultimately lead, and so we amended our State counterpart to 18 U.S.C. 2703 to require a search warrant for the disclosure for up to 30 days of the real-time location data of any electronic device. Exceptions were added to the statute

in situations where there is administrative subpoena in child pornography cases and when there is an emergency circumstance or consent.

This specific bill was geared towards the real-time location data of mobile phones whether through pinging the phone by an electronic communication service or through the use of the phone's internal GPS. While the location of the phone does not necessarily identify the present location of the phone's owner, practical experience tells us that most of the time it does.

However, in this bill, we specifically did not include historic cell tower information. We subscribe to the United States Supreme Court's opinions which stated that "an individual enjoys no legitimate expectation of privacy" in the information he "voluntarily turns over to a third party." But we were also influenced by both the absence of the simultaneous monitoring of a person's present location and the lack of specificity in that location provided by the cell tower information. While GPS can pinpoint location within a few feet, historic cell tower information is far less accurate with the distances measured within thousands of feet more or less. The lack of specificity in this technology is based on several factors relating to signal strength, including distance to tower, intervening objects between the towers and the phone, the number of towers in the area, and the number of calls that a particular tower is handling.

In 2015, we amended that statute even further to include a requirement for a search warrant before law enforcement could use what is commonly referred to as a stingray because we had inadvertently left that out of the 2014 legislation.

In 2015, we—there were some bills introduced in the Virginia General Assembly to limit the time period for passive use of automated license plate readers. The bills were ultimately vetoed by the Governor and have not been reintroduced, although the patrons have promised to reintroduce those bills in next year's session.

And that in a nutshell, Mr. Chairman, highlights the Virginia legislative efforts in geolocation data and technology and its relationship with the Fourth Amendment for the past 4 years in Virginia. And I look forward to the opportunity to answer any questions.

[Prepared statement of Mr. Doucette follows:]

GEOLOCATION TECHNOLOGY & PRIVACY, VIRGINIA'S LEGISLATIVE REACTION TO UNITED STATES v. JONES

Remarks before the House Oversight and Government Reform Committee
Michael R. Doucette
Commonwealth's Attorney
City of Lynchburg, VA

Chairman Chaffetz, Ranking Member Cummings, members of the committee, my name is Michael Doucette and I am the elected Commonwealth's Attorney out of Lynchburg, Virginia. I am also currently a board member of the National District Attorneys Association (NDAA), the largest association representing the voice of prosecutors across the country. I appreciate the invitation to testify before you today to provide Virginia's perspective on the use of geolocation information and changes made after the United States v. Jones court decision.

2012

United States v. Jones was decided and announced by the United States Supreme Court on January 23, 2012. By that time, the last day for introducing bills for the 2012 Virginia General Assembly session had elapsed. Yet, many of us realized that we needed to do something

quickly and could not wait until the 2013 session. (Virginia has a part-time legislature, which meets only for either 6 weeks or 8 weeks in the winter.)

However, the rules of the General Assembly allow the Governor to request the introduction of a bill after the filing deadline. As a result, Governor Robert McDonnell's office convened a small group consisting of prosecutors, defense attorneys and law enforcement to draft a bill to allow for a search warrant specifically for the use of a GPS device.

One of the problems we had to deal with related to the use of a GPS device was how to satisfy the "particularity requirement" for a search warrant when the product of the proposed search is neither in a particular location nor is a particular item. Another problem dealt with providing service of the warrant on the target of the GPS warrant without tipping him off that he is under surveillance. It would do no good to serve a copy of the search warrant with the attached affidavit to the person to be surveilled, and then tell that person to go about his usual (criminal) activity. There was much frank discussion behind the scenes and a bill was ultimately crafted.

HB1298 (Delegate David Albo) was introduced in the House of Delegates on February 15, 2012 and SB685 (Senator Bryce Reeves *et al*) was introduced in the Senate on February 16, 2012. After the bill was slightly amended in both chambers, it passed and was signed by Governor McDonnell on April 5, 2012. Because the bill had an emergency clause, it went into effect immediately upon the Governor's signature.

The language as passed was this:

§ 19.2-56.2. Application for and issuance of search warrant for a tracking device; installation and use. —

A. As used in this section, unless the context requires a different meaning:

"Judicial officer" means a judge, magistrate, or other person authorized to issue criminal warrants.

"Law-enforcement officer" shall have the same meaning as in § 9.1-101.

"Tracking device" means an electronic or mechanical device that permits a person to remotely determine or track the position or movement of a person or object. "Tracking device" includes devices that store geographic data for subsequent access or analysis and devices that allow for the real-time monitoring of movement.

"Use of a tracking device" includes the installation, maintenance, and monitoring of a tracking device but does not include the interception of wire, electronic, or oral communications or the capture, collection, monitoring, or viewing of images.

B. A law-enforcement officer may apply for a search warrant from a judicial officer to permit the use of a tracking device. Each application for a search warrant authorizing the use of a tracking device shall be made in writing, upon oath or affirmation, to a judicial officer for the circuit in which the tracking device is to be installed, or where there is probable cause to believe the offense for which the tracking device is sought has been committed, is being committed, or will be committed.

The law-enforcement officer shall submit an affidavit, which may be filed by electronically transmitted (i) facsimile process or (ii) electronic record as defined in § 59.1-480, and shall include:

1. The identity of the applicant and the identity of the law-enforcement agency conducting the investigation;

2. The identity of the vehicle, container, item, or object to which, in which, or on which the tracking device is to be attached, placed, or otherwise installed; the name of the owner or possessor of the vehicle, container, item, or object described, if known; and the jurisdictional area in which the vehicle, container, item, or object described is expected to be found, if known;

3. Material facts constituting the probable cause for the issuance of the search warrant and alleging substantially the offense in relation to which such tracking device is to be used and a showing that probable cause exists that the information likely to be obtained will be evidence of the commission of such offense; and

4. The name of the county or city where there is probable cause to believe the offense for which the tracking device is sought has been committed, is being committed, or will be committed.

C. 1. If the judicial officer finds, based on the affidavit submitted, that there is probable cause to believe that a crime has been committed, is being committed, or will be committed and that there is probable cause to believe the information likely to be obtained from the use of the tracking device will be evidence of the commission of such offense, the judicial officer shall issue a search warrant authorizing the use of the tracking device. The search warrant shall authorize the use of the tracking device from within the Commonwealth to track a person or property for a reasonable period of time, not to exceed 30 days from the issuance of the search warrant. The search warrant shall authorize the collection of the tracking data contained in or obtained from the tracking device but shall not authorize the interception of wire, electronic, or oral communications or the capture, collection, monitoring, or viewing of images.

2. The affidavit shall be certified by the judicial officer who issues the search warrant and shall be delivered to and preserved as a record by the clerk of the circuit court of the county or city where there is probable cause to believe the offense for which the tracking

device has been sought has been committed, is being committed, or will be committed. The affidavit shall be delivered by the judicial officer in person; mailed by certified mail, return receipt requested; or delivered by electronically transmitted facsimile process or by use of filing and security procedures as defined in the Uniform Electronic Transactions Act (§ 59.1-479 et seq.) for transmitting signed documents.

3. By operation of law, the affidavit, search warrant, return, and any other related materials or pleadings shall be sealed. Upon motion of the Commonwealth or the owner or possessor of the vehicle, container, item, or object that was tracked, the circuit court may unseal such documents if it appears that the unsealing is consistent with the ends of justice or is necessary to reasonably inform such person of the nature of the evidence to be presented against him or to adequately prepare for his defense.

4. The circuit court may, for good cause shown, grant one or more extensions, not to exceed 30 days each.

D. 1. The search warrant shall command the law-enforcement officer to complete the installation authorized by the search warrant within 15 days after issuance of the search warrant.

2. The law-enforcement officer executing the search warrant shall enter on it the exact date and time the device was installed and the period during which it was used.

3. Law-enforcement officers shall be permitted to monitor the tracking device during the period authorized in the search warrant, unless the period is extended as provided for in this section.

4. Law-enforcement officers shall remove the tracking device as soon as practical, but not later than 10 days after the use of the tracking device has ended. Upon request, and for good cause shown, the circuit court may grant one or more extensions for such removal for a period not to exceed 10 days each.

5. In the event that law-enforcement officers are unable to remove the tracking device as required by subdivision 4, the law-enforcement officers shall disable the device, if possible, and all use of the tracking device shall cease.

6. Within 10 days after the use of the tracking device has ended, the executed search warrant shall be returned to the circuit court of the county or city where there is probable cause to believe the offense for which the tracking device has been sought has been committed, is being committed, or will be committed, as designated in the search warrant, where it shall be preserved as a record by the clerk of the circuit court.

E. Within 10 days after the use of the tracking device has ended, a copy of the executed search warrant shall be served on the person who was tracked and the person

whose property was tracked. Service may be accomplished by delivering a copy to the person who, or whose property, was tracked or by leaving a copy with any individual found at the person's usual place of abode who is a member of the person's family, other than a temporary sojourner or guest, and who is 16 years of age or older and by mailing a copy to the person's last known address. Upon request, and for good cause shown, the circuit court may grant one or more extensions for such service for a period not to exceed 30 days each. Good cause shall include, but not be limited to, a continuing criminal investigation, the potential for intimidation, the endangerment of an individual, or the preservation of evidence.

F. The disclosure or publication, without authorization of a circuit court, by a court officer, law-enforcement officer, or other person responsible for the administration of this section of the existence of a search warrant issued pursuant to this section, application for such search warrant, any affidavit filed in support of such warrant, or any return or data obtained as a result of such search warrant that is sealed by operation of law is punishable as a Class 1 misdemeanor.

There were several key components to this drafting. Perhaps the most important was the definitional section at the very beginning.

- The concern was how to issue a search warrant in one particular jurisdiction but allow it to be valid in any other jurisdiction to which the object (usually an automobile) travelled in the future. For standard search warrants, a search warrant is issued in the jurisdiction in which there is probable cause to believe that the evidence or contraband sought will be located at that static point in time when the warrant is executed.

  To address this issue, we defined "use of a tracking device" to include the "installation, maintenance and ***monitoring***" of that device. The body of the statute then went on to discuss the mechanics of how a law enforcement officer would obtain and execute a search warrant for the use of a tracking device.

- The elements for the warrant's affidavit include identifying the object to be tracked, the names of the owner or possessor of that object, the jurisdiction in which that object is expected to be found, and the facts establishing probable cause to believe information about a criminal offense will be obtained by tracking that object.

- The search warrant itself is valid for 30 days from issuance. Additional 30 extensions may only be issued by the circuit court (Virginia's trial court of record). The installation of the tracking device must be completed within 15 days of the issuance of the warrant. The device must be removed within 10 days after the use of the device has ended. If for some reason the device cannot be removed, law enforcement must disable it.

- Upon issuance, the warrant and supporting affidavit are automatically sealed by the circuit court. Either the prosecution or any owner or possessor of the object tracked

> may move for unsealing. However, the warrant and affidavit must be served on the owner and the possessor, if different, within 10 days of the end of the use of the tracking device. Additional 30-day extensions of this service requirement may be granted by the circuit court if the investigation is still ongoing.

While we were not sure at the time that we were able to foresee all the problems of converting the general search warrant statute language to a GPS search warrant statute, it appears from the lack of any amendments to Section 19.2-56.2 since 2012 that we hit most of the high spots.

2014

Anticipating through legislation where we believed United States v. Jones might ultimately lead, in 2014 we amended VA Code §19.2-70.3 (Obtaining Records Concerning Electronic Communication Service or Remote Computing Service) to require a search warrant for the disclosure for up to 30 days of the ***real-time location data*** of any electronic device. (VA Code §19.2-70.3 is Virginia's version of 18 USC 2703.) Exceptions were added to the statute in situations where there is an administrative subpoena in a child pornography case and when there are emergency circumstances.

This bill was specifically geared towards the real-time location data of mobile telephones, whether through "pinging" the phone by an electronic communication service or through the use of the phone's internal GPS. While the location of the phone does not necessarily identify the location of the phone's owner, practical experience tells us that most of the time it does.

The 2014 amendments are in the italicized language as follows:

> C. *Except as provided in subsection D,* a provider of electronic communication service or remote computing service, including a foreign corporation that provides such services, shall disclose the contents of electronic communications *or real-time location data* to an investigative or law-enforcement officer only pursuant to a search warrant issued by a magistrate, a juvenile and domestic relations district court, a general district court, or a circuit court, based upon complaint on oath supported by an affidavit as required in § 19.2-54, or judicial officer or court of any of the several states of the United States or its territories, or the District of Columbia when the warrant issued by such officer or such court complies with the provisions of subsection G. In the case of a search warrant directed to a foreign corporation, the affidavit shall state that the complainant believes that the records requested are actually or constructively possessed by a foreign corporation that provides electronic communication service or remote computing service within the Commonwealth of Virginia. If satisfied that probable cause has been established for such belief and as required by Chapter 5 (§ 19.2-52 et seq.), the magistrate, the juvenile and domestic relations district court, the general district court, or the circuit court shall issue a warrant identifying those records to be searched for and commanding the person seeking such warrant to properly serve the warrant upon the foreign corporation.

D. A provider of electronic communication service or remote computing service, including a foreign corporation that provides such services, shall disclose a record or other information pertaining to a subscriber to or customer of such service, including real-time location data but excluding the contents of electronic communications, to an investigative or law-enforcement officer pursuant to an administrative subpoena issued pursuant to § 19.2-10.2 concerning a violation of § 18.2-374.1 or 18.2-374.1:1, former § 18.2-374.1:2, or § 18.2-374.3 when the information sought is relevant and material to an ongoing criminal investigation.

E. When disclosure of real-time location data is not prohibited by federal law, an investigative or law-enforcement officer may obtain real-time location data without a warrant in the following circumstances:

1. To respond to the user's call for emergency services;

2. With the informed, affirmative consent of the owner or user of the electronic device concerned if (i) the device is in his possession; (ii) the owner or user knows or believes that the device is in the possession of an employee or agent of the owner or user with the owner's or user's consent; or (iii) the owner or user knows or believes that the device has been taken by a third party without the consent of the owner or user;

3. With the informed, affirmative consent of the legal guardian or next of kin of the owner or user, if reasonably available, if the owner or user is reasonably believed to be deceased, is reported missing, or is unable to be contacted; or

4. If the investigative or law-enforcement officer reasonably believes that an emergency involving the immediate danger to a person requires the disclosure, without delay, of real-time location data concerning a specific person and that a warrant cannot be obtained in time to prevent the identified danger, and the possessor of the real-time location data believes, in good faith, that an emergency involving danger to a person requires disclosure without delay.

No later than three business days after seeking disclosure of real-time location data pursuant to this subsection, the investigative or law-enforcement officer seeking the information shall file with the appropriate court a written statement setting forth the facts giving rise to the emergency and the facts as to why the person whose real-time location data was sought is believed to be important in addressing the emergency.

J. A search warrant or administrative subpoena for the disclosure of real-time location data pursuant to this section shall require the provider to provide ongoing disclosure of such data for a reasonable period of time, not to exceed 30 days. A court may, for good cause shown, grant one or more extensions, not to exceed 30 days each.

K. For the purposes of this section:

"Electronic device" means a device that enables access to, or use of, an electronic communication service, remote computing service, or location information service, including a global positioning service or other mapping, locational, or directional information service.

"Real-time location data" means any data or information concerning the current location of an electronic device that, in whole or in part, is generated, derived from, or obtained by the operation of the device.

In a nutshell, these amendments resulted in the following:

- "Real time location data" may only be sought by law enforcement pursuant to a search warrant based on probable cause (or in the case of child pornography cases, pursuant to an administrative subpoena). This warrant is good for up to 30 days, with courts being authorized to grant additional 30 day extensions.

- Exceptions to this search warrant requirement include situations of emergencies, consent by a device's owner, consent by the next-of-kin of a missing person, or other exigent circumstances. If law enforcement invokes one of these emergency provisions, they must file with the court a written statement of the facts of the emergency.

Historic Cell-Tower Information

As drafters of this bill on real time location data, we specifically did not include "historic cell tower information." We subscribed to the United States Supreme Court's opinions which stated "an individual enjoys 'no legitimate expectation of privacy,' and so no Fourth Amendment protection, in information he "voluntarily turns over to a third party.' Smith v. Maryland, 442 U.S. 735, 743-44 (1979). This rule applies even when 'the information is revealed,' as it assertedly was here, 'on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.' United States v. Miller, 425 U.S. 435, 443 (1976)."

United States v. Graham, 796 F.3d 332, 378-79, (4th Cir. 2015)(J. Motz dissenting).

To a large degree, this was due to both the absence of simultaneously monitoring a person's present location and the lack of specificity in that location provided by cell tower information. While GPS can pinpoint location within feet, cell tower information is far less accurate with distances measured within thousands of feet, more or less. This technology is based on several factors relating to signal strength; including distance to tower, intervening objects between towers and the phone, the number of towers in the area and the number of calls a particular tower is handling.

2015

In 2015, Section 19.2-70.3 was further amended to include the requirement of a search warrant before law enforcement could use what is commonly referred to as a ***"sting ray."*** A "sting ray" is a fake cell phone tower used by law enforcement to locate cell phones.[1] "Sting Rays" were inadvertently left out of the 2014 legislation.

In 2015, there also were bills introduced in both chambers to limit the time period for the passive use of Automated License Plant Readers. These bills were debated extensively and modified many times. Ultimately, they passed the General Assembly as more expansive "surveillance technology" bills requiring a warrant. "Surveillance technology" was defined as "technology used to observe people, places or activities or to collect personal information, without the subject's knowledge or consent." Ultimately these bills were vetoed by Governor McAuliffe and were not reintroduced in the 2016 session, although the patrons have promised to raise the issue again in 2017 after further study.

United States v. Graham, 796 F.3d 332 (4th Cir. August 5, 2015)

On August 5, 2015, a three judge panel of the 4th Circuit Court of Appeals held that law enforcement's warrantless procurement of 221 days worth of historic cell tower information in the possession of electronic service providers to help prove that the defendants had participated in a string of robberies in Maryland was an unreasonable search in violation of the 4th Amendment. Historic cell tower information, although not as precise as GPS information, can be used to show generally the location of a mobile phone, and presumably the location of its owner.

However, because law enforcement acted in good faith on court orders (supported by less than probable cause) they obtained pursuant to the Electronic Communications Privacy Act and the Stored Communications Act, the Court held that the exclusionary rule did not apply in this case.

Specifically, the Court adopted the logic of the concurrence in United States v. Jones and held that "the government invades a reasonable expectation of privacy when it relies upon technology not in general use to discover the movements of an individual ***over an extended period of time***."

The 4th Circuit acknowledged that the 5th and the 11th circuits had reached the opposite conclusion concerning historic cell tower information. In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013); United States v. Quartavious Davis, 785 F.3d 498 (11th Cir. 2015). However, the 4th Circuit refused to "accept the proposition that cell phone users volunteer to convey their location information simply by choosing to activate and use

[1] *Stingray, the Fake Cell Phone Tower Cops and Carriers Use to Track Your Every Move,* ExtremeTech, http://www.extremetech.com/mobile/184597-stingray-the-fake-cell-phone-tower-cops-and-providers-use-to-track-your-every-move, June 17, 2014.

their cell phones and to carry the devices on their person" because "[c]ell phone use is not only ubiquitous in our society today but, at least for an increasing portion of our society, it has become essential to full cultural and economic participation."

In November 2015, the 4th Circuit issued an order calling for a rehearing *en banc* in this case. That hearing is scheduled to take place on March 22, 2016.

Thank you for the opportunity to testify before you today, and I look forward to answering any questions the committee may have on this subject.

Chairman CHAFFETZ. Thank you. I appreciate it.

Mr. Larkin, you are now recognized for 5 minutes.

STATEMENT OF PAUL J. LARKIN, JR.

Mr. LARKIN. Mr. Chairman, Mr. Ranking Member, and members of the committee, I want to thank you for the opportunity to try to help you puzzle through this difficult issue. I'm going to make only three points.

First, current settled Supreme Court case law allows the government to obtain historical cell-site or cell-location information without a warrant and without any showing of justification or need. It may be that the Supreme Court will change that law, but they've not yet done so, so that's the baseline from which we operate with respect to the Fourth Amendment. You of course could go further by statute, but the Fourth Amendment doesn't require you to go further at this point.

Second, the technology that the chairman mentioned—stingrays—are a new development that allow law enforcement to obtain this information without going through a carrier. The problem, however, is the way the device works. As I understand it, the device works by capturing all the cell phone signals within a radius of the operating device. The effect, therefore, is to shut off those other cell phones of everyone else who is within that radius. One of the problems in this regard is we don't know exactly how these devices work, and I think before deciding whether or not to regulate, that is an important factor that I think the committee has to take up the responsibility for learning.

Third, any legislation will require this committee or any other to draw arbitrary lines, but some arbitrary lines are better or worse than others. In my written statement, I've recommended several arbitrary lines that the committee, I think, should consider avoiding and several others that I think the committee should consider endorsing.

At the end of the day, however, in deciding whether to regulate any law enforcement practice, you have to ask yourself several questions. What are the benefits and harms of this practice? What is the likelihood of those benefits and harms coming to fruition? Who are the people that you're going to regulate? That is, do the police officers you're thinking about more closely resemble Joe Friday or Judge Dredd? Finally, what is the risk the public has to accept that you may be wrong in answering all of these questions?

Thank you for the opportunity to make a statement and prepare a written one. I'm glad to answer any questions you may have.

[Prepared statement of Mr. Larkin follows:]

HEARING: "GEOLOCATION TECHNOLOGY AND PRIVACY"
BEFORE THE HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
MARCH 2, 2016, RAYBURN HOUSE OFFICE BLDG. RM. 2154

WRITTEN SUBMISSION BY
PAUL J. LARKIN, JR.
SENIOR LEGAL RESEARCH FELLOW
THE HERITAGE FOUNDATION
214 MASSACHUSETTS AVE., NE
WASHINGTON, DC 20002-4999

HEARING: "GEOLOCATION TECHNOLOGY AND PRIVACY"
BEFORE THE HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
MARCH 2, 2016, RAYBURN HOUSE OFFICE BLDG. RM. 2154

WRITTEN SUBMISSION BY PAUL J. LARKIN, JR.
SENIOR LEGAL RESEARCH FELLOW, THE HERITAGE FOUNDATION

Mr. Chairman, Mr. Ranking Member, Members of the Committee:

My name is Paul J. Larkin, Jr. I currently am a Senior Legal Research Fellow at The Heritage Foundation. Most of my career has involved working in the criminal justice system in one capacity or another. For example, I worked at the Department of Justice in the Organized Crime and Racketeering Section of the Criminal Division and in the Office of the Solicitor General. I briefly was an Associate Independent Counsel under then-Independent Counsel Larry Thompson. I later was Counsel to the Senate Judiciary Committee when Senator Orrin Hatch was the Chairman. And I was a Special Agent-in-Charge with the Criminal Investigation Division of the Environmental Protection Agency. The views I express in this testimony are my own and should not be construed as representing any official position of The Heritage Foundation.

The questions of whether and, if so, how Congress should regulate the information-gathering abilities of new technologies presents important public policy issues.[1] The specific issue before the committee today—the use of geolocation technology to identify and track a person's whereabouts by locating his cell phone[2]—certainly is one of them.[3] There are more than 300 million cellphone subscribers in the United States,[4] and

---

[1] The literature on the relationship between new technologies (e.g., the Internet, modern tracking devices) and the Fourth Amendment, federal law, and privacy is large and continues to grow. *See, e.g.*, Jonathan Zittrain, *Searches and Seizures in a Networked World*, 119 HARV. L. REV. F. 83 (2006). Professor Orin Kerr, in particular, has been prolific scholar on the issues raised by the intersection of modern technology and the Fourth Amendment. *See, e.g.*, ORIN S. KERR, COMPUTER CRIME LAW (3d ed. 2012); Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285 (2015); Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403 (2013); Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 (2010); Orin S. Kerr, Ex Ante *Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241 (2010); Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700 (2010); Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503 (2007); Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279 (2005); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004); *see also* 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. 12085 (2004); Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607 (2003).

[2] For a discussion of the technology and mechanics involved, see United States v. Graham, 796 F.3d 332, 343 (4th Cir.), *reh'g en banc granted*, 624 Fed. Appx. 75 (2015); Stephanie Lockwood, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 308-10 (2004); Kevin McLaughlin, Note, *The Fourth Amendment and Cell Phone Location Tracking: Where are We?*, 29 HASTINGS COMM. & ENT. L.J. 421, 426-27 (2007).

[3] Various commentators have written on this subject. *See, e.g.*, Fabio Arcila, Jr., *GPS Tracking Out of Fourth Amendment Dead Ends:* United States v. Jones *and the* Katz *Conundrum*, 91 N.C. L. REV. 1 (2012);

law enforcement agencies submit massive number of requests for information to cell phone carriers each year.[5] The Baltimore Police Department alone has used a new, still largely secret technology to identify the location of cell phones 4,300 times since 2007.[6] It therefore is very important to law enforcement authorities and to the public at large whether and, if so, how the police may use the ability of cell phones to communicate their locations if the police need to locate the parties who own those phones.

For some time now, Congress has stepped in to regulate the government's use of information available through one new technology or another in order to balance law enforcement needs and privacy interests. Probably the two best-known examples are Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[7] which regulates the use of wiretapping to obtain the content of spoken communications, and the USA PATRIOT Act of 2001,[8] which revised numerous federal electronic surveillance laws in response to the 9/11 attacks to enhance the nation's abilities to share relevant information between our intelligence and federal law enforcement agencies. There are several other laws on

---

Evan Bernick, *Protecting Americans' Privacy: Why the Electronic Communications Privacy Act Should Be Amended*, THE HERITAGE FOUNDATION, LEGAL MEMORANDUM No. 118 (Feb. 28, 2014), http://thf_media.s3.amazonaws.com/2014/pdf/LM118.pdf; Patrick T. Chamberlain, *Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for a Probable Cause Standard*, 66 WASH. & LEE L. REV. 1745 (2009); William Curtiss, Note, *Triggering A Closer Review: Direct Acquisition of Cell Site Location Tracking Information and the Argument for Consistency Across Statutory Regimes*, 45 COLUM. J.L. & SOC. PROBS. 139 (2011); Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681 (2011); Renée McDonald Hutchins, *Tied Up in Knotts? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409 (2007); Megan L. McKeown, *Whose Line Is It Anyway? Probable Cause and Historical Cell Site Data*, 90 NOTRE DAME L. REV. 2039 (2015); Hon. Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1 (2013); Jeremy H. Rothstein, Note, *Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest*, 81 FORDHAM L. REV. 489 (2012); Eric J. Struening, *Checked in: Decreasing Fourth Amendment Protection Against Real-Time Geolocation Surveillance*, 45 U. MEM. L. REV. 561 (2015); Alexandra D. Vesalga, Comment, *Location, Location, Location: Updating the Electronic Communications Privacy Act to Protect Geolocational Data*, 43 GOLDEN GATE U. L. REV. 459 (2013); Jacob T. Whitt, Note, *Cell Phones as an Eye of the Government:* In re Application of the United States for Historical Cell Site Data, 88 TUL. L. REV. 831 (2014).

[4] 317.44 million as of 2014. http://www.statista.com/statistics/186122/number-of-mobile-cellular-subscriptions-in-the-united-states-since-2000/.

[5] *See* Stephanie K. Pell & Christopher Soghoian, *A Lot More Than A Pen Register, and Less Than A Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J. L. & TECH. 134, 152 (2014) ("wireless carriers receive tens of thousands of court orders requiring the disclosure of location data per year") (footnote omitted); *id.* 152 n.66 (citing a 2012 letter from Sprint stating that "[o]ver the past five years, Sprint has received . . . 196,434 court orders for location information.").

[6] Justin Fenton, *Baltimore Police used secret technology to track cellphones in thousands of cases*, BALTIMORE SUN (Apr. 9, 2015), http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-case-20150408-story.html.

[7] Pub. L. 90-351, 82 Stat. 197 (codified at various sections of Titles 18 and 42 (2012)).

[8] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Tit. II, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified at scattered sections of the U.S. Code).

those subjects as well.[9] Accordingly, there is nothing unusual in Congress deciding to become involved in the regulation of electronic information gathering technology by the government.

No particular bill is under discussion today, so I will address some general issues that would arise in connection with those issues and any potential federal legislation on those subjects. I would like to make three main points. First, current Supreme Court Fourth Amendment case law allows the government to acquire historical geolocational information without any showing of justification or need. It is possible that the Supreme Court could fundamentally change Fourth Amendment law, but it has not done so yet. Second, a new technology used by law enforcement permits a police officer to intercept outgoing cell phone's signals and thereby learn the phone's location without obtaining that information from a carrier. That technology, however, raises a serious Fourth Amendment issue because it operates only by capturing the signals from every cell phone in the device's operating radius, thereby effectively, albeit briefly, shutting off the ability of numerous cell phone users innocent of any crime to communicate with others. Third, any legislative solution would require Congress to draw arbitrary lines, but some arbitrary lines are worse than others. In that regard, I would like to offer some suggestions about lines that the committee should consider avoiding and drawing when deciding whether and how to regulate the government's acquisition and use of geolocational information.

I. THE FOURTH AMENDMENT AND THE GOVERNMENT'S ACQUISITION OF GEOLOCATIONAL INFORMATION FROM A TELECOMMUNICATIONS CARRIER

The Stored Communications Act provides that a judge "shall issue" an order directing a telecommunications carrier to release geolocational information to the government if it "offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought[ ] are relevant and material to an ongoing criminal investigation."[10] Federal, state, and local law enforcement officers often invoke that authority to obtain information necessary to identify, locate, and apprehend a suspected offender. It doubtless has proved invaluable in a considerable number of cases.

The Supreme Court has not squarely decided whether the Fourth Amendment requires law enforcement officers to obtain a search warrant, based on probable cause, to acquire historical geolocational information from a cell phone company. Three federal courts of appeals—the Third, Fifth, and Eleventh Circuits—have held that the government may obtain that information from a carrier without obtaining a warrant or establish-

---

[9] *See, e.g.*, Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (codified, as amended, at 47 U.S.C. §§ 1001-1010 (2012)); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified, as amended, at 18 U.S.C. § 2701 et seq. (2012)); Stored Communications Act (SCA), Pub. L. No. 99-508, 100 Stat. 1848 (codified, as amended, at 18 U.S.C. §§ 27201-2701 (2012); Video Privacy Protection Act of 1988, Pub. L. 100-618, § 2(a)(2), 102 Stat. 3195 (1988) (codified, as amended, at 18 U.S.C. § 2710 (2012)); Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified, as amended, at 50 U.S.C. ch. 36 (2012)); Privacy Act of 1974, Pub. L. 93-579, 88 Stat. 1896 (codified at 5 U.S.C. § 552a (2012)).

[10] 18 U.S.C. § 2703(d) (2012). The SCA was enacted as Title II of the Electronic Communications Privacy Act of 1986 (ECPA).

ing probable cause.[11] Settled Fourth Amendment law, known as the Third Party Doctrine,[12] strongly supports that conclusion. The rationale is that the government's acquisition of such information from a carrier does not infringe on the privacy of an individual because the sought-after information is contained in the carrier's business records, not in the subscriber's personal files. If the Supreme Court were to adhere to that longstanding doctrine, the Fourth Amendment would impose no requirement on the government's acquisition of historical geolocational information from a carrier because that conduct does not constitute a "search" for Fourth Amendment purposes.

Nonetheless, there is intellectual ferment regarding this aspect of Fourth Amendment law. Five Justices have signaled a willingness to reconsider at least some aspects of that settled doctrine. They could decide to endorse a different approach to questions like this one, an approach known as the Mosaic Theory.[13] That theory would treat the government's acquisition of this information as a "search" if it can help supply a larger, overall larger picture of a person's life, thereby forcing the government to establish probable cause before a neutral magistrate and obtain a search warrant (or establish an exception to the warrant requirement) to obtain geolocational information from a carrier.

It is impossible to know whether the Supreme Court will ultimately decide to fundamentally change Fourth Amendment law. Under current law, however, the government's practice does not violate that provision.

A. THE THIRD PARTY DOCTRINE

The Fourth Amendment bars the government from conducting an unreasonable "search" or "seizure."[14] Those are terms of description and limitation; government conduct that cannot be characterized as the one or the other is not subject to regulation under the Fourth Amendment.[15] A "search" requires the government to infringe upon some-

---

[11] *See* United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (en banc) (holding that the Fourth Amendment protects individuals from retrieval of cell phone location information); *In re* U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) (holding that orders to obtain historical cell site information for specified cell phones at the points where the user places and terminates a call are not categorically unconstitutional); *In re* U.S. for an Order Directing a Provider of Elec. Commc'ns Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010) (holding that the Stored Communications Act does not require the government to show probable cause to obtain a court order under 18 U.S.C. § 2703(d) for cell site information). Nonetheless, underneath the agreement among the federal circuits on the correct outcome of those cases is a fairly widespread disagreement as to the proper rule among the judges who considered those cases. The Fifth Circuit decided the *Davis* case by a 2-1 vote, and the en banc Eleventh Circuit split 8-3. In addition, a panel of the Fourth Circuit held that the government must obtain a search warrant to acquire geolocational records from a carrier, United States v. Graham, 796 F.3d 332, 343 (4th Cir. 2015), but the court of appeals granted rehearing en banc, United States v. Graham, 624 Fed. Appx. 75 (2015). Oral argument is tentatively scheduled for March 2016.

[12] *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009).

[13] *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).

[14] The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[15] *See, e.g.*, Maryland v. Macon, 472 U.S. 463, 468-69 (1985).

one's "reasonable expectation of privacy," while a "seizure" requires the government to materially interfere with a person's freedom of movement or his possessory interest in a "house, paper, or effect."[16] Viewing and recording the latitude and longitude coordinates collected by a cell tower is not a seizure of that information, because it deprives neither the subscriber nor his carrier of any freedom of movement or use of a cell phone,[17] so the only question is whether the acquisition and use of that information is a "search."

The Supreme Court has decided several cases involving the use of various types of modern-day electronic devices to obtain information, including a person's whereabouts.[18] None of those cases, however, dealt specifically with the acquisition from a cell phone carrier and later use of historical geolocational information. A few federal circuit courts of appeals have addressed this issue. While there is at present no conflict among the circuits on the legality of this issue, there has been considerable disagreement among the judges who have participated in the relevant cases. Nonetheless, the principles underlying closely analogous Supreme Court decisions permit the government to obtain that information without a search warrant or even a lesser showing of justification.

The principal decision in that regard is *Smith v. Maryland*.[19] In *Smith*, the telephone company, at the request of the police officers investigating a robbery and harassment of the victim by someone who claimed to have been the robber, installed a pen register device at its central office to capture the phone numbers called by Smith, who was the suspect in those crimes. Smith called the victim again, and, using information obtained from the phone company, the police obtained a search warrant for Smith's home, which turned up additional evidence of his crimes. He moved to exclude the evidence on the ground that the telephone company's installation of the pen register device at the behest of the police interfered with a reasonable expectation of privacy that Smith had in the content of his telecommunications. In an opinion by Justice Harry Blackmun, the Court rejected Smith's claim.

At the outset the Court noted that, because the pen register was installed on telephone company property at the company's central office, Smith could not claim "that his 'property' was invaded or that police intruded into a 'constitutionally protected area.'"[20] Moreover, because the pen register did not record the content of any of his conversations,

---

[16] *Id.* at 469.

[17] *See* Arizona v. Hicks, 480 U.S. 321, 324 (1987) ("[T]he mere recording of the serial numbers did not constitute a seizure. To be sure, that was the first step in a process by which respondent was eventually deprived of the stereo equipment. In and of itself, however, it did not "meaningfully interfere" with respondent's possessory interest in either the serial numbers or the equipment, and therefore did not amount to a seizure."); *Macon*, 472 U.S. at 468-69.

[18] *See, e.g.*, Riley v. California, 134 S. Ct. 2473 (2014) (search of a cell phone); United States v. Jones, 132 S. Ct. 945 (2012) (installation of a GPS tracking device on a person's car); Kyllo v. United States, 533 U.S. 27 (2001) (information obtained from a thermal imaging device); United States v. Karo, 468 U.S. 705 (1984) and United States v. Knotts, 460 U.S. 276 (1983) (installation of a beeper in a container of chemicals); Katz v. United States, 389 U.S. 347 (1967) (installation of a microphone on the outside of a phone booth).

[19] 442 U.S. 735 (1979).

[20] *Id.* at 741.

the Court reasoned, Smith's Fourth Amendment claim had to stand or fall on his argument that the installation and use of a pen register "constituted a 'search,'" which, in turn, necessarily rested on his submission that he had a legitimate expectation of privacy in the numbers he dialed on his phone.[21] The Court doubted that people actually have a legitimate expectation of privacy in the numbers they call, since people are aware that the phone company collects that information for billing purposes.[22] In any event, the Court added, a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties, like the phone company.[23]

In so ruling, the Court relied on its decision in *United States v. Miller*,[24] in which the Court had concluded that a bank depositor has no legitimate expectation of privacy in the financial information he voluntarily conveys to the bank.[25] As the Court had explained in *Miller* and reiterated in *Smith*, "[t]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[26]

Smith is but one example of the Third Party Doctrine. In several other cases, the Supreme Court has made it clear that a person has no legitimate expectation of privacy in information he voluntarily shares with third parties.[27] That is true even if the third party gives someone an assurance of confidentiality, the Court has noted, because we all must accept the risk of betrayal. "[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[28]

That principle traces its lineage to the longstanding practice of using police officers in an undercover capacity to identify offenders and collect evidence of their crimes. For decades the police have used undercover officers to infiltrate organized crime syndicates and ongoing drug trafficking operations, to perform activities that are likely to attract parties interested in selling or buying stolen articles, and in a variety of other ways. Undercover operations have proved to be a critical police practice for effective law enforcement in numerous cases that could not otherwise be adequately investigated.

---

[21] *Id.* at 742.

[22] *Id.* at 742-43.

[23] *Id.* at 743-44.

[24] 425 U.S. 435 (1976).

[25] *Id.* at 442-43.

[26] *Smith*, 442 U.S. at 744 (quoting *Miller*, 425 U.S. at 443).

[27] *See, e.g.*, *Miller*, 425 U.S., at 442–444; Couch v. United States, 409 U.S. 322, 335–336 (1973); United States v. White, 401 U.S. 745, 752 (1971) (plurality opinion); Hoffa v. United States, 385 U.S. 293 (1966); Lopez v. United States, 373 U.S. 427 (1963).

[28] *Smith*, 442 U.S. at 744 (internal punctuation omitted).

In the 1960s, the Warren Court upheld that practice even though it took advantage of the gullibility of some offenders and betrayed the confidence of the rest.[29] As the Supreme Court explained in 1966 in *Hoffa v. United States*,[30] "'The risk of being overheard by an eavesdropper or betrayed by an informer or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society. It is the kind of risk we necessarily assume whenever we speak.'"[31] Over the decades since its decision in the *Hoffa* case the Court has reconsidered and reaffirmed its Warren Court-era precedents.[32] It is firmly settled law that police undercover operations do not constitute a "search" or a "seizure." The Third Party Doctrines follows logically from the decisions approving that practice.

The result in *Smith* answers the question here. Each person voluntarily decides to carry a cell phone on his person—there is no law requiring anyone to carry a cell phone—and the average person knows that, given the technology that cell phones use to communicate, an active cell phone broadcasts its location to the nearest cell tower. Under those circumstances, the government does not commit a search whenever it acquires a person's historical locations from his cell phone carrier. The government's acquisition and use of geolocational information from a cell phone carrier is just another example of the Third Party Doctrine.

Nonetheless, there is an additional factor that complicates this problem. A new legal theory, the Mosaic Theory, could replace the Third Party Doctrine and establish new Fourth Amendment law by treating this practice, and perhaps many others, as a "search."

B. THE MOSAIC THEORY

The traditional Fourth Amendment analysis applied by the Supreme Court requires courts to examine a series of linked government actions on a step-by-step basis. The first step is to determine whether one action or another that led to the acquisition of evidence amounted to a search or seizure.[33] If none so qualify, the analysis is over, and the evidence may be admitted in the government's case-in-chief at trial. If one action (or more) does amount to a search or seizure, the next step is to ask whether that conduct is lawful—that is, whether the search or seizure was justified by probable cause or reasonable suspicion.[34] If it (or they) satisfied Fourth Amendment requirements, the analysis again is over, and the evidence may be admitted at trial. If one or more of those actions fails those requirements, the next step is to determine whether there is a causal connec-

---

[29] *See* Hoffa v. United States, 385 U.S. 293 (1966); Lopez v. United States, 373 U.S. 427 (1963).

[30] 385 U.S. 293 (1966).

[31] *Id.* at 465 (quoting Lopez v. United States, 373 U.S. 427, 450 (19063) (Brennan, J., dissenting)). As even Justice Brennan noted in his dissent in *Lopez*, "It is not an undue risk to ask persons to assume, for it does no more than compel them to use discretion in choosing their auditors, to make damaging disclosures only to persons whose character and motives may be trusted." 373 U.S. at 450 (1963) (Brennan, J., dissenting).

[32] *See* Illinois v. Perkins, 496 U.S. 292 (1990); United States v. White, 401 U.S. 745 (1971).

[33] *See, e.g.*, Maryland v. Macon, 472 U.S. 463 (1985).

[34] *See, e.g.*, Illinois v. Gates, 462 U.S. 213 (1983); Terry v. Ohio, 392 U.S. 1 (1968).

tion between them and the evidence. If there is no such connection[35] or (what is tantamount to the same conclusion) if the police would inevitably have discovered the evidence regardless of the illegality,[36] the analysis is over and the evidence may be admitted at trial. Finally, if there is a direct causal relationship, the question is whether a reasonable law enforcement officer would have known that his conduct violated the Fourth Amendment.[37] If not, the evidence is admissible. If, on the other hand, such an officer would have known that his conduct ran afoul of the Fourth Amendment—that is, if a police officer willfully violated the law—then the evidence must be suppressed. Courts must follow each step in that process before moving on to the next one. Moreover, the analysis does not permit a court to step back and evaluate the entire course of government conduct, as if it were a picture in a Rorschach Test, and decide whether the totality of the government's conduct was unlawful even though each step was justified.

Recently, however, several judges on the D.C. Circuit Court of Appeals, joined by perhaps five Justices of the Supreme Court, suggested that a different approach may be in order in the case of electronic surveillance. In *United States v. Jones*,[38] federal agents and local police officers, working together in a task force, placed a GPS tracking device on a suspect's car, monitored his movements for 28 days, and used that information to tie him to the drugs that were distributed by a group devoted to the sale of cocaine and crack. On appeal from his conviction, Jones argued that the installation of the GPS device violated the Fourth Amendment, requiring the exclusion of any data it reported. A panel of judges on D.C. Circuit agreed with Jones.[39]

Writing for the court, Judge Douglas Ginsburg concluded that settled Fourth Amendment law would allow the police to observe Jones as he drove on the open roads or city streets.[40] But Jones' case could not be decided so easily, Judge Ginsburg noted, because tracking Jones' car for 28 days was different in kind from watching his movements on any one particular day. As Judge Ginsburg put it, "no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life, nor the departure from a routine that, like the dog that did not bark in the Sherlock Holmes story, may reveal even more."[41] The judge then adverted to cases in which private parties demand the disclosure of information that the government seeks to withhold on national security grounds. In those cases, the court noted, the government often argues that a court, when deciding whether to disclose the sought-after information, must

---

[35] *See, e.g.*, Murray v. United States, 487 U.S. 533 (1988).

[36] *See, e.g.*, Nix v. Williams, 467 U.S. 431 (1984).

[37] *See, e.g.*, United States v. Leon, 468 U.S. 897 (1984).

[38] 132 S. Ct. 945 (2012).

[39] United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

[40] *See, e.g.*, United States v. Knotts, 460 U.S. 276, 281-82 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the defendant] traveled over the public streets, he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.").

[41] *Maynard*, 615 F.3d at 562.

consider the entire body of potentially relevant information, rather than one specific item taken out of context, because separate, individual pieces of information when combined could create a "mosaic" that enables someone to learn information damaging to the nation.[42] The same principle, the court concluded, should apply to searches like the one in Jones' case. "The whole of one's movements over the course of a month is not constructively exposed to the public because, like a rap sheet, that whole reveals far more than the individual movements it comprises."[43] The D.C. Circuit therefore set aside Jones' convicted and remanded his case to the district court.

The Supreme Court granted the government's certiorari petition and affirmed the D.C. Circuit's judgment, but on a narrower ground than the basis for the circuit court's ruling. All nine Justices believed that the government's conduct was unlawful, but only five Justices joined in the majority opinion written by the late Justice Antonin Scalia. The majority concluded that the government had committed a search by attaching the GPS device to Jones' vehicle and using at trial the evidence acquired by monitoring his whereabouts for the ensuing four weeks.[44] A vehicle is clearly an "effect" for purposes of the Fourth Amendment, the majority explained, and the attachment of the GPS device constituted a physical trespass on Jones' car.[45] Because the government had not preserved its argument that any search was justified,[46] the majority upheld the D.C. Circuit's judgment.

Five justices joined in one of two other opinions.[47] Justice Samuel Alito, joined by Justices Ruth Bader Ginsberg, Stephen Breyer, and Elena Kagan, wrote an opinion concurring in the judgment. Justice Alito found the common-law approach used by the majority to be an artificial way to examine a problem that could only have arisen in the twenty-first century. In his words, "Is it possible to imagine a case in which a constable secreted himself somewhere in a coach and remained there for a period of time in order to monitor the movements of the coach's owner?"[48] Rather, he would have asked whether the long-term monitoring of the movements of his vehicle violated Jones' reasonable ex-

---

[42] *Id.* at 562.

[43] *Id.* at 561-6 "Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels 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 political groups—and not just one such fact about a person, but all such facts." *Id.* at 562.

[44] United States v. Jones, 132 S. Ct. 945 (2012).

[45] *Id.* at 949-51.

[46] *Id.* at 954.

[47] Although five Justices joined the two separate opinions, they did not all join in one opinion and therefore did not establish a majority opinion for the Court. The opinion by Justice Scalia constituted the majority opinion.

[48] *Id.* at 958 (Alito, J., concurring in the judgment).

pectations of privacy,[49] the same methodology that the Court had consistently followed since its 1969 decision in *Katz v. United States*,[50] a case involving wiretapping. Aside from being inconsistent with *Katz*, the majority's analysis, according to Justice Alito, was flawed in a variety of ways.[51] He believed that the majority came to the correct result, just for the wrong reasons.

Justice Sonia Sotomayor, who joined the majority opinion, also wrote a separate concurring opinion. In that opinion, Justice Sotomayor agreed with the majority's conclusion that the case should be decided on the narrow ground that the government had committed a trespass,[52] but also expressed sympathy for Justice Alito's conclusion that a physical trespass is an unnecessary predicate in the case of electronic surveillance.[53] She added, however, that perhaps it was time to reconsider the Third Party Doctrine, in its entirety or at least in the case of electronic surveillance, because the doctrine no longer represents a reasonable way to look at information storage in the digital age.[54]

---

[49] *Id.* at 958 (Alito, J., concurring in the judgment).

[50] 389 U.S. 347 (1967).

[51] *Id.* at 961-62 (Alito, J., concurring in the judgment) (citations omitted; emphasis in original):

> First, the Court's reasoning largely disregards what is really important (the *use* of a GPS for the purpose of 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). Attaching such an object is generally regarded as so trivial that it does not provide a basis for recovery under modern tort law. . . .But under the Court's reasoning, this conduct may violate the Fourth Amendment. By contrast, if long-term monitoring can be accomplished without committing a technical trespass—suppose, for example, that the Federal Government required or persuaded auto manufacturers to include a GPS tracking device in every car—the Court's theory would provide no protection.
>
> Second, the Court's approach leads to incongruous results. If the police attach a GPS device to a car and use the device to follow the car for even a brief time, under the Court's theory, the Fourth Amendment applies. But if the police follow the same car for a much longer period using unmarked cars and aerial assistance, this tracking is not subject to any Fourth Amendment constraints.
>
> . . . . .
>
> Third, under the Court's theory, the coverage of the Fourth Amendment may vary from State to State. If the events at issue here had occurred in a community property State or a State that has adopted the Uniform Marital Property Act, respondent would likely be an owner of the vehicle, and it would not matter whether the GPS was installed before or after his wife turned over the keys. In non-community-property States, on the other hand, the registration of the vehicle in the name of respondent's wife would generally be regarded as presumptive evidence that she was the sole owner. . . .
>
> Fourth, the Court's reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked.

[52] *Id.* at 954-55 (Sotomayor, J., concurring).

[53] *Id.* at 955-56 (Sotomayor, J., concurring).

[54] "More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.. . . This approach is ill suited to

C. COMPARING THE TWO DOCTRINES

Pointing to the views of the five Justices who joined the opinions of Justices Alito and Sotomayor in *Jones*, various commentators have predicted that the Supreme Court will eventually adopt the Mosaic Theory to analyze electronic information gathering and surveillance. Although that outcome is possible, it would signal a material change in the Supreme Court's longstanding Fourth Amendment analysis. It would also have several adverse consequences.[55]

One such consequence is the elimination or crippling of the Third Party Doctrine. The Mosaic Theory leaves open numerous questions that the courts would need to grapple with over a lengthy period.[56] Answering those questions, moreover, would force the courts to undertake an arbitrary line-drawing exercise as they attempt to decide which observations are too long, too intrusive, or too fruitful.[57] The courts also would need to decide whether there are other relevant factors, such as the crime under investigation. (Are longer periods justified for drug trafficking than murder investigations because the former endure for longer period, or are longer periods justified for murder cases because murder is a more serious crime? What about traffickers suspected of having committed murder?) If so, surveillance law could vary from one law enforcement department to another given their different missions (Is halting the shipment of drugs more important than halting the shipment of stolen firearms?) and the different resources they can bring to bear (Can a five-person sheriff's department conduct a longer period of technology-

---

the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice ALITO notes, some people may find the tradeoff of privacy for convenience "worthwhile," or come to accept this diminution of privacy as inevitable, . . . and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." *Id.* at 957 (Sotomayor, J., concurring) (citations and internal punctuation omitted).

[55] *See* Kerr, 107 Mich. L. Rev. at 566-600.

[56] "Although the mosaic theory derives from an admirable goal, I believe it is a troubling approach that courts should reject. The mosaic theory should be repudiated for three reasons. First, the theory raises so many novel and puzzling new questions that it would be difficult, if not impossible, to administer effectively as technology changes. Second, the mosaic theory rests on a probabilistic conception of the reasonable expectation of privacy test that is ill suited to regulate the new technologies that the mosaic theory has been created to address. And third, the theory interferes with statutory protections that better regulate surveillance practices outside of the sequential approach." *Id.* at 346.

[57] Consider, for example, the difficulty of knowing exactly how to characterize observations of a suspect. "Modern technological tools such as GPS devices can be programmed to record at any interval. The ability to program surveillance tools greatly complicates legal standards based on time. To appreciate this, imagine the police use a GPS device that is programmed to turn on and record the location of the car for only one hour a day. The device is otherwise dormant. If the police monitor that device over twenty-eight days, does that count as twenty-eight days of monitoring? Or is that only twenty-eight hours of monitoring?" *Id.* at 333. For other difficulties posed by the Mosaic Theory, see *id.* at 328-53.

reliant surveillance than the FBI, because the latter has more than 14,000 special agents it can draw on?).

The continuous development of new technologies also would force the courts to be willing to upset settled expectations and stare decisis considerations by reconsidering their decisions every few years or so as new devices (iPhones) replace older ones (pagers). That outcome would unsettle Fourth Amendment and police practices on a regular basis.

Worsening the problem of ongoing disruption in the law is the delay between the advent of a new device and a court ruling on its legality. Years could pass.[58] If technology has moved on, the decision becomes of only historical interest, with no ongoing practical significance for privacy-protection purposes, but leaving in its wake a potentially large number of convictions that must be set aside.

The current, discrete step-by-step approach to Fourth Amendment analysis is not perfect—What human invention is?—but it does not morph into an entirely new approach with every new product put out by Microsoft, Google, or any other firm in the high-tech industries. There is something to be said for the proposition that the devil you know is better than the devil you don't.

Those results would occasion a fundamental change in the approach to Fourth Amendment doctrine in another way. For the last half-century, the Supreme Court has sought to craft easily understandable rules for law enforcement to follow, in the belief that a rule-oriented body of law would be clearer and easier for police officers to understand than one that asked simply whether their conduct was reasonable. Of course, a "rule of reason" does have something to say for itself. It would be consistent with the text of the Fourth Amendment—which demands that searches and seizures be "reasonable"—and it would be follow along with the Supreme Court's oft-stated proposition that "reasonableness" is the governing principle in all Fourth Amendment inquiries.[59] A general reasonableness approach would also avoid the need to draw new lines as advanced information-gathering technologies come on stream.

But it would accomplish those results at a loss of considerable clarity in Fourth Amendment doctrine as courts grapple with the task of deciding what is "reasonable." Under that approach, the identical law enforcement conduct could be reasonable or unreasonable depending on the facts and circumstances of each case, such as the crime involved and the risk to public safety if it goes unsolved.[60] Different lowers courts could

---

[58] For example, the FBI placed the GPS tracker on Jones' car in 2005, but the Supreme Court did not decide that the placement was a search until 2012. *Jones*, 132 S. Ct. at 945, 948.

[59] *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2482 (2014) ("As the text makes clear, "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'") (citation omitted).

[60] *See, e.g.*, Brinegar v. United States, 338 U.S. 160, 183 (1949) (Jackson, J., dissenting) ("If we assume, for example, that a child is kidnapped and the officers throw a roadblock about the neighborhood and search every outgoing car, it would be a drastic and undiscriminating use of the search. The officers might be unable to show probable cause for searching any particular car. However, I should candidly strive hard to sustain such an action, executed fairly and in good faith, because it might be reasonable to subject travelers to that indignity if it was the only way to save a threatened life and detect a vicious crime. But I should

find identical conduct to be reasonable or not based on their individual judgments about the importance of particular crimes (Should kidnapping be treated the same as murder? Should drug trafficking be treated the same as murder if the suspects are senior members of a drug cartel known for violence?) or the difficulty that particular law enforcement officers will have in investigating them (Should there be one rule for the NYPD, which has more than thirty thousand police officers, and a different rule police department with far fewer officers?) The absence of clear rules defining "searches" and "seizures", as well as the different justifications for each one, does not assist law enforcement perform its job or guarantee individuals that the government will respect their privacy interests.

Finally, unraveling the Third Party Doctrine puts at risk law enforcement undercover operations, practices that the Supreme Court has upheld for more than 50 years. The rationale given in cases such as *Hoffa v. United States*,[61] *United States v. White*,[62] and *Illinois v. Perkins*[63] that were decided by the Warren, Burger, and Rehnquist Courts why undercover practices do not constitute a search, a seizure, or a coercive environment is that we assume the risk that information we share with others is no longer secret and may not remain private. Each person can choose to whom he discloses details of his life or business. In so doing, however, given the fact that people are not always trustworthy, we each take the risk of further disclosure, whether done accidentally or due to a betrayal. The Fourth Amendment does not protect us against the negligence or dishonesty of others; that is our burden.

The Mosaic Theory would undercut that principle by creating an exception for instances in which we disclose digital information, rather than physical records or spoken words, to telecommunications carriers, under the theory that we "need" cell phones despite their location-identifying features. Perhaps, the Supreme Court would draw a line distinguishing police undercover operations from their use of cell phone technology, but that line would be an arbitrary one, because the principles underlying the Court's approval of undercover operations logically gave rise to the Third Party Doctrine that the Mosaic Theory would erase.

Those issues, however, are ones that the Supreme Court may take up in a future case. At present, cases like *Smith* are still good law.

II. THE FOURTH AMENDMENT AND THE GOVERNMENT'S DIRECT INTERCEPTION OF GEOLOCATIONAL INFORMATION

A recent technological development may have changed the Fourth Amendment calculus, regardless of whether the Supreme Court adopts the Mosaic Theory. Technology now enables law enforcement officers to obviate the need to obtain geolocational information from a carrier for a particular individual. Instead, the government may purchase a commercially available device known as a "cell site simulator" that, by posing as

---

not strain to sustain such a roadblock and universal search to salvage a few bottles of bourbon and catch a bootlegger.").

[61] 385 U.S. 293 (1966).

[62] 401 U.S. 745 (1971).

[63] 496 U.S. 292 (1990).

a true cell tower, intercepts cell phone transmissions before they reach the carrier's own tower.[64] The simulator works as follows: When turned on, a cell phone sends a signal to the nearest cell tower in case there is an outgoing or incoming communication. As a person moves from one cell tower area to another the phone disconnects from the original tower and connects to the closest one available, changing as a person moves. These devices work by capturing the communications emitted by a cell phone en route to a telecommunications carrier before they can reach the closest available real tower. In essence, these devices pose as a carrier's cell tower and trick a cell phone into sending it the same geolocational information that the phone would transmit to one of the carrier's own towers.

The Supreme Court and the federal circuit courts have not yet addressed the government's acquisition of geolocation information via a cell tower simulator. In fact, few courts have analyzed the issue at all, in part due to the federal government's efforts to keep the existence of such a device secret.[65] Cases are now pending before different lower appellate courts challenging the use of such devices on the ground that, by precisely identifying a person's location, they enable law enforcement authorities to conduct a search without a warrant or probable cause.[66] None of those cases has yet been decided, and their outcome is uncertain.

There are several material differences between the government's acquisition of information by using a cell tower simulator and by obtaining information from a telecommunications carrier. First, a simulator enables the government to obtain real-time information indicating where a cell phone owner *is*, rather than historical information where

---

[64] *See, e.g.*, U.S. Dep't of Justice, Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology (2015), http://www.justice.gov/opa/file/767321/download; William Curtis, *Triggering a Closer Review: Direct Acquisition of Cell Site Location Tracking Information and the Argument for Consistency Across Statutory Regimes*, 45 COLUM. J. L. & SOC. PROBS. 139 (2011); Stephen E. Henderson, *Real-Time and Historic Location Surveillance After United States v. Jones: An Administrable, Mildly Mosaic Approach*, 103 J. CRIM. L. & CRIMINOLOGY 803 (2013); Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 1 (2014); Pell & Soghoian, 16 YALE J. L. & TECH. at 145-47; Spenser S. Hsu, *Constitutionality of StingRay use by D.C. police is challenged*, WASH. POST (Feb. 23, 2016), https://www.washingtonpost.com/local/public-safety/constitutionality-of-stingray-use-by-dc-police-is-challenged/2016/02/23/d197cb52-d9b2-11e5-81ae-7491b9b9e7df_story.html; Andrea Noble, *D.C. police use of secret cellphone tracking technology challenged in sex assault case*, WASH. TIMES (Feb. 23, 2016), http://www.washingtontimes.com/news/2016/feb/23/dc-police-use-of-secret-cellphone-tracking-technol/print/. These devices go by the names StingRay, Triggerfish, Kingfish, and Hailstorm. The devices can be installed in a vehicle, added to a drone, or carried by hand. *See* Pell & Soghoian, 16 YALE J. L. & TECH. at 145-47.

[65] *See* Fenton, *supra* note 6.

[66] *See* Jones v. United States, No. 15-CF-322 (D.C. Ct. App.); Maryland v. Andrews, Sept. Term 2015, No. 1496 (Md. Ct. Spec. App.); *see also In re* Application by the United States for an Order Relating to Telephones Used by [Suppressed] (N.D. Ill. Nov. 9, 2015) (setting conditions non the issuance of a search warrant for such a device); *see also In re* Application by the United States for an Order Relating to Telephones Used by [Suppressed] (N.D. Ill. Nov. 9, 2015) (Magistrate Judge Ian Johnston) (imposing conditions on the used of information acquired by use of cell tower simulators). The Wisconsin Supreme Court in *State v. Tate*, 849 N.W.2d 798 (2015), assumed that use of such a device was a search and found it reasonable because it was supported by probable cause and a warrant.

he *was*. That information can be extremely valuable in the case of a crime, like kidnapping, that remains in progress as long as the victim is alive and prevented from leaving the offender's custody. Second, a simulator captures a cell phone's outgoing signals that are necessary for it to make or receive calls. In the process, the simulator briefly but effectively disables or "quiets" the phone for the duration of time that it remains within the operating radius of the device.[67] Acquiring historical cell phone data from a carrier does not have that effect. Third, a simulator does not disable only the cell phone of the particular suspect within its reach; it disables *every* phone within that perimeter, even the phones possessed and used by parties who are entirely innocent of any crime. The number of parties who suffer a loss of cell phone use when a simulator is used in a rural area could be small, but that is not the case when a simulator is used in a densely populated urban area, such as the borough of Manhattan in New York City. Fourth, a simulator enables the government to avoid presenting any justification for its use to a neutral magistrate because no federal law regulates its use. The Department of Justice has issued a policy statement seeking to regulate the use of simulators by federal law enforcement officers and any allied state or local officers working as part of a task force or team. But the bulk of state and local officers are under no federal legal obligation to comply with the Justice Department's policy when they use such a device to investigate state crimes.

Given those differences, this question arises: Is it reasonable to treat the government's interception of telecommunications data by using a cell tower simulator in the same manner as its acquisition of this information from a telecommunications carrier pursuant to a court order. A strong argument can be made that the former is a more intrusive practice and should be subject to at least some degree of regulation.

To start with, it is important to recognize that the Third Party Doctrine has no bearing on the proper answer to that question. That doctrine rests on the proposition that the sought-after records belong to the *carrier*, *not* the *subscriber*, even though they contain information about or provided by the subscriber to the carrier. By intercepting a signal before it reaches the intended carrier, the company never acquires the data and never compiles it into its own business records. Accordingly, cases like the Supreme Court's decision in *Smith* are beside the point.

Moreover, regardless of the effect that a simulator has on a *subscriber's* desire to remain secluded,[68] whenever a simulator disables *all* cell phones within its working radius, the government has interfered with the liberty and property interests of people who are not the suspect of any crime. A cell phone is an "effect" protected by the Fourth

---

[67] It is unclear how long a disruption can last, what is the average length of a disruption, or, on average, how many cell phones are disrupted.

[68] That effect will differ depending on whether the simulator discloses only that someone is in a public area (*e.g.*, a highway) rather than in a protected area (*e.g.*, a home). Disclosure of the fact that someone is on a public highway, for example, is not a Fourth Amendment search, *see* United States v. Karo, 468 U.S. 705 (1984), but the electronically-aided disclosure where a person can be found in his home is a search, *see* United States v. Knotts, 460 U.S. 276 (1983). The relevant question is not, as some have argued, whether a simulator provides a more precise location of a cell owner than past cell tower records; it may. The pertinent question is whether that more precise location is within a protected area like a home, or an unprotected location, like a highway.

Amendment,[69] and the government's use of a device that disables a cell phone from being used to communicate is tantamount to the "seizure" of that phone for as long as the device is in operation.[70] In densely populated urban areas, the number of affected cell phones could be quite large. Even a temporary seizure of someone's cell phone must be justified by reasonable suspicion that a crime is afoot[71] or a comparable legitimate justification for the need to briefly separate a person from his property.[72]

III. A LEGISLATIVE SOLUTION MAY REQUIRE CONGRESS TO DRAW ARBITRARY LINES, BUT SOME ARBITRARY LINES ARE WORSE THAN OTHERS

A. IS NEW LEGISLATION NECESSARY?

Arguments can be made on both sides of the question whether Congress should consider additional legislation on these subjects. Some may argue in favor of waiting for the courts to gain additional familiarity with these practices before attempting to adopt a new set of rules by legislation. The courts have proved quite capable of resolving these issues based only on existing legislation and the Fourth Amendment so there is no need to bring their efforts to a halt through new acts of Congress. New legislation would only disrupt the common law-like decisionmaking process, the argument would conclude, that we have traditionally accepted as the best approach to resolve contested law enforcement police practices.

By contrast, the argument in favor of taking up these subjects now would go as follows: The Supreme Court has been willing to grant Congress considerable deference in legislating on topics like this one. For example, after the Court struck down the then-existing New York state wiretapping law in *Berger v. New York*,[73] some people feared that the Court would prohibit wiretapping altogether. Congress revised then-pending federal wiretap legislation in light of the *Berger* decision, and the Supreme Court has never found that law to be unconstitutional.[74] Moreover, the Court has recently made known its belief that legislatures can do a better job than courts when it comes to regulating the permissible use of new technologies for evidence-gathering purposes.[75] In fact,

---

[69] *See* Riley v. California, 134 S. Ct. 2473 (2014) (ruling that the Fourth Amendment regulates the government's search of a cell phone's contents).

[70] *See, e.g.*, Illinois v. McArthur, 531 U.S. 326 (2001) (barring a homeowner from entering his house while the police execute a search warrant is a "seizure"); United States v. Place, 462 U.S. 696 (1983) (ruling that the temporary seizure of a person's luggage for inspection must be justified by reasonable suspicion); United States v. Van Leeuwen, 397 U.S. 249 (1970) (treating the detention of a mailed package as a seizure, but finding it reasonable in that case).

[71] *See, e.g.*, Terry v. Ohio, 392 U.S. 1 (1968) (ruling that the temporary detention of a person for questioning must be justified by reasonable suspicion).

[72] *See, e.g.*, *McArthur*, 531 U.S. at 311-33 (concluding that the temporary exclusion of a person from his home must be justified); *supra* note 70.

[73] 388 U.S. 41 (1967).

[74] *See, e.g.*, Dalia v. United States, 441 U.S. 238 (1979); Scott v. United States, 436 U.S. 128 (1978); United States v. Donovan, 429 U.S. 413 (1977).

[75] *See* City of Ontario, Cal. v. Quon, 560 U.S. 746, 759 (2010) ("The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amend-

the Court has pleaded with Congress to "let this cup pass away" from them[76] by taking up the issue itself.[77] That factor would counsel in favor of readdressing the existing legislation governing geolocational information acquisition and use now, particularly in light of the use of the new simulation technologies.

Legislatures are better than courts at line-drawing, especially when there is no alternative to using an arbitrary line to define, for example, the time period within which law enforcement officers may pursue a certain practice without first obtaining judicial approval. For example, the police may detain a suspect for questioning if they have a reasonable suspicion that he has been or may be involved in criminal activity, a brief detention known in the argot of law enforcement as a *Terry* stop.[78] A *Terry* stop "must be temporary and last no longer than is necessary to effectuate the purpose of the stop,"[79] but there is no fixed time period under the Fourth Amendment past which law enforcement may detain someone. "Much as a bright line rule would be desirable, in evaluating whether an investigative detention is unreasonable," the Court has explained, "common sense and ordinary human experience must govern over rigid criteria."[80] Congress, however, could define a specific time limit—say, 30 minutes—on the lawfulness of a *Terry* stop (although few might find that to be a good idea). Just as Congress could define a bright-line rule limiting the length of *Terry* stops for federal law enforcement officers, Congress could fix a limit on the length of time that federal law enforcement officers may gather historical or real-time geolocational information from a telecommunications carrier or by using a simulator without obtaining judicial approval.

Law enforcement use of a cell phone simulator involves a more pressing issue than the acquisition of historical cell location data from a carrier. Federal law does not

---

ment implications of emerging technology before its role in society has become clear. . . . In *Katz* [v. United States, 389 U.S. 347, 353 (1967)], the Court relied on its own knowledge and experience to conclude that there is a reasonable expectation of privacy in a telephone booth. . . . It is not so clear that courts at present are on so sure a ground. Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices.").

[76] *Matthew* 26:39.

[77] *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment) ("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.").

[78] *See, e.g.*, Terry v. Ohio, 392 U.S. 1 (1969).

[79] United States v. Sharpe, 470 U.S. 675, 684 (1985) (citation omitted).

[80] *Id.* at 685; *see also, e.g., id.* at 685 ("Obviously, if an investigative stop continues indefinitely, at some point it can no longer be justified as an investigative stop. But our cases impose no rigid time limitation on *Terry* stops. While it is clear that the brevity of the invasion of the individual's Fourth Amendment interests is an important factor in determining whether the seizure is so minimally intrusive as to be justifiable on reasonable suspicion, . . . we have emphasized the need to consider the law enforcement purposes to be served by the stop as well as the time reasonably needed to effectuate those purposes. . . . . We understand the desirability of providing law enforcement authorities with a clear rule to guide their conduct. Nevertheless, we question the wisdom of a rigid time limitation. Such a limit would undermine the equally important need to allow authorities to graduate their responses to the demands of any particular situation.") (citations and internal punctuation omitted).

expressly regulate that practice, and the Justice Department's policy does not govern the independent actions of state and local police officers. Supreme Court law indicates that the intentional disruption of cell phone use by entirely innocent parties must be justified by, at least, reasonable suspicion.[81]

B. WHAT SHOULD NEW LEGISLATION LOOK LIKE?

There are several different ways that Congress could regulate the acquisition and use of geolocational information from carriers via court orders or by using cell tower simulators. As a practical matter, it is impossible to do so without drawing arbitrary lines. Some arbitrary lines, however, are worse than others. The reason is that some lines might appear to be sensible, but on closer analysis turn out to be unreasonable.

1. UNREASONABLE ARBITRARY LINES

There are several potential regulatory approaches that would involve drawing arbitrary lines that are unreasonable. Congress should avoid pursuing those approaches.

Limiting Unrestricted Geolocational Information-Gathering Ability to Identified Law Enforcement Agencies: One possibility would be to limit the authority to obtain geolocational information or use simulators without any prior showing of need or justification to only certain particular domestic law enforcement agencies, such as the Federal Bureau of Investigation (FBI or Bureau) or the U.S. Secret Service. The argument would be that those agencies have a greater need to immediate access to geolocational information than any other law enforcement agency may have. The FBI is responsible not only for domestic federal law enforcement crimes such as kidnapping, but also for counterterrorism and counterespionage efforts, while the Secret Service is responsible for protecting the lives of the President and Vice-President, all of which are matters as to which time may be of the essence. This approach would give those two agencies the ability to have unlimited acquisition and use of geolocational information, while requiring every other agency to obtain a search warrant. The effect would be to wall off the Bureau and Secret Service from all other police agencies.

That approach, however, is not likely to work as planned. In the first place, no such wall is likely to stand forever. It would not be long before other federal law enforcement agencies—the Drug Enforcement Administration readily comes to mind—seek to be added to that category on the ground that, for example, narcotrafficking is as great a threat to the national security as the crimes investigated by the FBI and Secret Service. Having made one hole in the wall, Congress would be under pressure to make others, for agencies like U.S. Marshal's Service or the Bureau of Alcohol, Tobacco, Firearms, and Explosives, on the ground that they too deal with violent criminals. State and local police departments would also maintain that they pursue violent criminals as well, more, in fact, than the federal government does. Congress may not have the authority to generally make rape a federal crime,[82] but the states certainly do, and every one of them has done so. The states will argue that, considering the number of violent crimes that they must

---

[81] *See supra* note 70 (collecting cases).

[82] *See, e.g.*, United States v. Morrison, 529 U.S. 598 (2000).

investigate, they have a far greater need for unlimited access to geolocational information than federal law enforcement officers generally have.

An additional problem is that the Bureau and Secret Service work with other federal, state, and local law enforcement partners in formal task forces or on an informal basis. That raises the problem of deciding what geolocational information FBI and Secret Service agents can share with their law enforcement colleagues. In order for a task force or informal group of officers to work together effectively, each partner must be able to share information with others. It would make little sense to decide that FBI agents should have unlimited access to geolocational data when investigating a kidnapping, but the local police detectives working side-by-side with them should not.

Atop that, any effort to distinguish among state and local law enforcement agencies regarding immediate access to geolocational information—say, authorizing only the New York City Police Department and a few other similar departments to have the same access as the FBI and Secret Service—is likely doomed to fail. Kidnappings in Mayberry, North Carolina, are no less important than kidnappings in the borough of Queens, New York. Denying the detectives investigating a kidnapping in a small jurisdiction access to the same information under the same conditions available to their counterparts in a major metropolitan area does little to enhance privacy, but could do a great deal to impede an investigation. That would be particularly true if the two jurisdictions are working together on the same case.

The final reason why this approach would not work is realpolitik. Few Members of Congress outside of New York would be willing to say to their state and local police agencies (let alone to their constituents) that they are not as good or as trustworthy as the NYPD. The result is that, over time, Congress is very likely to add additional federal, state, and local law enforcement departments to the category of favored agencies, thereby undoing any effort to regulate the acquisition of geolocational information by limiting its automatic availability to a limited number of federal agencies with a unique and compelling need for it.

Limiting Unrestricted Geolocational Information-Gathering Ability to Identified Offenses: Another option is to limit the acquisition and use of this information to the investigation of certain identified crimes. For example, Congress could limit acquisition and use of geolocational information to violent crimes or terrorism offenses. Unfortunately, that approach likely would run aground due to several legal and practical problems with its implementation.

To start with, there is no federal crime of "terrorism" per se. Acts of terrorism can be prosecuted as murder, kidnapping, mayhem, assault, and so forth, but there is no general federal crime of murder, kidnapping, mayhem, or assault. The federal government can prosecute murder only if it occurs on federal property (*e.g.*, the Pentagon) or the victim is someone expressly identified in federal law (*e.g.*, a Member of Congress). Otherwise, murder is a state crime, punishable under a state's general "police power," a power that the federal government lacks.[83]

---

[83] *See, e.g.*, United States v. Morrison, 529 U.S. 598 (2000); United States v. Lopez, 514 U.S. 549 (1995).

Congress could attempt to limit use of a simulator to investigations involving a "crime of violence." But that limitation is also likely to come a cropper. In 2015, the Supreme Court concluded that the term "violent felony," a term defined by federal law to include any felony that "involves conduct that presents a serious potential risk of physical injury to another,"[84] was unconstitutionally vague.[85] Approaching this problem in that manner therefore may not move the ball downfield very far. Moreover, attempted violent crimes and conspiracies to commit violent crimes are not *themselves* violent crimes, but law enforcement officers may need cell location information in order to prevent such crimes from occurring. It makes little sense to force police officers to await the commission of a substantive crime of violence before they can obtain information that would have enabled them to stop an offender in his tracks.

Finally, no limitation is likely to remain exclusive for long. Consider the history of Congress's repeated additions to the offenses for which the government may use wiretapping as an investigative technique. What started out as a small list now approaches virtually every federal crime defined by the U.S. Code. The same outcome would occur here. Whenever the media splash a crime across the headlines or on TV, some Member of Congress will seek to add it to that list, and no Member of Congress is likely to be willing to incur the wrath of a colleague or the voting public by opposing an effort to enlarge it. It makes little sense to assume the contrary.

2. Reasonable Arbitrary Lines

There are at least three reasonable (albeit arbitrary) lines that Congress could draw. First, a statute could authorize federal, state, and local law enforcement authorities to obtain geolocational information whenever (a) they have a reasonable suspicion that a crime has occurred, is in progress, or is in the offing; (b) they have a reasonable belief that the information may be necessary for a legitimate intelligence or national security reason that may not be connected to the commission of a crime; or (c) they have a reasonable belief that the information is necessary for a legitimate non-law enforcement purpose, such as the need to find a lost child or to find someone who may be in distress on medical grounds or otherwise.[86] Second, a statute could impose a domestic search warrant requirement if, after a reasonable period of time has elapsed—say, three, seven, or ten days—the government still has a legitimate need for geolocational information for one of the above reasons. Third, a statute could permit the government to maintain, and to share with other law enforcement or intelligence agencies, whatever geolocational information it acquires but only in connection with the particular suspect(s) at issue. Information relating to other parties should be quickly destroyed.

---

[84] 18 U.S.C. § 924(e)(1) and (e)(2)(B) (2012).

[85] *See* Johnson v. United States, 135 S. Ct. 2551 (2015).

[86] Law enforcement officers may intervene to protect public safety even when no potential crime may be involved. *See, e.g.*, Brigham City, Utah v. Stuart, 547 U.S. 398, 403 (2006) ("[L]aw enforcement officers may enter a home without a warrant to render emergency assistance to an injured occupant or to protect an occupant from imminent injury. . . . The role of a peace officer includes preventing violence and restoring order, not simply rendering first aid to casualties; an officer is not like a boxing (or hockey) referee, poised to stop a bout only if it becomes too one-sided.").

Those lines would balance law enforcement or intelligence needs against the public's reasonable expectations of privacy. A reasonable suspicion requirement would not burden law enforcement. The reasonable suspicion requirement first adopted in *Terry v. Ohio*[87] enables a police officer to draw on his training, experience, and common sense, applied to the totality of the circumstances, when deciding whether criminal activity is afoot.[88] The individual factors that comprise reasonable suspicion may each be entirely innocent when considered by themselves, but when considered together establish a reasonable belief that a crime was, is being, or may be committed.[89] Reasonable suspicion requires more than a "hunch" that someone is involved in crime, but it demands only "some minimal level of objective justification,"[90] an amount of evidence that is far less proof than what would be necessary to satisfy a probable cause requirement.[91]

---

[87] 392 U.S. 1 (1968).

[88] *See, e.g.*, United States v. Arvizu, 534 U.S. 266, 277 (2002) (the totality-of-the-circumstances approach "allows officers to draw on their own experience and specialized training to make inferences from and deductions about the cumulative information available to them that might well elude an untrained person") (citations and internal punctuation omitted); United States v. Cortez, 449 U.S. 411, 417-18 (1981) ("[T]he essence of all that has been written is that the totality of the circumstances—the whole picture—must be taken into account. Based upon that whole picture the detaining officers must have a particularized and objective basis for suspecting the particular person stopped of criminal activity. . . . The idea that an assessment of the whole picture must yield a particularized suspicion contains two elements, each of which must be present before a stop is permissible. First, the assessment must be based upon all the circumstances. The analysis proceeds with various objective observations, information from police reports, if such are available, and consideration of the modes or patterns of operation of certain kinds of lawbreakers. From these data, a trained officer draws inferences and makes deductions—inferences and deductions that might well elude an untrained person. . . . [T]he evidence thus collected must be seen and weighed not in terms of library analysis by scholars, but as understood by those versed in the field of law enforcement. The second element contained in the idea that an assessment of the whole picture must yield a particularized suspicion is the concept that the process just described must raise a suspicion that the particular individual being stopped is engaged in wrongdoing.") (citations omitted).

[89] *See, e.g., Arvizu*, 534 U.S. at 277 ("A determination that reasonable suspicion exists, however, need not rule out the possibility of innocent conduct."); United States v. Sokolow, 490 U.S. 1, 9-10 (1989) ("Any one of these factors is not by itself proof of any illegal conduct and is quite consistent with innocent travel. But we think taken together they amount to reasonable suspicion. . . . We said in *Reid v. Georgia*, [448 U.S. 438, 441 (1980)], there could, of course, be circumstances in which wholly lawful conduct might justify the suspicion that criminal activity was afoot. . . . Indeed, *Terry* itself involved a series of acts, each of them perhaps innocent if viewed separately, but which taken together warranted further investigation. We noted in [*Illinois v. Gates*, 462 U.S. 213, 243–44 n.13 (1983)] that innocent behavior will frequently provide the basis for a showing of probable cause, and that in making a determination of probable cause the relevant inquiry is not whether particular conduct is innocent or guilty, but the degree of suspicion that attaches to particular types of noncriminal acts. That principle applies equally well to the reasonable suspicion inquiry.") (citations, footnotes, and internal punctuation omitted).

[90] *See, e.g., Sokolow*, 490 U.S. at 7; INS v. Delgado, 466 U.S. 210, 217 (1984).

[91] *See, e.g., Sokolow*, 490 U.S. at 7 ("The officer, of course, must be able to articulate something more than an inchoate and unparticularized suspicion or hunch. . . . The Fourth Amendment requires some minimal level of objective justification for making [a] stop. . . . That level of suspicion is considerably less than proof of wrongdoing by a preponderance of the evidence. We have held that probable cause means a fair probability that contraband or evidence of a crime will be found, and the level of suspicion required for a *Terry* stop is obviously less demanding than that for probable cause[.]") (citations and internal punctuation omitted). There also is no requirement that law enforcement officers undertake the least intrusive method of investigation. *See, e.g., id.* at 10-11.

Proof that a reasonable suspicion standard will not disrupt law enforcement can be seen in the Justice Department policy on the use of cell tower simulators. The Department requires a federal agent to have probable cause before he may use such a device. It follows that a reasonable suspicion requirement will not disrupt investigations into criminal activity.

CONCLUSION

Geolocation technology, if appropriately used, can serve as a valuable law enforcement tool. But it raises serious constitutional questions as well as legitimate issues about the privacy of those people who are innocent of any crime but whose phone service would be disrupted and whose data would be captured. Congress may wish to consider establishing some reasonable rules of the road to address those issues.

Thank you for the opportunity to help you work through these issues.

APPENDIX A

The Heritage Foundation is a public policy, research, and educational organization recognized as exempt under section 501(c)(3) of the Internal Revenue Code. It is privately supported and receives no funds from any government at any level, nor does it perform any government or other contract work.

The Heritage Foundation is the most broadly supported think tank in the United States. During 2014, it had hundreds of thousands of individual, foundation, and corporate supporters representing every state in the U.S. Its 2014 income came from the following sources:

Individuals 75%

Foundations 12%

Corporations 3%

Program revenue and other income 10%

The top five corporate givers provided The Heritage Foundation with 2% of its 2014 income. The national accounting firm of RSM US, LLP, audits the Heritage Foundation's books annually.

Members of The Heritage Foundation staff testify as individuals discussing their own independent research. The views expressed are their own and do not reflect an institutional position for The Heritage Foundation or its board of trustees.

Chairman CHAFFETZ. Thank you.

Ms. Guliani, you are now recognized for 5 minutes.

STATEMENT OF NEEMA SINGH GULIANI

Ms. GULIANI. Chairman Chaffetz, Ranking Member Cummings, and members of the committee, thank you for the opportunity to testify today on behalf of the American Civil Liberties Union.

In today's world, law enforcement can easily and inexpensively track virtually any American who owns a cell phone. GPS chips embedded into our phones provide real-time precise information about our every movement. Meanwhile, phone companies keep historical records that log information about our phone's location every time we make or receive a call, make or receive a text, or even receive a weather alert.

These advances have provided law enforcement with a powerful new surveillance tool that they routinely use. For example, in 2015, AT&T received over 76,000 requests for cell phone location information. Over 58,000 of these requests were for historical information which the company keeps for a period of 5 years.

Unfortunately, our Federal law has not kept pace with these technological realities. As a result, law enforcement officials and the public have been left to interpret a patchwork of State laws, conflicting legal precedent, and nonbinding policies to determine what policies apply.

This mosaic of standards has resulted in law enforcement officials routinely accessing location information without a warrant. For example, in one case in Baltimore, police collected over 7 months of historical location information without a warrant. This information allowed police to infer that an individual was likely at his pregnant wife's OB/GYN at some point during this period. In another case in Michigan, police collected over 6 months of location information without a warrant.

The Department of Justice has taken the position that a probable cause for warrant is not required for these types of collection. The ACLU disagrees with the government's position in this case. The Supreme Court's decision in Jones makes clear that the Fourth Amendment requires a probable cause warrant to collect historical or real-time location information.

In her concurrence in the Jones opinion, Justice Sotomayor emphasized the intimate nature of information that might be collected by GPS surveillance, including trips to a psychiatrist, trips to an AIDS treatment center, church, or even trips to a strip club.

In that same case, Justice Alito noted that society's expectation has been that law enforcement agents and others would not and could not "secretly monitor and catalog every single movement of an individual's car for a very long period of time." Due in part to these concerns, a majority of Justices in the Jones case found that long-term GPS tracking impinged on expectations of privacy.

More recently, the Supreme Court has expressed concern that cell phone location data can "reconstruct someone's specific movements down to the minute not only about town but also within a particular building." That's—what we're seeing is often a gap between law enforcement practices on one hand and on the other

hand the sensitivity with which Americans and the Supreme Court view our location information.

The ACLU urges Congress and the Department of Justice to take three steps to address this gap. Number one, the ACLU urges Congress to pass legislation such as the Geolocation Surveillance and Privacy Act introduced by Chairman Chaffetz that would require police to get a warrant before accessing location information. This bill takes a sensible approach. It would require police to follow the same procedures they follow when collecting a variety of sensitive information. At the same time, it preserves the ability of law enforcement to act without a warrant in truly exigent circumstances. This bill also reflects the approach that States like Utah, New Hampshire, and Montana have already taken.

Number two, until such legislation is passed, the ACLU urges the committee to continue to protest the Department of Justice to fully disclose its interpretation of the Supreme Court's Jones decision and any associated guidance. The public and Members of Congress should not be left in the dark about these important issues. By withholding this information, the DOJ has cut off the robust public debate and oversight that this issue demands.

Number three, we urge the committee to press the Department of Justice to adopt and publicly release a policy that requires a probable cause warrant to obtain real-time or historical information. Last year, the Department of Justice released guidance on stingrays demonstrating that it can operate under a warrant standard and release information about its policies without compromising investigations. These actions are obviously not a substitute for legislation, but they are necessary to protect the rights of Americans.

Thank you again for the opportunity to testify today, and I look forward to answering any questions that you may have on these important issues.

[Prepared statement of Ms. Guliani follows:]

Written Testimony of Neema Singh Guliani on behalf of the American Civil Liberties Union Before the U.S. House of Representatives Committee on Oversight and Government Reform

Hearing on

"Geolocation Technology and Privacy"

Wednesday, March 2, 2016 at 10:00am

Submitted by the
ACLU Washington Legislative Office

For further information, please contact Neema Singh Guliani, Legislative Counsel, at nguliani@aclu.org or 202.675.2322

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee:

Thank you for the opportunity to testify on behalf of the American Civil Liberties Union (ACLU).[1] As technology has advanced, consumers increasingly rely on electronic devices to work, communicate, surf the internet, or even hail a taxi. Many of these devices, including mobile phones, track and collect sensitive location information. Unfortunately, our laws have not kept pace with these new technological developments – resulting in confusion among the courts, law enforcement officials, and the public over the protections that apply to location information. As a result, law enforcement officials across the country routinely collect location information without a probable cause warrant or other appropriate privacy protections. For example:

- The Department of Justice (DOJ) has taken the position that a warrant is not required to collect historical cell site location information – even for a period spanning over seven months.[2]
- U.S. Attorney's Offices in the District of New Jersey and the Southern District of Florida have obtained precise mobile phone location data without a probable cause warrant, despite DOJ policy that recommends obtaining a warrant in such cases.[3]
- Numerous states and localities use cell phone tracking devices known as Stingrays, often funded by federal dollars, to collect location information without obtaining a warrant, adopting appropriate retention policies, or providing required notice to criminal defendants.

Congress and the Administration must act to remedy these deficiencies. We urge Congress to pass comprehensive legislation, beginning with the Geolocation Privacy and Surveillance Act, which requires law enforcement officials to obtain a probable cause warrant to obtain real-time or historical location information unless narrow exceptions apply. Until such legislation, this committee should ensure that the DOJ adopts a policy requiring a probable cause warrant before law enforcement can collect such information. In addition, this committee should demand that the DOJ publicly release unredacted

[1] For nearly 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and laws of the United States guarantee everyone in this country. With more than a million members, activists and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico and Washington, D.C., to preserve American democracy and an open government.

[2] Supplemental En Banc Brief of Appellee, United States v. Graham, 796 F.3d 332 (4th Cir. 2015) (rehearing en banc granted).

[3] Letter from William G. Stewart II, Assistant Director, Office of Information and Privacy, U.S. Dept. of Justice to Catherine Crump, Staff Attorney, American Civil Liberties Union (Dec. 31, 2008) *available at,* https://www.aclu.org/sites/default/files/pdfs/freespeech/cellfoia_released_074132_12312008.pdf (responding to FOIA request for mobile phone tracking information from the U.S. Attorney's Office for the District of New Jersey); Letter from William G. Stewart II, Assistant Director, Office of Information and Privacy, U.S. Dept. of Justice to Catherine Crump, Staff Attorney, American Civil Liberties Union (Dec. 31, 2008) *available at,* https://www.aclu.org/sites/default/files/pdfs/freespeech/cellfoia_released_074135_12312008.pdf (responding to FOIA request for mobile phone tracking information from the U.S. Attorney's Office for the Southern District of Florida).

copies of the memoranda that provide the Department's interpretation of the Supreme Court's decision in *U.S. v. Jones* and all existing guidance governing the collection of location information.

I. Current Technology Enables Invasive Tracking of Americans' Movements

A. Mobile phone data

In today's world, owning a cell phone is not a luxury. More than 90% of American adults have a cell phone,[4] and landline phones are becoming obsolete.[5] Americans increasingly rely on mobile phones to communicate, surf the internet, or even read the news. Americans carry mobile phones with them to a variety of sensitive or private locations, including homes, churches, doctor's offices, domestic abuse shelters, or even gun rallies. As the Supreme Court has noted, "nearly three-quarters of smart phones users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower."[6]

Mobile phones have revolutionized the way that Americans live their daily lives – but they have also provided law enforcement an unprecedented new surveillance tool. With the assistance of mobile phone carriers, at any given time, the government now can inexpensively obtain historical and real-time location information associated with any of the over 320 million U.S. mobile phone accounts.[7] Mobile phones yield information about users' past and present location, including Global Positioning System data and cell site location data.

1. Global Positioning System (GPS) data

Service providers can precisely locate cell phones in real time in two ways: by accessing information from the GPS receiver hardware built into a cell phone to determine the phone's coordinates based on signals from global positioning satellites, and by triangulating the phone's precise location using cell phone signals received by multiple cell towers in the area. This capability stems from rules adopted in 1996 and implemented by 2001, under which the Federal Communications Commission (FCC) required cell phone providers to have "the capability to identify the latitude and longitude of a mobile unit making a 911 call."[8] Although intended as a public safety tool for use in locating 911 callers, most service providers have made the same precise real-time location data available to law enforcement investigators as

---

[4] Lee Rainie, *Cell Phone Ownership Hits 91% of Adults,* PEW RESEARCH CENTER (June 6, 2013), http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/.

[5] STEPHEN J. BLUMBERG, PH.D. & JULIAN V. LUKE, WIRELESS SUBSTITUTION: EARLY RELEASE OF ESTIMATES FROM THE NATIONAL HEALTH INTERVIEW SURVEY, JANUARY-JUNE 2015, NATIONAL CENTER FOR HEALTH STATISTICS (Dec. 2015), *available at* http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201512.pdf.

[6] Riley v. California, 134 S. Ct. 2473, 2490 (2014) (citing 2013 MOBILE CONSUMER HABITS STUDY (CONDUCTED BY HARRIS INTERACTIVE), JUMIO (2013), *available at* http://pages.jumio.com/rs/jumio/images/Jumio%20-%20Mobile%20Consumer%20Habits%20Study-2.pdf).

[7] Cecilia Kang, *Number of Cellphones Exceeds U.S. Population: CTIA Trade Group,* W.S.J., Oct. 11, 2011, https://www.washingtonpost.com/blogs/post-tech/post/number-of-cell-phones-exceeds-us-population-ctia-trade-group/2011/10/11/gIQARNcEcL_blog.html.

[8] Report and Order and Further Notice of Proposed Rulemaking, *In re* Revision of the Communications Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Sys., 11 F.C.C. Rcd. 18676, 18683-84 (1996).

well. In January 2015, the FCC adopted new rules designed to increase precision when identifying the location of individuals indoors, including identification of the floor where a mobile device is located. The GPS systems of some mobile phones can pinpoint location with an accuracy of up to 3 meters,[9] and researchers are reportedly developing new technology that can pinpoint location to within centimeters.[10]

2. Cell site location data

Service providers also collect "cell site" data or "cell site location information," which identifies the location of the cell tower ("cell site") to which the phone is connected, the direction of the phone relative to the tower's antennas (the cell site "sector") and, in some instances, the phone's distance from the cell site. This data is generated because whenever individuals have their mobile phones on, the phones automatically and frequently communicate with nearby cell towers in order to facilitate the routing of calls, text messages, and other communications. In some circumstances, mobile carriers may be able to provide this ongoing registration information to law enforcement. More commonly, any time a phone makes or receives a call or sends or receives a text message, the service provider logs and retains a record of the cell site and sector to which the phone was connected. Service providers may also retain location information for passive data activities (e.g. weather notifications or e-mail synchronizations). In addition to tower and sector information, mobile carriers can now log more precise historical location information than before, including the estimated distance of the phone from the nearest tower, or the phone's precise location based on "triangulation," which entails collecting and analyzing data of the precise time and angle at which the mobile phone's signal arrives at multiple cell towers.

The precision of cell site location information depends, in part, on the size of the coverage area of each cell tower. This means that as the number of cell towers installed in cities and towns has increased and the coverage area for each cell tower has shrunk, cell site location information has become more precise. 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 office.[11] In addition, customers with poor cell phone coverage in their homes can even ask their carrier to provide them a "femtocell," a small cellular base station, which can cover just one home.

B. Internet connected devices and applications

As technology develops, consumers are embracing a host of internet-connected devices that log

---

[9] *What is GPS?* GARMIN (Feb. 25, 2016), http://www8.garmin.com/aboutGPS/.

[10] Press release, University of Texas at Austin, New Centimeter-Accurate GPS System Could Transform Virtual Reality and Mobile Devices (May 5, 2015), *available at* http://news.utexas.edu/2015/05/05/engineers-develop-centimeter-accurate-gps-system.

[11] *Hearing on Electronic Communications Privacy Act Reform and the Revolution in Location Based Technologies and Services Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on Judiciary*, 111th Cong. 5 (2010) (statement of Professor Matt Blaze), *available at* http://judiciary.house.gov/hearings/pdf/Blaze100624.pdf; Thomas Farely, *Cellular Telephone Basics: AMPS and Beyond*, PRIVATE LINE (Jan. 1, 2006), http://www.ccs.neu.edu/home/futrelle/teaching/com1204sp2001/Farley/Cellbasics.html .

location information. For example, as people use smart cars, medical devices, and wearable fitness devices more often, those devices collect more and more of consumers' location information. In addition, applications supported on smartphones, such as weather, restaurant, shopping, or even dating apps, often rely on and log location information. This location information is often stored by third party app providers in the cloud, not just locally on the consumer's device. The number of these applications and devices is only expected to grow. As of July 2015, there were over 3 million applications available just through the Google Play and Apple App Store.[12] Thus, as smartphones continue to advance and the "Internet of Things" becomes a more dominant reality, the availability of precise location information is likely to extend far beyond mobile carriers to other third parties. Despite these developments, the laws governing law enforcement access to location information held by these third parties remains unclear.

II. Law Enforcement Agencies Routinely Access Americans' Location Information

A. Information requests to mobile carriers

Law enforcement agents can request three types of location information from mobile carriers: historical cell site data, which can be used to retrace previous movements; prospective cell phone location data, which can be used to track mobile phones in real time; and "tower dumps," which provide the data of all the people whose phones were using a particular cell phone tower at a particular time. In recent years, law enforcement agencies have demanded this data from mobile carriers in a significant number of cases. For example:

- In 2015, AT&T received 76,340 requests for cell phone location information; 58,189 were for historical cell site location information.[13]
- In the second half of 2015, Verizon received approximately 20,289 requests for cell phone location data, and 4,558 requests for "tower dumps."[14]
- In the first half of 2015, Sprint received approximately 35,528 requests for real-time location data.[15]

The availability of historical information and the length of time this information is stored varies with the policies of each mobile phone carrier. Verizon has reported storing location information for one year;[16] T-Mobile keeps historical cell site information for six months;[17]

---

[12] *Number of Apps Available in Leading App Stores as of July 2015*, STATISTA (2015), http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/.

[13] AT&T, TRANSPARENCY REPORT 4 (2016), *available at* http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_Transparency%20Report_Jan%202016.pdf.

[14] *Verizon's Transparency Report for the 2nd Half of 2015*, VERIZON, http://transparency.verizon.com/us-report?/us-data (last visited Feb. 22, 2016).

[15] SPRINT CORPORATION TRANSPARENCY REPORT, SPRINT (July 2015), http://goodworks.sprint.com/content/1022/files/TransaparencyReportJuly2015.pdf.

[16] Letter from William B. Peterson, General Counsel, Verizon Wireless to the Honorable Edward J. Markey, United States Senator 3 (Oct. 3, 2013), *available at* http://www.markey.senate.gov/imo/media/doc/2013-12-09_VZ_CarrierResponse.pdf.

[17] U.S. Dep't of Justice, *Retention Periods of Major Cellular Service Providers* (Aug. 2010), *available at* https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart.

Sprint reportedly stores information from 18 to 24 months,[18] and AT&T retains location information for up to five years.[19]

B. Use of IMSI Catchers ("Stingrays")

The DOJ, Department of Homeland Security ("DHS"), Internal Revenue Service, and at least 60 state and local agencies have also purchased IMSI catchers – devices capable of gathering location information of all cell phones within range.[20] IMSI catchers, also known as cell site simulators or Stingrays,[21] function by impersonating legitimate cell phone towers operated by U.S. telecommunications companies. Depending on the particular features of the device and how the operator configures them, Stingrays can be used to identify nearby phones, to locate them with extraordinary precision,[22] and even to block service, either to all devices in the area or to particular devices.[23] They operate by sending probing signals into all homes and offices in range, which forces nearby cell phones to emit identifying signals which transmit their unique electronic serial numbers. By tracking these transmissions, Stingrays can locate cell phones and other mobile devices precisely.

Even when the government is only trying to locate a particular suspect's phone, Stingray technology, by design, sweeps up information about all bystanders' phones in the area. Some agencies, such as the U.S. Marshals Service,[24] attach these devices to planes, helicopters and

---

[18] *Id.*

[19] Letter from Timothy P. McKone, Executive Vice President, Federal Relations, AT&T to the Honorable Edward J. Markey, United States Senator (Oct. 3, 2013), *available at* http://www.markey.senate.gov/imo/media/doc/2013-10-03_ATT_re_Carrier.pdf.

[20] *See Stingray Tracking Devices: Who's Got Them,* ACLU, https://www.aclu.org/maps/stingray-tracking-devices-whos-got-them (last visited Feb. 22, 2016). The Department of Justice is charged with coordinating the use of Stingrays by state and local law enforcement agencies. IMSI catchers are so named in reference to the unique identifier—or international mobile subscriber identity—of wireless devices that they track.

[21] "StingRay" is the name for one cell site simulator model sold by the Harris Corporation, the leading vendor of the technology to U.S. law enforcement agencies. Other models include the "TriggerFish," "KingFish," and "Hailstorm." *See* Ryan Gallagher, *Meet the Machines That Steal Your Phone's Data*, Ars Technica, Sept. 25, 2013, bit.ly/1mkumNf. Other companies selling cell site simulators to domestic law enforcement agencies include Boeing subsidiary Digital Receiver Technology (DRT). *See* Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program*, W.S.J., Nov. 13, 2014, http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533. A number of companies in addition to the Harris Corporation produce and sell cell site simulator equipment. *See* CELLXION LTD., UGX SERIES 330: TRANSPORTABLE DUAL GSM / TRIPLE UMTS FIREWALL AND ANALYSIS TOOL, http://s3.documentcloud.org/documents/810703/202-cellxion-product-list-ugx-optima-platform.pdf (last visited Feb. 22, 2016) (including as features, "[c]omprehensive identification of IMSI, IMEI and TMSI information" and "[s]imultaneous high speed acquisition of handsets (up to 1500 per minute), across up to five networks").

[22] *See* Memorandum from Stephen W. Miko, Resource Manager, Anchorage Police Department, to Bart Mauldin, Purchasing Officer, Anchorage Police Department (June 24, 2009), *available at* http://files.cloudprivacy.net/anchorage-pd-harris-memo.pdf ("[The] system allows law enforcement agencies . . . the ability to . . . [i]dentify location of an active cellular device to within 25 feet of actual location anywhere in the United States.") [hereinafter Miko Memorandum].

[23] *See,* CELLXION LTD., *supra* note 21 (including as features, "[c]omprehensive identification of IMSI, IMEI and TMSI information"and "[s]imultaneous high speed acquisition of handsets (up to 1500 per minute), across up to five networks") (describing device's ability to "[d]isable all handsets except operationally friendly"); *See* Miko Memorandum, *supra* note 22 ("[The] system allows law enforcement agencies . . . the ability to . . . [i]nterrupt service to active cellular connection [and] [p]revent connection to identified cellular device.").

[24] U.S. Immigration and Customs Enforcement (ICE) has also purchased equipment to mount Stingrays on aerial

other aircraft, increasing the impacted geographic area and the number of innocent people whose telephones reveal identifying information to the government. [25] Though comprehensive information is not available, it appears that many agencies are using Stingrays not just occasionally, but frequently. For example,

- The Baltimore Police Department has used the devices in approximately 4,300 investigations since 2007,[26] and the Baltimore County Police Department has used them 622 times over five years.[27]
- The U.S. Marshals service has used cell site simulators in nearly 6,000 cases over a still undisclosed period of time.[28]
- The Sacramento Sheriff's Department initially estimated that it used cell site simulators in about 500 criminal cases, but later said it could be as many as 10,000.[29]

III. Law Enforcement Should be Required to Obtain a Warrant to Access Historical or Real-Time Location Information

Law enforcement should be required to obtain a probable cause warrant to access historical or real-time location information. 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. [30] In *United States v. Jones*, [31] 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 non-stop for 28 days.[32] 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.[33] As Justice Alito explained, "[s]ociety's expectation has been that law enforcement agents and others would not -- and indeed, in the

---

devices. PURCHASE ORDER, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT 44, *available at* https://www.documentcloud.org/documents/479397-#document/p44. The FBI has acknowledged operating IMSI catchers aboard aircraft at least five times. Eileen Sullivan, Jack Gillum, & Eric Tucker, *FBI: Surveillance Flights by the Book, Rarely Track Phones*, A.P., June 18, 2015, http://bigstory.ap.org/urn:publicid:ap.org:1240a8a42edf4a86aff72a0246525a95.

[25] Barrett Devlin, *supra,* note 21.

[26] Justin Fenton, *Baltimore Police Used Secret Technology to Track Cellphones in Thousands of Cases*, BALTIMORE SUN, Apr. 9, 2015, http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-case-20150408-story.html.

[27] Alison Knezevich, *Baltimore Co. Police Used Secretive Phone-Tracking Technology 622 Times*, BALTIMORE SUN, Apr. 9, 2015, http://www.baltimoresun.com/news/maryland/crime/bs-md-co-county-stingray-20150409-story.html.

[28] Brad Heath, *U.S. Marshals Secretly Tracked 6,000 Cellphones,* USA TODAY, Feb. 23, 2016, http://www.usatoday.com/story/news/2016/02/23/us-marshals-service-cellphone-stingray/80785616/ .

[29] *New Developments in Sacramento "Stingray" Case*, ABC 10, Jan. 8, 2016, http://legacy.abc10.com/story/news/local/sacramento/2016/01/08/new-developments-sacramento-stingray-case/78541240/.

[30] *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.").

[31] United Sates v. Jones, 132 S. Ct. 945, 954 (2012)

[32] *Id.* at 954.

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

main, simply could not -- secretly monitor and catalog every single movement of an individual's car, for a very long period."[34]

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."[35] 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."[36]

There have always been facets of American life which have been uniquely safeguarded from the intrusive interference and observation of government. Location tracking threatens to make even those aspects of life an open book to government. As Justice Sotomayor pointed out in *Jones*, "Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."[37] Further, location information from cell phones can reveal people's locations and movement within their homes and other spaces that receive heightened protection under the Fourth Amendment.[38] As the Supreme Court has noted, cell phone location data can "reconstruct someone's specific movements down to the minute, not only about town but also within a particular building."[39]

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.[40]

---

[34] *Id.* at 964 (Alito, J., concurring).
[35] *Id.* at 955 (Sotomayor, J., concurring) (quoting *People v. Weaver*, 12 N.Y.3d 433, 442 (N.Y. 2009)).
[36] United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd sub nom. Jones*, *supra* note 31.
[37] *Jones*, *supra* note 31 at 956 (Sotomayor, J., concurring) (quotations omitted).
[38] *See* Tracey v. State, 152 So.3d 504, 524 (Fla. 2014) ("We cannot overlook the inexorable and significant fact that, because cell phones are indispensable to so many people and are normally carried on one's person, cell phone tracking can easily invade the right to privacy in one's home or other private areas."); *see also* In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304, 318 (3d Cir. 2010).
[39] *Riley*, *supra* note 6 at 2490.
[40] *Jones*, *surpa* note 31 at 956 (Sotomayor, J., concurring) (quotations omitted).

Furthermore, while the government has argued 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."[41] Historical records provide the government with a new power, a veritable time machine that allows it to learn sensitive information about a person's movements and activities months and even years into the past.

While the *Jones* case dealt with long-term tracking of movements, even single points of mobile phone location data can intrude upon reasonable expectations of privacy– a single GPS data point revealing that someone is in the waiting room of a psychiatrist's office, at a church, or at an AA meeting can reveal information that is highly sensitive.[42] The Supreme Court has held that location tracking even using relatively crude "beeper" trackers implicates reasonable expectations of privacy where it "reveals information that could not have been obtained through visual surveillance from a public space."[43] For this reason, and because law enforcement agents often will not know whether a particular piece of mobile phone location data will implicate a person's privacy interest in their location in private spaces, the better rule is an across-the-board requirement that law enforcement agents obtain a warrant based on probable cause for location data.

IV. Current Laws Fail to Protect Americans' Privacy

There is confusion among law enforcement agents, courts, and members of the public regarding what legal standard law enforcement agents must meet to obtain location data – underscoring the need for legislation. This is due in part to the fact that the principal law that governs law enforcement access to records regarding electronic communications, the Electronic Communications Privacy Act of 1986, does not expressly address law enforcement access to location data. As a result, location tracking is governed by a patchwork of state and local laws, non-binding policies, and inconsistent court cases.

Twelve states – California, Indiana, Illinois, Maine, Maryland, Minnesota, Montana, New Hampshire, Utah, Virginia, Washington, Wisconsin – have passed laws requiring police to get a warrant to obtain real-time location information.[44] Six of these states require a warrant for collection of historical cell site information.[45] In addition, at least seven states require a warrant

[41] *In re* Application of the United States for an Order Authorizing Release of Historical Cell-Site Information, 736 F.Supp.2d 578, 585 (E.D.N.Y. 2010).

[42] United States v. Davis, 754 F.3d 1205, 1216 (11th Cir. 2014) ("[E]ven on a person's first visit to a gynecologist, a psychiatrist, a bookie, or a priest, one may assume that the visit is private if it was not conducted in a public way. . . . Thus, the exposure of the cell site location information can convert what would otherwise be a private event into a public one. . . . [E]ven one point of cell site location data can be within a reasonable expectation of privacy."), *rev'd* 785 F.3d 498 (11th Cir. 2015) (en banc).

[43] United States v. Karo, 468 U.S. 705, 707 (1984).

[44] Cal. Penal Code § 1546; 16 Maine Rev. Stat. § 648; Md. Code, Criminal Procedure 1-203.1(b)(1); Minn. Stat. §§ 626A.28(3)(d), 626A.42(1)(d); Mont. Code § 46-5- 110(1)(a); N.H. Stat. § 644-A; Va. Code § 19.2-56.2; Wash. Rev. Code § 9.73.260.725; Ill. Comp. Stat. 168/10; Ind. Code § 35-33-5-12; Wis. Stat. § 968.373(2); Utah Code § 77-23c-102.

[45] Cal. Penal Code § 1546; 16 Maine Rev. Stat. § 648; Minn. Stat. §§ 626A.28(3)(d), 626A.42(1)(d); Mont. Code § 46-5-110(1)(a); N.H. Stat. § 644-A; tah Code § 77-23c-102.

before installing an electronic tracking device, and Washington, Virginia, and California have passed legislation limiting Stingray use.[46] While these laws alone are not sufficient to protect the rights of all individuals, they reflect a growing consensus among Americans that location information should be afforded a high degree of protection.

Not surprisingly, given the variations in law, law enforcement agencies' practices also vary widely. In August 2011, 35 ACLU affiliates submitted public records requests with state and local law enforcement agencies around the nation seeking information about their policies, procedures, and practices for obtaining mobile phone location data.[47] Over 200 local law enforcement agencies responded. While the overwhelming majority engaged in at least some cell phone tracking, the legal standards they met varied widely. For example, police in Lincoln, Nebraska, obtained even GPS data without a warrant based upon probable cause. Police in Wilson County, North Carolina, obtained historical cell site location information by proffering only that the data is "relevant and material" to an ongoing investigation. Some police departments, including police in the County of Hawaii, Wichita, and Lexington, secured warrants based upon probable cause to obtain mobile phone location data.

U.S. Attorney's Offices have also acted inconsistently. DOJ recommends that law enforcement agents obtain a warrant based upon probable cause to access precise real-time location data.[48] However, litigation by the ACLU and Electronic Frontier Foundation revealed that U.S. Attorney's Offices in the District of New Jersey and the Southern District of Florida have obtained even what DOJ classifies as precise mobile phone location data without obtaining a warrant or showing probable cause.[49]

The courts have only provided incomplete guidance on the protections that should apply to law enforcement requests for location information. In *United States v. Jones*, the Supreme Court held that attaching a GPS device to a car and tracking its movements is a search under the Fourth Amendment. *Jones*, however, left unresolved how its holding would apply to surveillance performed with other technologies such as mobile phone tracking or Stingrays. The DOJ has issued two guidance memoranda setting out its view of how *Jones* affects the constitutionality of various forms of location tracking; unredacted copies of these memos have not been made public despite an ACLU request for them under the Freedom of Information Act and numerous Congressional inquiries.

Circuit courts, interpreting the *Jones* decision, have provided inconsistent guidance on the appropriate standard governing law enforcement access to location information. With regard to historical location information, the Fifth Circuit has ruled that a warrant is not required, as

---

[46] Cal. Penal Code § 637.7; Del. Code § 1335(a)(8); Haw. Rev. Stat. § 803- 42(a)(8); Minn. Stat. § 626A.35; Tenn. Code § 39-13-606; Tex. Penal Code § 16.06; Va. Code § 18.2-60.5.; Wash. Rev. Code § 9.73.260.

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

[48] *The Electronic Communications Privacy Act: Government Perspective on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on Judiciary*, 125th Cong. 7 (2011) (statement of James A. Baker, Associate Deputy Att'y Gen., U.S. Dep't of Justice), *available at* https://www.gpo.gov/fdsys/pkg/CHRG-112shrg70856/pdf/CHRG-112shrg70856.pdf.

[49] *ACLU v. Department of Justice: ACLU Lawsuit To Uncover Records of Cell Phone Tracking,* ACLU https://www.aclu.org/cases/aclu-v-department-justice (updated Feb. 19, 2014).

has the en banc Eleventh Circuit, which reversed a unanimous three-judge panel of that court holding that a warrant is required. In the Fourth Circuit, a three-judge panel held that a warrant is required, but that decision is being reconsidered by the en banc court. The Third Circuit has ruled that magistrates have the discretion to demand a warrant for location information; a case is pending in the Sixth Circuit; and the government has dropped its appeal to a Ninth Circuit case in which a lower court ruled that a warrant was required.[50] As to real-time cell phone location tracking, the Florida Supreme Court has held that a warrant is required for even short-term tracking, while the Sixth Circuit held that, at least in some circumstances, no warrant is required.[51] Most federal magistrate judges to consider the issue have held that a warrant is required for real-time tracking as a statutory matter, but have not addressed the constitutional questions involved.[52] Thus, absent a Supreme Court examination of this issue, there will continue to be a lack of uniformity among lower courts on the protections that apply to location information. And, courts may continue to lag one step behind the privacy threats that face Americans daily.

V. Congress Should Pass the Geolocation Privacy and Surveillance Act

Given that it will likely take years before the Supreme Court once again considers the constitutionality of location tracking, Congress must act now to ensure that Americans' privacy is protected. For this and the many other reasons set forth herein, the ACLU supports passage of the Geolocation Surveillance and Privacy Act.

Importantly, the Geolocation Surveillance and Privacy Act (H.R. 491) would require a warrant to obtain historical or real-time location information from any entity, unless specific exceptions apply. As such, the bill reflects the long-standing preference by the Supreme Court to "provide clear guidance to law enforcement through categorical rules."[53] Such an approach is preferable to the current environment, where there is inconsistent guidance at the federal and state levels. In addition, this formulation also anticipates future technological developments, in which a variety of third parties are likely to collect and store location information for varying purposes. Thus, the bill allows law enforcement to access this data – but only with appropriate standards.

In addition, the H.R. 491 includes exemptions to the warrant requirement, which preserve the ability of law enforcement to operate in special circumstances. For example, the bill provides exceptions to the warrant requirement to retrieve a lost or stolen phone; where there is not time to secure a warrant; in emergencies where it is reasonable to believe that the life or safety of an individual is threatened; or with consent. Moreover, the bill includes appropriate suppression remedies, in cases in which location information is improperly collected.

---

[50] *In re* Application of the United States for Historical Cell Site Data, No. 11-20884 (5th Cir. July 30, 2013); United States v. Davis, 785 F.3d 498 (11th Cir. 2015); United States v. Graham, 796 F.3d 332, 360 (4th Cir. 2015) (rehearing en banc granted); *In re* Application of U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to Gov't, 620 F.3d 304 (3d Cir. 2010); United States v.Carpenter, Nos. 14-1572 & 14-1805 (6th Cir.); *In re* Application for Telephone Information Needed for a Criminal Investigation, U.S. Dist. 2015 WL 4594558 (N.D. Cal. 2015).

[51] Tracey v. State, 152 So.3d 504 (Fla. 2014); United States v. Skinner, 690 F.3d 772 (6th Cir. 2012).

[52] *See* United States v. Espudo, 954 F. Supp. 2d 1029, 1035 (S.D. Cal. 2013) (collecting cases).

[53] *Riley*, *supra* note 6 at 2491.

The Geolocation Surveillance and Privacy Act, however, could be strengthened by:

- Including clear rules on the use of Stingrays, and other devices that collect location and other information. These rules should require a warrant to use a Stingray; require timely purging of non-target information; specify the information that must be included in any warrant application; and require prosecutors to notify individuals in cases where information obtained or derived from a Stingray is used;
- Eliminating exceptions that permit the collection of location information without a warrant under provisions of the Foreign Intelligence Surveillance Act, which have been abused to permit bulk collection; and
- Requiring law enforcement agencies' to report statistics on their collection of location information, to facilitate effective oversight.

As Congress considers location-tracking legislation, however, we cannot afford to let the DOJ sit idle. We urge this committee to insist that DOJ take steps to protect the rights of Americans by promptly adopting a policy requiring a warrant to collect real-time and historical location information. Such a policy would reflect Americans' reasonable expectation of privacy; the finding by a majority of the Supreme Court that long-term GPS monitoring infringes on reasonable privacy expectations; and the limits the Fourth Amendment places on government access to Americans' private information.

In addition, the committee should demand that DOJ disclose information on how it is interpreting the *Jones* decision, and publicly release its policies surrounding law enforcement collection of location information. To date, the DOJ has refused to release this information to the public or members of Congress, citing concerns that disclosures could reveal sensitive law enforcement methods. Such concerns, however, are unfounded. Just last year, the DOJ was able to publicly release guidance on the use of Stingrays, without compromising law enforcement activities. Similarly, on an issue of this paramount importance, the DOJ must respond to demands from the public and Congress for greater transparency.

VI. Conclusion

The ACLU agrees with Justice Alito that, in this time of rapid technological change, Congress has an important role to play in regulating the use of surveillance technology by government. Thus, we urge Congress to pass legislation, and in the interim, for the committee to urge DOJ to adopt policy requiring a probable cause warrant to collect historical and real-time location information, disclose information on how it is interpreting *Jones,* and to publically release its policies on law enforcement collection of location information. Such an approach safeguards Americans' privacy interests, while preserving the ability of law enforcement to appropriately access the information necessary to perform their duties.

Chairman CHAFFETZ. Thank you all for your testimony.

I would like to enter into a colloquy with Mr. Cummings here prior to our questioning.

We had good word from the Department of Justice just within the last 24 hours that they would allow myself and Mr. Cummings, plus we would each allow one staff person to review the post-Jones guidance. Now, while I appreciate that gesture, I need to say that it is frustrating that it has literally taken years to get to this point. I serve on the Crimes Subcommittee within the Judiciary Committee, and I am the chairman of the Oversight Committee, and thus far, the Department of Justice has refused to allow those of us who serve in Congress to even understand how they are using these types of materials.

This is a positive step forward. I appreciate it. But as Ms. Guliani just pointed out, the public doesn't know what is happening, and we don't know what is happening. I look forward to seeing that information and working with Mr. Cummings on this.

Let me yield to Mr. Cummings.

Mr. CUMMINGS. Mr. Chairman, first of all, I agree with you. These issues are very, very important to our committee and the Congress and the American people, and so I am happy that we could work together with the Department of Justice over its production of Jones memoranda.

The Department has agreed to provide us with full access to all of the information we requested with no redactions, and we have agreed to consult closely with the Department going forward. We were able to reach an appropriate balance between legitimate congressional oversight and protecting law enforcement sensitivities. I commend the Department for responding to our concerns, and I commend the chairman for working through this issue in a very thoughtful way. We did this in a bipartisan manner, and I hope that we can continue this approach on other information requests important to this committee. Congressional oversight is a critical function, and we have to have the cooperation of entities subject to our oversight, whether that is in the public of the private sector.

And with that, I will yield back.

Chairman CHAFFETZ. I thank the gentleman.

I would also want everybody to know that it is not just the Department of Justice that owns, maintains, and operates the cell phone simulators, stingrays, whatever you want to call them. There are different brand names, different versions of the technology. For instance, the Internal Revenue Service has these machines. They have deployed these machines. How in the world is the Internal Revenue Service using this information? We don't know. So today, we are going to be focused much on the Department of Justice, but there are also other parts of government.

I will also credit the ACLU for the good work that they did in surveying law enforcement across the country at various levels. Whether it be State, county, or municipal, there are lots of machines that are out there and available in other law enforcement situations that are not focused at the Federal level at the Department of Justice. And so the use of that type of information is more pervasive than just at the Federal level.

And finally, I would remind members that you can go on the Web and buy these machines, so don't think that this is just limited to the good guys in law enforcement. I do think we are living in a world and an age where the price point will dramatically decrease where organized crime, somebody with nefarious intent, some punk, whatever, is going to go out there and want to be able to use this type of information to gather information about somebody's geolocation and then be able to track that person back and then go find them with such specificity that if you were in New York City, as was mentioned, you could tell not only that they are on a certain block, you could tell which floor they are on and which apartment they are in or which office they are in. That is some pretty scary stuff, and that is something that I think we have to also consider.

So with that as the backdrop, and I appreciate the colloquy, let's go to the questions. I am going to recognize myself first, and we will start here with Mr. Downing. And I do appreciate you being here. I really do. These are tough, difficult questions.

I still struggle with how the Department of Justice considers geolocation. Is it metadata or is it content? Because the district court ruled that it is content. How does the Department of Justice view this information?

Mr. DOWNING. Thanks very much for the question. That's, I think, the interesting and tricky thing about this label that we've placed on it as geolocation data because it can come in very many different forms. At times, I would say that it is metadata. That is, it is not the content of a communication but simply information about the location of where a phone is.

But if you think broadly about the way that location information can be stored, if I send an email to my mom and say I'm at the office, well, that's actually location information and it's in that form the content. That might also be true, for example, if I were to post a photograph on Facebook that contained information that might be part of that photograph and therefore content.

Chairman CHAFFETZ. But does the Department of Justice believe that if it knew I was at the hospital at the oncology department, isn't that the content of my life? And then I move from there to somewhere else, why is that not content? You think that is simply metadata?

Mr. DOWNING. So, the general construct is the content of the communication versus information about a communication. That's the general way that we look at these kinds of questions. If I were to place a call using my landline phone, the number that I dialed would widely be considered metadata, but the fact that I'm calling Home Depot is—gives an idea about what I might be talking about, but it's still metadata even though it can be used to infer certain things.

Chairman CHAFFETZ. And this is where I think I beg to differ. I think geolocation certainly used for more than just a split second snapshot in time, even if it was, you can tell a lot about what they are doing. If I called from the local jail, that is going to provide a lot more information than just the fact that I called Bob.

Is there anything that Ms. Guliani or Mr. Larkin or Mr. Doucette said, Mr. Downing, that you disagree with or you found in their testimonies?

Mr. DOWNING. One thing that I think is important to understand is that we often hear discussion about whether something was obtained without a warrant. And of course that is true. That is the Department's position. But it brushes over the idea that when we use a court order under section 2703 of ECPA that there are substantial privacy protections built into that, that it's not that law enforcement is waltzing in and just obtaining it at a whim but in fact a series of process which require specific facts presented to the judge before we can obtain that information. That's one response I would have that I would offer.

Chairman CHAFFETZ. Is the IRS doing that?

Mr. DOWNING. I don't oversee the IRS, but I do believe that they would be, yes, because ——

Chairman CHAFFETZ. Why do you believe that?

Mr. DOWNING. Because the carriers know what sort of process to expect ——

Chairman CHAFFETZ. So it is up to AT&T to police the IRS? I mean, you have jumped to a conclusion and an assumption that the IRS is living up to the standard of the Department of Justice. I want to know why you think that is.

Mr. DOWNING. Well, I think all law enforcement agents and prosecutors ——

Chairman CHAFFETZ. But is the IRS ——

Mr. DOWNING.—we follow the law, and the law is that, at a minimum, you need to obtain a—this kind of court order to obtain records or other information pertaining to a customer or subscriber. That's the law.

Chairman CHAFFETZ. Ms. Guliani, is that the way you see that?

Ms. GULIANI. No, we disagree with the Department of Justice. The standard that is under 2703(d) is not a probable cause standard, and we believe that doesn't reflect the intimate nature of location information. It doesn't reflect how Americans view this information. Under polling, 80 percent of Americans view their location information over time as sensitive. That's a greater percentage than view their relationship history or their religion as sensitive.

And the Department of Justice's position also doesn't comport with what courts have said about the sensitivity of this information. Courts have recognized that location information over time can tell you whether someone is a regular churchgoer, is an unfaithful husband, is a heavy drinker. And given the intimate nature of this information, we believe that a probable cause standard is the correct standard, as many courts have found.

Chairman CHAFFETZ. So the FBI Director testified that they do use probable cause, but what about all the rest of the Department of Justice? Do they or do they not under the description Ms. Guliani cited there?

Mr. DOWNING. I think I would go back to the general overarching point here, which is there are many kinds of location information. We certainly do use warrants for cell-site information when it is collected by the cell-site simulator. We also use warrants when we are collecting precise GPS location from the providers.

The difference is, and the courts have supported us in this, when we are obtaining less precise information that is a business record of a carrier, cell-site information, then that does not require a war-

rant, although there are many standards that have to be met that are built in for the protection of the privacy of the individual.

Chairman CHAFFETZ. My time is expired, but I do wish you would provide that standard to the public and to the Congress. We are different than most every other country on the planet, I get it, but we do value our privacy, too.

Ms. Guliani, I will let you speak and then we will go to the ranking member.

Ms. GULIANI. Yes, I just wanted to address the point of this idea that some—historical cell-site information is not as precise as GPS information, and that doesn't reflect the way technology is moving. We're increasingly seeing this information be very precise because it's not just the tower you connect to, it's the direction, it's the distance. Even in cases people have microcells, so a tower that only serves their home. And given this, the precision of cell site information, historical cell-site information is quite accurate and I think doesn't—I think our—the standards that we've used have—does not reflect that accuracy.

Chairman CHAFFETZ. Thank you. I will recognize the ranking member, Mr. Cummings.

Mr. CUMMINGS. Ms. Guliani, geolocation information is a critical law enforcement tool, I think you will agree, but it has significant implications for an individual's privacy rights. We have to balance the need of our law enforcement authorities to access this information with the importance of protecting the privacy rights of American citizens.

Cell phones and other wireless communication devices provide location information to service providers each and every time a phone call is placed. Is that correct?

Ms. GULIANI. That's correct.

Mr. CUMMINGS. You mentioned the Baltimore case a little bit earlier.

Ms. GULIANI. Right.

Mr. CUMMINGS. And you said that apparently they had surveillance for 7 months. Is that what you said?

Ms. GULIANI. They had obtained historical cell-site information for a period of over 7 months, that's correct.

Mr. CUMMINGS. And what happened in that case?

Ms. GULIANI. In that case, police did not obtain a probable cause warrant. They operated under a lower standard, and that case is being challenged.

Mr. CUMMINGS. Now, should individuals have a reasonable expectation of privacy with respect to their location information?

Ms. GULIANI. We believe that individuals do have a reasonable expectation of privacy and that that has been reflected in statements from the Supreme Court that have recognized that the Fourth Amendment has always acknowledged that there are facets of American life that should be free from improper government intrusion. And your location, whether you're in your home, whether you're in a church, that those are aspects that should be protected.

Mr. CUMMINGS. Mr. Doucette, geolocation information can be used to provide critical assistance in complicated criminal investigations to apprehend dangerous and violent fugitives or help lo-

cate kidnapped children. Can you describe how geolocation information can be useful in these types of complex criminal cases?

Mr. DOUCETTE. Mr. Chairman, Mr. Cummings, the—we've had a number of cases, especially dealing with historical cell tower information, where we've been able to obtain this particular information through a court order, a 2703 court order, and were—and specifically in one case in Lynchburg we were able to solve a rather serious homicide where we had no suspects at all, and basically through the course of doing this particular investigation developed the estranged son-in-law.

But we had no information whatsoever to beat his alibi that he was in Richmond 2 hours away until we were able to get his historical cell tower information through a court order and show that, no, at the time that the murder occurred he was actually in city of Lynchburg. But that was not enough to get any sort of a conviction. We had to go forward and do a lot of police work afterwards, but again, that led us down the right path and led us through to be able to ultimately bring this person to justice.

Mr. CUMMINGS. You know, when you watch 20/20, you find the use of this cell phone information to be extremely helpful in a lot of very, very serious cases showing where the location of a person was at a certain time and to kill an alibi easily. Mr. Downing, how precise is historical cell-site information?

Mr. DOWNING. Historical cell-site information varies considerably depending on the size of the coverage area of the particular antenna. In rural areas, it tends to be extremely large, a matter of miles perhaps. In urban areas, it tends to be smaller, and in certain cases, may be quite small, down to the level of a much smaller area.

Mr. CUMMINGS. So when you say rural, I mean, can you give me a max, just general, what, 5 miles, 10 miles, 20 miles?

Mr. DOWNING. I don't know the specifics, but it's on the order of, yes, 5 to 10 miles, something like that.

Mr. CUMMINGS. What impact would a search warrant requirement for historical cell-aside information have on a criminal investigation?

Mr. DOWNING. We are troubled by the idea of requiring a probable cause warrant because there are situations like the one I mentioned involving the person shooting at the judge where we are at an early stage of we do not yet have probable cause, but the ability to gather that sort of information can be very important to follow up on leads such as Mr. Doucette mentioned and to exclude people, frankly, that are not involved or that weren't involved in the crime. So that's an important and useful tool, and it should be considered as we debate this question.

Mr. CUMMINGS. Mr. Doucette, do you agree?

Mr. DOUCETTE. Absolutely, sir.

Mr. CUMMINGS. And what impact do you think a search warrant requirement would have on a criminal investigation?

Mr. DOUCETTE. Again, as pointed out by Mr. Downing, a lot of times we're strictly in the investigative stage. It would shut down the investigation completely because we would not have that level of probable cause. We're using this particular information to establish probable cause, not that we already have it.

Ms. Guliani, a search warrant is not required for physical surveillance of a suspect. Why should a search warrant be required for geolocation information?

Ms. GULIANI. The nature of the information we're talking about is quite different from a police officer, for example, following someone. You know, with phone information, the law enforcement can inexpensively and easily track virtually anybody, and it's not constrained by resources as you would normally have in a situation where police are following somebody.

But I also want to follow up on this question of, you know, whether a probable cause warrant will interfere with the ability of law enforcement in certain cases. The idea of a warrant for this information is not a novel idea. There have been many States to have passed laws that require a warrant for real-time or historical information, and there's no evidence that, for example, in Utah or in Montana where such a standard exists that law enforcement has been stopped from doing their job.

Mr. CUMMINGS. And last but not least, I want to go back to something that the chairman was talking about. And I guess he was talking about the stingrays. You know, one of the things that I have always been concerned about, the domestic violence cases where you have usually a woman who is trying to get away from a dangerous situation. She relocates trying to hide really from danger. And I guess, as she was talking, I was thinking that is a lot of power for someone who wants to get to her. Is that right, Mr. Doucette? Would you agree?

Mr. DOUCETTE. Absolutely, sir. And we did include—because the—when we are dealing with real-time location data such as whether it comes from a cell phone or provider or through a stingray, we do in Virginia require a search warrant because we do have probable cause. And again, you know, if a perpetrator wants to use this, the Fourth Amendment does not deal with him. We're going to have to pass laws, but outside of the realm of the Fourth Amendment.

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

Chairman CHAFFETZ. Thank you. I now recognize the gentleman from Ohio, Mr. Jordan ——

Mr. JORDAN. Thank you ——

Chairman CHAFFETZ.—for 5 minutes.

Mr. JORDAN. Thank you, Mr. Chairman.

Ms. Guliani, you are familiar with the stingray technology that the chairman referenced a little bit ago?

Ms. GULIANI. Yes.

Mr. JORDAN. Yes. And the fact that it mimics a cell site, tricks phones into going to that so that the person using the stingray can get access to the numbers and therefore where this person in fact is located?

Ms. GULIANI. That's correct, all phones in range.

Mr. JORDAN. And the fact that every major law enforcement agency in the Federal Government is using that, I assume that troubles you a little bit like it does me?

Ms. GULIANI. We are very troubled specifically by the notion that these devices have been shrouded in secrecy. The public didn't know about them, judges in many cases, defense attorneys.

Mr. JORDAN. And did you also know that it wasn't just limited to law enforcement, that it included the Department of Energy and more importantly, as the chairman pointed out, the Internal Revenue Service?

Ms. GULIANI. Yes ——

Mr. JORDAN. Did you know that?

Ms. GULIANI. There have been recent reports that the IRS and other agencies are also using these devices.

Mr. JORDAN. Mr. Downing, did you know the IRS was using the stingray technology?

Mr. DOWNING. I believe that—I do understand that. It's the criminal part of the IRS, the criminal investigators.

Mr. JORDAN. But did you know they were using it or did you learn it in the press like the rest of us did?

Mr. DOWNING. I personally didn't have specific knowledge of it, no.

Mr. JORDAN. I know you have got this Jones memo that you have given to all law enforcement in the Federal Government but won't show Congress and therefore the American people. Has the Jones memo gone to the Internal Revenue Service to tell them how you think they should use this stingray technology that you didn't know they were using?

Mr. DOWNING. No, it did not to my knowledge.

Mr. JORDAN. So you haven't sent it to them, but this is the guideline on how we are supposed to deal with this important privacy issue that you thought was so important that you gave it to everyone in the Justice Department? You won't let Congress see it, but you know an agency has used the technology and you didn't give them the memo, the guidelines on how they should appropriately use it?

Mr. DOWNING. We have given them the cell-site policy of ——

Mr. JORDAN. No, no, I am asking about the Jones memo, this secret document that you won't let us see. Has it been given to the Internal Revenue Service? After all, they have used this technology on American people.

Mr. DOWNING. The Jones memo is a memo that advises ——

Mr. JORDAN. Has it gone to the Internal Revenue Service?

Mr. DOWNING. I don't know the answer to that. I don't believe so.

Mr. JORDAN. Well, that is scary because let me just remind you all of something here. The Internal Revenue Service, for a sustained period of time, systematically targeted Americans who were exercising their First Amendment liberties, and they sent questionnaires and information to these—told these groups to answer questions like this: "Please provide board members or officers who have run or will run for public office who are in your group." "Please provide handouts you provided to the audience participants and to the public." "Please provide detailed contents of any speeches given at your meetings," copies of current Web pages. They ask them, "Will you attempt to influence the outcome of specific legislation?" That is a fancy way of asking will you exercise your First Amendment rights. Are you kidding me?

And now this same agency has stingray technology, has used stingray technology, and you haven't even given them the memo to

tell them how they should appropriately use it? This is unbelievable. "Give copies of all communications, pamphlets, advertising, copies of any radio, television, Internet advertising you have done," another 33 questions sent to another Tea Party group. "Have you conducted or will you conduct voter education activities?" This is amazing. "Provide details regarding your relationship with"—they list a person's name, Justin Thomas.

Now, think about this. All these questions that I think go right to the First Amendment liberties, and now this agency has a technology that they can go into an area where let's say there is a political rally going on. They go into an area, say we are going to trick every cell phone to come into this device so we can get people's phone numbers, know who they are, who they have been talking to, who they associate with in this context, and you didn't even know about it and you haven't even advised them on how to use it?

Mr. Larkin, is that a little concerning to you?

Mr. LARKIN. The predicate facts are very disconcerting, very troubling. One of the lines that I think the committee should consider not drawing is trying to limit the use of these sort of devices by agency because, over time, it will bleed over into every other agency. And that doesn't even begin to count the number of State and local agencies that can use these devices. So there's a very troubling aspect of this problem.

Mr. JORDAN. Yes, it seems to me at a minimum you need a probable cause warrant before you can do this. I mean, again, I think you have to view everything in context. You have to view it within the framework of what we have seen from this administration going after people's First Amendment liberties, people's Fourth Amendment liberties, and now they have this technology that the Internal Revenue Service is using with no guidance from our own Justice Department? I mean, that boggles the mind, boggles the mind.

Ms. Guliani, I will give you the last word.

Ms. GULIANI. Sure. I mean, I would echo the same concerns. We're concerned that the guidance that exists doesn't apply to States and localities or other Federal agencies, but I will note even that guidance has loopholes and deficiencies. There's a warrant requirement by default except for exceptional circumstances. Exceptional circumstances aren't defined, and we've had no additional information as to what that even means. So given this and some of the other deficiencies, how are judges informed of this, how are defense attorneys informed of information from these devices being used? There's just no clarity right now.

Mr. JORDAN. This Jones memo, the guidelines, this secret memo that we can't see but the night before the hearing they tell the chairman and the ranking member, oh, we will let you view it in private with your secret 3–D glasses or whatever it is and they won't let the IRS know how they should do this, unbelievable. Well, I mean, it is truly unbelievable what we're seeing in America today from this Justice Department.

I yield back, Mr. Chairman.

Chairman CHAFFETZ. I thank the gentleman.

I would now recognize the gentleman from California, Mr. Lieu, for 5 minutes.

Mr. LIEU. Thank you, Mr. Chairman.

Mr. Downing, you had testified in your earlier testimony that these stingray devices track geolocation but they don't track content. It is true, however, that these stingrays can in fact be configured to track the content of conversations, correct?

Mr. DOWNING. The devices that we use are not configured, nor do they have the necessary software to do that. And if they did, it would be in violation of our policy. But as a general matter, this type of technology could be used in that manner that you suggest.

Mr. LIEU. Could this technology also be configured to track text messages and emails, the contents of those communications as well?

Mr. DOWNING. If you have the right software and you configured it and you violated the policy, then yes, you could do that as ——

Mr. LIEU. Is there anything stopping the Department of Justice from changing the policy next month or next year?

Mr. DOWNING. No, we have the ability to change the policy.

Mr. LIEU. The IRS has these stingrays. Does your policy apply to them?

Mr. DOWNING. It doesn't apply to them directly, but if they were to be used in compliance with the pen register statute, then they would need to have a prosecutor—a department employee involved in that.

Mr. LIEU. Does your policy apply to local law enforcement agencies?

Mr. DOWNING. It does not apply to ——

Mr. LIEU. Okay.

Mr. DOWNING.—local law enforcement agencies.

Mr. LIEU. So these stingrays could in fact be used by the IRS or local law enforcement agencies to not just track geolocation information but also the content of communications, including text messages and emails, correct?

Mr. DOWNING. If they did it without a wiretap order, then it would likely be a Federal criminal offense, but I suppose, yes, anything is possible.

Mr. LIEU. Let's talk about historical data versus real-time tracking. My understanding is the Department of Justice believes that you don't need a warrant to access historical geolocation data, but you do need one for real-time tracking. Am I understanding your position correctly?

Mr. DOWNING. We have taken the position publicly that we do not need—you do not need a warrant for historic cell location information. If we were to use real-time tracking, if what you mean is specific precision GPS location on a prospective basis going forward, we, yes, agree a warrant is required in that circumstance.

Mr. LIEU. So let's say someone has cancer and doesn't want people to know about it, they go to a clinic that just treats cancer, why would it matter from a privacy perspective whether that person went to that cancer clinic last week or they are there right now or they are about to go to it tomorrow? Isn't the privacy interest exactly the same?

Mr. DOWNING. The data that would be the basis for historical and perspective that we were just talking about is not identical in its precision, nor is it identical in the way that it's collected, so I'm not sure we're comparing apples and oranges. But of course whether somebody is being tracked in real time going forward has historically been recognized as something that is more intrusive than looking at a historical view of somebody's activities.

Mr. LIEU. I completely don't understand that distinction. I think it is stupid and meaningless. So, Ms. Guliani, can you elaborate on that distinction?

Ms. GULIANI. We also don't believe that there should be that distinction between historical and real-time data. You know, as one judge put it, the idea that something is less intimate because you're looking at a picture that's already been painted just simply isn't accurate.

It's also important to note that courts recognize that there are areas where you're entitled to enhanced protection, for example, in your own home, and historical data captures whether you're in your home, how often you're in your home, when you leave your home. And given the accuracy of historical data, and we anticipate that it's only going to become more accurate, we believe that it should be treated with the sensitivity it deserves and a probable cause warrant should apply.

Mr. LIEU. Thank you. Mr. Larkin, what do you think about that distinction?

Mr. LARKIN. It depends whether you're talking about it as a matter of law or policy. As a matter of Fourth Amendment law, there's probably no distinction between past data about a person and present data. The Fourth Amendment would not require a search warrant or probable cause in either case. But if you're talking about the effect of privacy, then, yes, it can be the same in both cases.

See, the Fourth Amendment treats not past and present as the distinction. It treats—it makes the distinction in other ways, between protected areas and non-protected areas. If you are on a city street, the Fourth Amendment would allow the police to see what you're doing and follow you, whether they've done it 100 times in the past or are doing it now. If you're in your home, that's a protected area and that's different.

Mr. LIEU. Thank you. Mr. Downing, can I see this super-secret memo or only the chairman and the ranking member?

Mr. DOWNING. Let me say that the Department has great respect for the needs of this committee and wants to work towards developing—giving the information that's required. Of course, at times there are going to be situations where the content of documents has the effect of inhibiting the kinds of things that we do such as by giving criminals warning about the types of activities that we might use to investigate them and also to reveal the litigating positions of the Department, which is an important internal deliberation.

All that being said, as the chairman and ranking member announced, we seek to seek an accommodation with the committee to get the committee the information that it needs, and so I under-

stand that our Office of Legislative Affairs has worked out a compromise that we're going to try to pursue at this point.

Mr. LIEU. Mr. Chairman, could I have 15 seconds to respond?

Chairman CHAFFETZ. Sure.

Mr. LIEU. I fully trust Chairman Chaffetz and Ranking Member Cummings. I just want to note that the message you're sending to me and other members of this committee is you don't trust us. I find that offensive, disrespectful, and it will affect my dealings with the Department, maybe other members here in their dealings with your department on an ongoing basis.

And I yield back.

Chairman CHAFFETZ. I thank the gentleman. I now recognize the gentleman, Mr. DesJarlais from Tennessee, for 5 minutes.

Mr. DESJARLAIS. Thank you, Mr. Chairman, and thank you, panel.

As you all know, the Fourth Amendment provides the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, in other words, protection against unreasonable government search is a fundamental right.

Mr. Downing, as the courts have made clear in their rulings, all evidence that is obtained through an unconstitutional search is inadmissible in court. Would this exclude all the tracking information, even the information obtained where the suspect had no reasonable expectation of privacy like driving on public roads?

Mr. DOWNING. So the constitutional suppression would only apply to that information that is indeed protected by the Constitution. So if a court found that the information was not implicating the Fourth Amendment, then constitutional suppression would not apply in that situation.

Mr. DESJARLAIS. Okay. So then what are some examples of situations where a warrant would not be necessary when placing a GPS on a vehicle?

Mr. DOWNING. There might be situations that come up where there is a life-and-limb emergency, for example, where the courts have long recognized that the warrant requirement doesn't apply. So, for example, in that situation law enforcement officers could search a house without a warrant because of the immediate need. Those kinds of exceptions would apply also in the case of tracking devices on vehicles.

Mr. DESJARLAIS. Mr. Lieu touched on this a bit. What should be the legal standard for historical geolocation information?

Mr. DOWNING. I'm sorry, was that question to me or Mr. Doucette?

Mr. DESJARLAIS. Yes. Yes, sir.

Mr. DOWNING. I apologize. Historical location information?

Mr. DESJARLAIS. Yes, what should be the legal standard for historical geolocation information? In other words, why would you have less privacy interest in where you were last Saturday than where you will be next Saturday?

Mr. DOWNING. So the Department's position is that historical cell-site information does not require a warrant, and three circuit courts have agreed that that's the case. The reason that it is different is that it is less precise in general, that it is a business

record collected by the company, that it is not continuous but only recorded when communications occur. And so for all of those reasons, it's a different category of information than, say, real-time GPS information that's collected prospectively. For that reason, the courts have recognized that that does not have constitutional protection.

Mr. DESJARLAIS. How far can law enforcement go back, a year, 3 years, 5 years?

Mr. DOWNING. The amount of time that you could go back would depend entirely on the record collection and retention practices of the company because these are company records that are not mandated to be stored. It's a choice that the companies make. And so it's variable. Some go back for a short period of time, others for longer.

Mr. DESJARLAIS. Ms. Guliani, would you like to comment or share your opinion on those issues?

Ms. GULIANI. Sure. You know, as I mentioned before, we believe this distinction between real-time and historical information is artificial and not just because of the increasing accuracy of cell-site information but also because of the very real privacy interests that Americans have in protecting the fact that they've been to an AA meeting six times in the last week or the fact that they only sleep at home 5 out of 7 days a week.

With regards to historical cell-site information and the time period that providers keep that information, in some cases that can be close to 5 years, for example, in AT&T's case; with Sprint, 18 to 24 months, and that's incredibly intimate information about someone's life. And given this, we believe that a probable cause warrant, the same standard that would apply if law enforcement wanted to read a letter of yours, is the correct standard.

Mr. DESJARLAIS. Mr. Downing, do you agree with that?

Mr. DOWNING. With all due respect, I do not agree. The reason that the—this information is different—first of all, let me say we respect that it is private information, and we believe that it should be protected. We believe it is protected. The Electronic Communications Privacy Act already creates rules. It's not at a probable cause standard, but nevertheless, it is quite protected and not instantly available to law enforcement whenever it chooses.

We have analyzed, though, the constitutional rules here and have taken the position that the Constitution does not require a probable cause standard for the reasons that I explained before.

Mr. DESJARLAIS. Ms. Guliani, do you agree with that?

Ms. GULIANI. Respectfully, we disagree, and there are many courts that have recognized that historical information is extremely sensitive. For example, a Fourth Circuit opinion that is waiting en banc review where the court found that historical cell-site information was sensitive and should be provided a higher standard.

I think it is important to note that States across the country have recognized this, have recognized the sensitivity with which Americans view this information and have on their own adopted, you know, in many cases by nearly unanimous votes in their State Legislatures, legislation that protects historical and real-time cell-site information.

And given this trend, both at a State level and both in terms of the American view of this information, we feel that this is a case where it's ripe for Congress to make clear that this information should be afforded a higher level of protection through legislation and by pressing the Department to change its policies and its position.

Mr. DESJARLAIS. Thank you both for your time. I yield back.

Chairman CHAFFETZ. I thank the gentleman.

I will now recognize the gentleman from Pennsylvania, Mr. Cartwright, for 5 minutes.

Mr. CARTWRIGHT. Thank you, Chairman Chaffetz.

The first thing I want to do is I want to clarify something. It was heard in this room not 10 minutes ago that it was a great revelation about stingrays being used by the IRS. Please do not be misled by that. It was not a revelation this month. This committee was briefed on stingrays back in November, November 12, 2015, by Richard Weber, the chief of the Office of Criminal Investigation, and also has received at least two briefings, one in January of this year and one in November from the Department of the Treasury from TIGTA on the use of stingrays. So anybody claiming this is a revelation wasn't showing up for the meetings.

I want to talk about geolocation, the legal standard. Ms. Guliani, law enforcement currently has the ability to obtain geolocation data through the use of a valid court order. Law enforcement relies on legal authority provided in the Stored Communications Act to obtain an order compelling a service provider to disclose cell-site location information. These orders call for specific and articulable facts showing that there are reasonable grounds to believe that the cell-site information is relevant and material to an ongoing criminal investigation.

There has been disagreement in the Federal courts over whether this is the proper standard, and some Federal courts have decided that there is an expectation of privacy in cell-site location information, and they have imposed stricter requirements for law enforcement to obtain the information.

I wanted to ask you, what is the impact of a lack of a uniform standard governing access to geolocation information?

Ms. GULIANI. There are very practical impacts. I mean, I think the first and foremost is the reality that many Americans' information may not be adequately protected. So if you happen to live in a State that has not passed a law protecting information, law enforcement may be able to access your information under a lower showing.

And I think that, you know, the Supreme Court has recognized, courts have recognized that the Fourth Amendment is important not just to protect people's privacy but also for freedom of expression, freedom of association. You know, the idea that law enforcement may be able to track your every movement could chill, you know, the desire of someone to go to a protest, to visit their psychiatrist. And these are very real effects and the reason why we believe that it's so important that a high standard apply when law enforcement collect this information.

Mr. CARTWRIGHT. Thank you for that. And I want to shift over to you, Mr. Downing. Do you agree with that?

Mr. DOWNING. We do not agree. We think and have taken the position in litigation that it is appropriate to have that lower standard and that the—although it is lower than probable cause, it is not a no-standard. There is in fact a lot of protection that is built into that. The reason that it's particularly important, however, is that, as mentioned in—before, the early stages of investigation can certainly benefit from the ability to get this sort of information at a time when we don't have probable cause, and so there is a real cost to the public and to the solving of crimes and seeking justice if the standard were to be raised.

Mr. CARTWRIGHT. Not to interrupt you, but I'm not asking about the level of the standard. I'm talking about the uniformity of the standard. What do you believe the impact of the lack of a uniform standard has been?

Mr. DOWNING. I don't see an enormous impact as a result of the lack of uniformity. In the law, we often see circuit splits and differences from one part of the country to another. We have to deal with that as law enforcement officers and as prosecutors, and so we need to follow the law in our local area. Usually, those differences of opinion get worked out and we come up with a consistent standard in due course.

Mr. CARTWRIGHT. Well, Mr. Downing, are you aware of any instances in those States that the warrant requirement impeded their efforts?

Mr. DOWNING. I'm not aware of which States have them and which don't, nor do I have any information for you on that.

Mr. CARTWRIGHT. Mr. Doucette, the State of Virginia currently requires a warrant for real-time tracking. Am I correct in that?

Mr. DOUCETTE. That is correct.

Mr. CARTWRIGHT. And what has been the experience in Virginia?

Mr. DOUCETTE. It's been our experience for real-time tracking that we do generally have—we have the probable cause. We had the probable cause before, and that's why—if we are looking where somebody is right now, we have reason to believe, we have probable cause to believe that they are involved in a particular criminal activity. It's ——

Mr. CARTWRIGHT. How would law enforcement practices change if a higher legal standard were uniformly to be adopted?

Mr. DOUCETTE. And I think we've mentioned this, both Mr. Downing and I, is that it would have a severe impact as far as the criminal justice and the criminal prosecution provisions where we're using this particular information to aid us in this particular investigation.

And I realize this is not directly an answer to the question, but Ms. Giuliani—Guliani has raised an issue about a particular case in the Fourth Circuit, United States v. Graham, which is coming up for an en banc hearing. As I understand the majority opinion in that particular case, it wasn't that they were using historical cell tower information without a probable cause determination. It was the amount of time that went on. It was 221 days that they were using this court-ordered information. And so it wasn't 1 day or 2 days. That would have been fine under the ECPA standard. It was the 221 days, and that's what's ——

Mr. CARTWRIGHT. Thank you for that. And I just want to give Ms. Guliani just a few moments to respond to that.

Ms. GULIANI. Mr. Doucette is right. In that case there was a long amount of time, but I think it's important to note that the Department of Justice's position is that even for a lengthy period of time, even for 5 months or 6 months, a warrant would not be required for historical information, and that is not consistent with what some courts have—the way some courts have assessed this issue.

But like I said, this issue is still pending in many courts. There's not uniformity among States and among courts. I mean, it's for that very reason that it's so important that we develop a uniform policy and legislation that addresses this important issue and ensures that what law enforcement is doing comports with the Fourth Amendment. And our view is that the Fourth Amendment protects Americans against law enforcement getting their information unless there is appropriate cause, and in this case, that cause is probable cause, which is a standard, but it's not a standard that is different from what law enforcement applies in a variety of circumstances when investigating many serious crimes.

Mr. CARTWRIGHT. Understood. And I yield back, Mr. Chairman.

Chairman CHAFFETZ. I thank the gentleman.

I now recognize the gentleman from Kentucky, Mr. Massie, for 5 minutes.

Mr. MASSIE. Thank you, Mr. Chairman.

Ms. Guliani, in your opinion, should Congress act now or wait for the Supreme Court to decide this issue?

Ms. GULIANI. I think that Congress should act now. We don't know when or if the Supreme Court will take this case. It could be 5 years or 10 years. And candidly, in many cases are—legal cases have lagged behind technology.

And we're at a point where location information is becoming increasingly more accurate and is being collected by a wide variety of parties. Smart cars, smart medical devices, we're fairly close to having information about our location collected by these third parties. And given this, it's—we believe that Congress can protect the rights of Americans ensuring that location information is afforded the high level of protection and do so in a way that is reflective of our current technological realities.

Mr. CARTWRIGHT. Same question, Mr. Larkin. Should we wait for the Supreme Court to decide this issue or should we pass legislation?

Mr. LARKIN. You should not wait. You should look into the facts and then address the issue. In the Jones case, for example, the beeper was placed on the vehicle in 2005. The Supreme Court didn't decide the case until 2012. You can decide things a lot faster than it took the Supreme Court to resolve that issue.

Secondly, whatever you decide I think would be well received by the Supreme Court. Justice Alito, for example, in his concurring opinion almost pleaded with Congress to address this issue and let it pass from the Supreme Court. The same thing has happened in all the other cases where Congress has addressed electronic acquisition of information. The Supreme Court has been very deferential realizing that Congress can balance considerations and has access to data it does not have.

Mr. MASSIE. This is a larger question but I know that Heritage speaks to this question. Doesn't Congress lose power to the other branches when it abdicates its responsibility to legislate on these issues?

Mr. LARKIN. It depends on what the particular issue areas, but the general answer is yes. Power not used tends to wither, and then when you try to use it later, you have a long line of precedence that people tend to point to to say that you no longer have this power; you've passed it on to somebody else.

Mr. MASSIE. Right. That is what the late Justice Scalia told me, in fact.

Mr. Downing, when we vote on this issue and legislate and amend this legislation, how many of us in the House of Representatives are going to be voting on this?

Mr. DOWNING. I'm sorry, I don't understand your question.

Mr. MASSIE. How many Members of the House of Representatives are eligible to vote on this issue?

Mr. DOWNING. I believe it's 435. Is that ——

Mr. MASSIE. That is correct, 435. So why would you share the post-Jones memorandum with only two? I mean, ostensibly, whatever we legislate is going to have a profound effect on how you are allowed to interpret these issues. So why wouldn't you want Congress to be informed?

Mr. DOWNING. Congressman, we very much do want to have Congress be informed and want to respect the need of this committee to have the information that it legitimately needs to make its decisions. However, there are certain circumstances where particular memos contain information that if it were released publicly or—it would be detrimental to the ability of us to do our jobs. And so we seek to try to find some accommodations to allow for ——

Mr. MASSIE. Let me just echo ——

Mr. DOWNING.—that ——

Mr. MASSIE.—what Mr. Lieu said. This breeds mistrust when you don't trust Congress, and we are trusted with many other secrets of national importance, and I think the people's representatives, if not the people, at least the people's representatives deserve to know how the laws are being interpreted and how they are going to affect them.

And I would remind you that there are also 435 of us vote on your budget as well.

Mr. DOWNING. Thank you. We have actually done a lot to try to provide and answer any questions that the committee may have as a result of that. We've provided our public positions, which really go through all sorts of the positions that are relevant to these decisions. I've also briefed staff and answered all of their questions. We're really trying very hard to give the information to the committee that it ——

Mr. MASSIE. I would like you to try a little bit harder and give me that post-Jones memorandum.

Should it be legal to turn off precise geolocation on a phone, Ms. Guliani?

Ms. GULIANI. You in fact cannot turn off precise geolocation on your phone. Under FCC rules, all cell phones must have the ability

to have GPS information. The idea of this was to provide the ability for emergency personnel ——

Mr. MASSIE. 911, yes.

Ms. GULIANI.—to access you. But this information is routinely provided to law enforcement, and based on new regulations that the FCC has put out, they've asked carriers to increase the accuracy of this information so they can be able to assess, you know, what floor of a building you're on.

Mr. MASSIE. You know, I remember in the early 2000s I was in the tech industry and went to a factory to get something manufactured, and they were too busy. They were retooling all the cell towers so that all of your phones could be tracked. And it was under a mandate that presumably Congress issued. And it strikes me if this data didn't exist, we wouldn't be having this issue, or if a person had the right to turn that off. And you could see how it could easily work with a microcell where, you know, you plug this element into the Internet and then your cell phone works magically wherever the internet is, but I know that it won't come on until the GPS finds a signal.

Because of what we have done here in Congress, you are not allowed as a consumer to make a phone call unless the government is able to find out where you are. And we did all that under the pretext of safety.

So, you know, one of the suggestions I would have, Mr. Chairman, is giving some exemption to that law, allowing people to have privacy because we are saying, well, it is not private when you share it with a third-party, yet we are not even allowing you to make the phone call without sharing it with the third party. So with that ——

Chairman CHAFFETZ. I thank the gentleman.

Mr. MASSIE.—I thank you. I yield back.

Chairman CHAFFETZ. I now recognize the gentleman from Massachusetts, Mr. Lynch, for 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman.

Let me say at the outset that, absent any compelling reason, I would side with the chairman, Mr. Chaffetz, and Senator Wyden in requiring your reasonable cause a standard for this type of intrusion. And it would help your case, as Mr. Massie has laid out, if more members of this committee and if Congress had access to those memoranda that state your case. You are going to need it, I think.

One of the differentials we have here is that Congress continues to move at a very slow pace, whereas the velocity of change in the areas of technology is breathtaking. Anybody with a 16-year-old daughter understands that, you know, cell phones are part of our personal effects now intimately and that the network of cell towers, it really does, as one of the courts described, provide a mosaic of a person's personal and private life.

And I think it was not a recent case, Katz v. United States, that says the Fourth Amendment doesn't just protect places, it protects people. And with the advent of wearable technology, you know, the iPhone is connected to your cell phone. It is paired, so it really is—you know, technology has really permeated our private life.

One of the things I can't get beyond is in other areas of surveillance for the Department of Justice, let's take the Foreign Intelligence Surveillance Act, we require in the FISA Court that the Department of Justice provide probable cause that a person is an agent of a foreign power or acting on behalf of a foreign power. So we require you to prove—to make probable cause in that case. Why would we provide a lesser standard for good old American citizens when the consequences, you know, are not regarding terrorism or, you know, imminent threats?

Mr. DOWNING. I can't speak to the FISA side of the House. That's not ——

Mr. LYNCH. We can though. We oversee FISA.

Mr. DOWNING. Of course.

Mr. LYNCH. Yes.

Mr. DOWNING. But I want to emphasize the way that this works is that there are many different kinds of location information. Certainly, if the access were to really precise information like the GPS information that's on the chip that was just being discussed were accessed by the Department of Justice in order to track someone and follow them around, we would indeed use a warrant for that.

Mr. LYNCH. Let me just reclaim my time because I think you are going to use it all up. But you have access to all of that and without proving probable cause right now. And so while you sort that all out, let me give you another example. In the FISA instance, Foreign Intelligence Surveillance, if there is a critical, urgent need, we allow the Department of Justice, the FBI to go out in the first instance and actually conduct that surveillance if the judge is going to be shot or, you know, there is an emergency situation. In the short term we allow them to go forward with that surveillance, but immediately, immediately, they have to go back to the FISA Court and ask to verify that surveillance and to legalize that surveillance under a standard of probable cause.

So they are allowed to make the surveillance, but they have got to be in front of that FISA Court as soon as practicable, and they will be judged on their action by probable cause. Why would we not have that for instances that you engage in with respect to American citizens?

Mr. DOWNING. The answer to your question, I think, is that there are different kinds of information. Some of it is more protected and more sensitive and more ——

Mr. LYNCH. Yes, I know that. You are going back to the same point again, but we have an opportunity here for probable cause for you to make your case in each and every instance. I just don't buy it.

We have had plenty of investigations here of the FBI acting illegally with respect to the Boston ops of the FBI. We have had other situations where the FBI has overreached with, you know, confidential informants. So the trust—and, look, you know, I know they are cleaning up their act, they are doing a good job, but we have had too many instances where government agencies have overstepped their bounds, and I think that Mr. Jordan's point about the IRS, you know, is probably a very strong example of why we should require reasonable cause.

Mr. DOWNING. Well, the answer, I think, though ——

Mr. LYNCH. Probable cause, excuse me.

Mr. DOWNING. If I may be allowed to respond is there are situations like the judge shooting case where we don't have probable cause. That is, we have suspects that are in the case. We'd like to be able to include them or exclude them so as to guide the investigation, but we just don't have probable cause at that stage. It's an early stage of the investigation, and having the necessary building blocks to build to probable cause is necessary. That's why we think having ability to gather information about the lesser standard, the lesser protected stuff is actually very important.

Mr. LYNCH. All right. I clearly disagree, but thank you.

I yield back.

Chairman CHAFFETZ. I thank the gentleman.

I would now recognize the gentleman from North Carolina, Mr. Walker, for 5 minutes.

Mr. WALKER. Thank you, Mr. Chairman. Thank you, panel, for being here today.

My colleague from Kentucky just a few minutes ago in the discussion, I believe you said that part of the problem is that you can't release this information publicly, to use your words. Congress isn't public.

You also said that you and your staff have answered questions from the committee, but I would like to go back to last October on a question that we are still waiting for. In fact, it was asked by me in asking the representative from DOJ on whether cell-site simulators to collect the content of information or communications. Are you doing that before implementing its internal policy requirement warrants for the technology that you implemented in September, a month earlier?

Mr. DOWNING. I'm sorry, if I understand correctly, are we requiring warrants to be used in following of the policy, is that correct?

Mr. WALKER. That is correct, yes. The witness said she was not aware of this but would get back to us.

Mr. DOWNING. We do require warrants except under those rare situations where there's an exception like life-and-limb emergency.

Mr. WALKER. Okay. So how many cases did you guys obtain a warrant before collecting this content?

Mr. DOWNING. I don't have exact numbers for—well, first of all, I would disagree whether it's content or not, but I don't have exact numbers. But the policy does require the collection of that information, and so we should be figuring that out as we go forward.

Mr. WALKER. All right. So from your perspective as far as you know, when you implemented this new policy, you guys, you are telling me, on all the components that you captured, collected or the communications that you retained, there were warrants issued in that process?

Mr. DOWNING. If I'm understanding you correctly, after the policy went into effect, are we using warrants? Is that the question?

Mr. WALKER. That's correct, yes.

Mr. DOWNING. Yes, except under those rare circumstances where the policy has an exception.

Mr. WALKER. Okay. All right. Fair enough. Thank you for answering that.

Mr. Larkin, I have a question for you. In your testimony you referenced three reasonable arbitrary lines that Congress can draw to better protect Americans. Your second suggestion was to impose a warrant requirement if, after a reasonable period of time has elapsed, the government still has a legitimate need for this geolocation information. Other than the two areas you mentioned, intelligence and non-law-enforcement interests, my question is this: Why should law-enforcement not be required to obtain a warrant from the onset for the geolocation information?

Mr. LARKIN. There may be instances, as my panel member colleague said, where you can't satisfy probable cause but you can satisfy reasonable suspicion. I think one thing that hasn't been adequately explained is that there is a material difference between the two. It's very difficult to try to put percentages on how right you are when you're deciding whether it is probable cause or reasonable suspicion, but it's clear that reasonable suspicion is far lower.

Mr. WALKER. And you would build me a case of when you would say a warrant is not needed here but there is reasonable suspicion. Give me a sample situation, Mr. Downing or Mr. Larkin. What would that look like?

Mr. LARKIN. Well, I think his example of someone who is shot and you want to see, for example, based on the people who have a motive to do it, who had cell phones in that area. You don't have probable cause to believe that any one of the perhaps dozen people actually committed the crime, but you know that there are 50 people that hated someone and you want to find out how many of those 50 were in a particular area. So you find out that information. Now, you have something that you can work on that you never would have gotten if you didn't—if you had a probable cause requirement. And then you can go from there.

I mean, one of the—I mean, one way to try to balance this out is to have only reasonable suspicion requirement for a limited number of days at the front, and then after a certain period of time, if you thought that privacy interests demanded a probable cause showing, the probable cause showing would come into play only after a certain number of days. That would allow somebody to try to accommodate the privacy and law enforcement.

Mr. WALKER. Mr. Downing, do you want to follow up on that same idea as far as what situations, what conditions, sample-wise? Would you say you wouldn't need a warrant because there is probable cause?

Mr. DOWNING. Actually, Mr. Larkin's explanation is far better than mine. That's exactly the kind of situation. We also have certain cases where, as another one was mentioned in my testimony, written testimony, where we just don't have probable cause yet. We have scattered pieces of information, and if we could get that extra bit of information, it might put us over the line and be able to figure out who the person is that was responsible. So it does come up, and that's going to be the burden if that source of information is offered.

Mr. WALKER. Thank you, Mr. Chairman. I yield back.

Chairman CHAFFETZ. I thank the gentleman.

I now recognize the gentlewoman from Illinois, Ms. Duckworth, for 5 minutes.

Ms. DUCKWORTH. Thank you, Mr. Chairman.

Appropriately balancing the privacy interests of Americans against need of law enforcement is of great concern to me. I really feel that it is a responsibility for Members of Congress to provide the oversight for government interactions in the daily lives of the American citizens. While I agree that a person's interests and privacy is compelling and that it should be respected, I also cannot ignore the compelling interests of law enforcement to obtain information necessary to conduct criminal investigation.

Mr. Downing, the collection of cell-site location data implicates both, and we have talked about this. Can you talk a little bit—you know, if there is no uniform standard for how we collect this information, does the Department have a different standard for whether the geolocation information can be obtained depending on where the target is located?

Mr. DOWNING. I'm sorry, I'm not sure I understand "where the target is located." You mean in what part of the country?

Ms. DUCKWORTH. Or situation that they may be located in. And do you have—because there is no uniform standard, it makes it very hard to sort of pin down what we are trying to do here.

Mr. DOWNING. Well, of course, before the cell phone company were to disclose that information to the investigative officer, we're not going to know necessarily where that person is. In fact, that's kind of the goal of what's going on. So it wouldn't be possible to in advance say, well, we only want information about the location if it's in a certain context or otherwise. Does that answer your question?

Ms. DUCKWORTH. It does, but is there any effort or any usefulness to some sort of a minimum uniform standard as you are trying to move forward with this?

Mr. DOWNING. Well, I think the law already provides for a minimum standard. Under the Electronic Communications Privacy Act, for example, we would have to obtain a court order with a specific-and-articulable-facts standard. So when we're speaking of historical cell-site location information in particular, it is very much the case that it is not unprotected; it's simply not quite as protected as other types of information which require a probable cause standard.

Ms. DUCKWORTH. Okay. So then let's talk about once you get the information. Does the Department have a consistent practice for how geolocation information is treated once it is collected? And, you know, specifically describe how that information is handled once it has been collected. If there is not a standard for what you can get, at least is there a standard for what you do with it once you get it?

Mr. DOWNING. So the Department investigators, of course, encounter all sorts of very sensitive and private information from—personally identifiable information about people, their financial information, perhaps their medical information. So we very much respect the need to protect that information, to keep it safe and protected from disclosures—improper disclosures and so that it's used only for the official purpose for which it's collected. So site location information and other location information is treated similarly with due care to make sure that it is not inadvertently disclosed.

Ms. DUCKWORTH. Mr. Doucette, does your jurisdiction have similar safeguards in place when these kinds of data are being collected?

Mr. DOUCETTE. Mr. Chairman, Ms. Duckworth, the—in Virginia, in order for us to have real-time location data, we do have—we do require probable cause there, and we do require a search warrant. At this point in time, given historical cell tower information, our standard is that of what is required by ECPA, that there be a reasonable standard—reasonable and articulable standard before we can obtain that information through a court order. And it's not that we just go and say, okay, we've made the determination that we have reasonable—probable—an articulable suspicion and therefore, phone company, give us this particular information. We have to take that information before a court and the court has to say, yes, you do or no, you don't. And we've had these particular orders refused by courts when they say you haven't even risen to the level of reasonable articulable suspicion. So those are our standards in Virginia.

Ms. DUCKWORTH. What I am concerned with is we have clear standards for how we treat physical evidence, but when you are talking about data that is gathered electronically, are there clear standards for how we handle that data, how it is tracked, how it is recorded, how it is shared, how it is preserved, when is it destroyed, all of that? Are there standards for the electronic data not necessarily in the same manner as physical evidence but are there standards? And either one of you can address this.

Mr. DOUCETTE. Are there standards? If I understand your question correctly, are there standards as—once we receive that information, how ——

Ms. DUCKWORTH. Yes, once you have the data, how do you—do you safeguard it in the same way you safeguard physical evidence of a crime?

Mr. DOUCETTE. Obviously, we have discovery obligations, we have exculpatory evidence obligations that we do have to provide to defense counsel, and we take those quite seriously. And so we do disclose that particular information. How it gets disclosed from defense counsel from then on, I have no way of controlling that. I do not release it out into the general public.

Ms. DUCKWORTH. Is it available to be mined by other people on other cases that may be unrelated? Do you see what I am trying to get to?

Mr. DOUCETTE. I may or may not. I mean, any information that I release in open court, obviously, anybody is allowed to be in court and say, okay, this particular person's phone was in this particular location at that particular point in time.

Ms. DUCKWORTH. I guess what I am saying is, for example—and I am sorry, Mr. Chairman, I am over time. May I just follow a little bit ——

Chairman CHAFFETZ. Go ahead. Finish the question.

Ms. DUCKWORTH. So the question is if you get the data that you want that Mr. Larkin was mentioning, we want to know how many guys were in the vicinity of a crime that happened, and you get the data for this particular investigation and it takes place, what happens to that information? Is it just sitting there for other people to

come back and see who all else was there at that point in time later on, or is that evidence only used for that particular instance? I am worried that there are not ——

Mr. DOUCETTE. Yes.

Ms. DUCKWORTH.—safeguards and standards in place for how that information, now that you have it, is safeguarded and used in the future.

Mr. DOUCETTE. Mr. Chairman, ma'am, the answer under Virginia law is none of my files are subject to FOIA. Everything is considered a criminal investigative file under our State Freedom of Information Act, and so no one can have access and say—hit me with a FOIA request and say what-do-you-have sort of thing. I do have an obligation, however, for discovery purposes and exculpatory evidence purposes to turn over to defense counsel. I do have a—obviously, whenever I present in open court as far as evidence is concerned, anyone is allowed to be in that open court and hear what evidence we present. But that is the only way they would have access to the information that we're gathering.

Chairman CHAFFETZ. I thank the gentlewoman.

And to the gentlewoman's point, part of the issue is Virginia, Utah, there are very few States that actually have these things in place, and then you have agencies outside of the Department of Justice that have this tool such as the IRS. And nobody knows what they are doing with it, and that is the point.

I will now recognize the gentlemen from Georgia, Mr. Hice, for 5 minutes.

Mr. HICE. Thank you, Mr. Chairman.

And I really appreciate this hearing and what we are discussing today. And I share with my colleagues a great deal of concern with what we have seen in the past of abuse of government and the Fourth Amendment and the concerns that have been brought up today, I think, are extremely valid and need answers.

I would like to go a little bit more on a bit more of a practical direction at this point and, Mr. Larkin, ask you a couple of questions. Could you expand on the differences between the step-by-step traditional Fourth Amendment analysis and mosaic theory?

Mr. LARKIN. Sure. Mosaic theory is like a Rorschach test. You look at the entire picture and see if the entire picture is reasonable. And in deciding whether it's reasonable, one of the things you take into account is the amount of information that you acquire. If all you're doing is looking at someone over the course of one day, you may get a very different answer than if you look at it over the course of 30 days. Twenty-eight days was the number of days that was at issue in Jones, and the concern was you got a lot more information following somebody for 28 days than one, which is absolutely true.

If you look at it, however, the way matters normally have been looked at, you look at each step in what the government does, analyze each one separately, and if each one separately is lawful or justified, then you don't worry about what happened at steps 1 and 2 when you're looking at step 3, and you don't worry about what happened at step 3 when you're looking at step 10. You don't ever step back and do the sort of Rorschach analysis.

The problem for a court is in drawing the line. You have to draw an arbitrary line. You have to say 2 days is enough, is okay, 20 days is too much. And you have to then figure out where between those two. Congress can do that. Congress can draw arbitrary lines by deciding that at a certain point you cannot—you can go up to a certain point based on, say, reasonable suspicion or based even on no justification at all. But we're concerned after that so we're going to cut it off at whatever day you choose, 3, 7, or 10.

Mr. HICE. Is it a fair assumption to believe that you believe Congress should make that determination?

Mr. LARKIN. Yes.

Mr. HICE. Okay.

Mr. LARKIN. Now, you could leave it just at reasonable suspicion throughout. That's what the Department is doing now, I think, with the exception of the policy.

Mr. HICE. But it is fairly vague at that ——

Mr. LARKIN. But there is a material difference between reasonable suspicion and probable cause. The latter is much more serious. So one way you could balance this law enforcement and privacy interest is to have a cutoff period.

Mr. HICE. Okay. Well, let's go with reasonable cause. From my understanding of this whole third-party doctrine issue, I believe you mentioned earlier, has been affirmed by the courts for decades now. But as we all know, since then, technology has changed drastically. People use email now more than they do the Postal Service, for example. So in a time like this where technology has evolved so much, do you believe that the bar for reasonable cause for privacy has it changed or should it have changed?

Mr. LARKIN. I wouldn't say that the way you define reasonable suspicion should change. What I would say is that at a certain point you may want to say that's insufficient and that you need probable cause because I don't think you want to change the standards themselves, but you may decide that at a certain point a reasonable suspicion standard allows you to accumulate so much information, you're violating the privacy of people involved.

Mr. HICE. Okay. But from a technological perspective, how do you see the changes in technology where we are all walking around with our smartphones, our emails, as opposed to 30, 40, 50 years ago? It was through the mail or other means. How has the changing of technology, do you believe, has it altered or should it have altered the bar as it relates to reasonable expectation?

Mr. LARKIN. There's no doubt that it has, and the reason it has is, as was pointed out in, I think, Justice Alito's opinion, practicality was a basic limitation on the ability to acquire evidence in the past. Now, if you had 10 people in your police department, you couldn't do the same sort of intensive surveillance that you could if you had 10,000 people in your police department. The NYPD can do a lot more than a very small police department can, and those sorts of practicalities were to some extent, I think, factors that courts considered in deciding how far the Fourth Amendment should go. You could say that they balanced the two to some extent.

Unfortunately, the historic limitation that practicality imposed no longer is with us because the ability to collect and analyze infor-

mation has so superseded the ability of any individual to do either of those that it may be necessary to reexamine the entire area.

Mr. HICE. Okay. Well, thank you very much, and I yield back. Thank you.

Chairman CHAFFETZ. I thank the gentleman.

I will now recognize the gentleman from North Carolina, Mr. Meadows, for 5 minutes.

Mr. MEADOWS. Thank you, Mr. Chairman, and thank each of you for your testimony.

I find myself in a very difficult spot. I don't know that I have on many occasions ever agreed with the ACLU, and I don't know on many occasions that I have ever gone against law enforcement, and yet this fundamental question that we are here today addressing is, Mr. Downing, very troubling because of the expectation of privacy and what foundationally is what all Americans presume that they should enjoy.

And so I guess under what scenario can you justify not sharing with Members of Congress the Jones guidance? And let me caution you because I go into a skiff here and I see all kinds of national security secrets that I am not allowed to divulge, and yet somehow your Jones guidance would supersede our nuclear capability in terms of my ability to see a memo.

Mr. DOWNING. As I said before ——

Mr. MEADOWS. Is it more important than our nuclear capability?

Mr. DOWNING. The Department is very much interested in providing whatever information the ——

Mr. MEADOWS. So you are going to provide to all the Members?

Mr. DOWNING. At this point there are, however ——

Mr. MEADOWS. Because having an interest and doing something are two different things, Mr. Downing. So are you going to provide to the Members of Congress? I can see all kinds of national security secrets, some that you may not even get to see.

Mr. DOWNING. We are seeking to do an appropriate accommodation with the committee ——

Mr. MEADOWS. Appropriate according to who?

Mr. DOWNING. Mutually appropriate accommodation to the committee ——

Mr. MEADOWS. Well, we think is appropriate that the entire committee should be able to see it, so ——

Chairman CHAFFETZ. If the gentleman will yield?

Mr. MEADOWS. Yes.

Chairman CHAFFETZ. I don't think we should be treated any different than every other Member of Congress. I have been fighting this for years. And even though we are grateful, it is amazing to me that I have to negotiate as a Member of Congress, as a chairman of the committee, as someone that serves on the Judiciary Committee to an accommodation—I mean, part of this deal is we are not supposed to take notes, we are not supposed to do certain things. What? What? Seriously?

The reason I have resisted every other gesture thus far is because of all these conditions. I shouldn't have to have a condition. I represent 800,000 people. They trust me to go in in this republic, and look at this information and keep it confidential, that we sign oaths, we abide by the law. If we don't do that, then you should

prosecute us. But we see, as Mr. Meadows said, some of the most sensitive information that you can possibly have, but the guidance on post-Jones is somehow so sacred that thus far you are only granting two out of 535 people to go see this? It seems very inconsistent.

I am sorry. I yield back to the gentleman.

Mr. MEADOWS. You go ahead. You can comment.

Mr. DOWNING. It's not really a matter of trust. I think that's not the right way to think about this. The Department has confidentiality needs in things like the way—the positions that we're going to take. We're also worried that disclosures of one sort will be regarded later by a court as a waiver of a privilege as well. So there's a number of factors that go into this consideration.

Mr. MEADOWS. But it is a matter of trust because if you are saying that you can't—I mean, because we are protected in that. If Members of Congress—maybe not our staff, but Members of Congress would be protected.

But let me go a little bit further because what you are saying is reasonable suspicion is enough to be able to use this, is that correct, in some cases?

Mr. DOWNING. For the historical cell-site information, yes ——

Mr. MEADOWS. All right. So is it ——

Mr. DOWNING.—we've been very public about that.

Mr. MEADOWS. Is it okay for the IRS to use reasonable suspicion as their guidance?

Mr. DOWNING. If what we're talking about is historical cell-site information, they would have the same rules as all the other law enforcement agencies, yes.

Mr. MEADOWS. All right. So let me ask you is when we have had this whole Lois Lerner thing, and I don't normally harp on that, but they had reasonable suspicion according to them—according to DOJ they had reasonable suspicion. So what you are saying is they could use a stingray for every single group that they had out there that was asking for 501(c)(4) status?

Mr. DOWNING. I don't have any ——

Mr. MEADOWS. Well, that is what they are saying.

Mr. DOWNING.—responsibilities ——

Mr. MEADOWS. It was DOJ that we actually had a hearing the other day, so that is troubling to me that we would do that. Wouldn't it be troubling to you?

Mr. DOWNING. I think there should be a consistent standard for all law enforcement investigations, and the one that ——

Mr. MEADOWS. But the consistent standard should be probable cause, wouldn't you think, with an expectation of privacy?

Mr. DOWNING. There are particular situations like the shooting at the judge, though, that caused the probable cause standard to not be ——

Mr. MEADOWS. I don't know of any Tea Party group that shot anybody, do you?

Mr. DOWNING. I don't.

Mr. MEADOWS. Well, so let's not talk about shooting of a judge and comparing it to the IRS, I mean, because you are somehow justifying that that would be appropriate.

Mr. DOWNING. I'm merely saying that ——

Mr. MEADOWS. They can use your same standard.
Mr. DOWNING. There should only be one standard ——
Mr. MEADOWS. So what about ——
Mr. DOWNING.—yes.
Mr. MEADOWS. All right. So is it breaking the law if a criminal buys a stingray and they start to use this?
Mr. DOWNING. Yes, it is.
Mr. MEADOWS. Now, why would that be because there is no probable cause standard?
Mr. DOWNING. No, whether something's a crime and whether something is available to the government under ——
Mr. MEADOWS. Yes, but here is—the difference is what you are doing is superseding the judicial branch by basically saying the executive branch here knows best because what you are saying is we don't really need probable cause and go before a judge because we have this reasonable suspicion standard.
Mr. DOWNING. I would emphatically disagree. It's the courts that decide this. And when we have obtained those orders, it's by going to a judge in order to obtain it, and they've signed the—and then it's litigated later. And today, the three circuit courts that have decided this issue have not had their opinions vacated, have ruled that there is no reasonable expectation of privacy ——
Mr. MEADOWS. Well, here is where I would caution you, and I am going to yield back to the chairman. This is very problematic in a bipartisan way, and you have a choice here today, to start to work it where we can help law enforcement enforce and still protect our Fourth Amendment rights or you are going to find yourself without a tool very quickly because I think there is a bipartisan desire here to make sure that the protection for all Americans is something that they should expect.
I appreciate the patience of the chair.
Chairman CHAFFETZ. The gentleman yields back.
I now recognize the gentleman from Wisconsin, Mr. Grothman, for 5 minutes.
Mr. GROTHMAN. Thank you.
I am going to switch a little bit more to some other ways people are tracked. We are going to start out here with Mr. Downing, but we will go on if someone else wants to jump in.
How would Justice obtain information from, say, OnStar or a similar feature? There is a GPS feature built into cars and about car movements.
Mr. DOWNING. So in the situation where there is a GPS chip in a car or, for that matter, in a phone and the company activates that chip in order to determine the location of the phone or the car and reports that back, that's a situation where we would use a search warrant unless there were an exception to the Fourth Amendment.
Mr. GROTHMAN. Okay. Would a grand jury subpoena be sufficient?
Mr. DOWNING. No, not in that situation.
Mr. GROTHMAN. Okay. What would be the procedure followed to obtain real-time or prospective GPS location from an OnStar-like device, and is it different from past movements?

Mr. DOWNING. So as I mentioned, a search warrant would be the type of tool that we would use when it's that kind of GPS level and collecting it prospectively. I don't believe that OnStar collects historical location information. I'm not familiar with that.

Mr. GROTHMAN. Okay. Can you have a service provider send real-time data location from the device's GPS?

Mr. DOWNING. If you're asking—if it's a real-time collection of that GPS information, that would be, as I said, with a search warrant to the provider.

Mr. GROTHMAN. Okay. I will yield the remainder of my time.

Chairman CHAFFETZ. Before he yields, let me—if the gentleman would yield just to kind of follow up on that.

Can the government have them turn on the GPS device in a car?

Mr. DOWNING. Yes, I believe in many ways a car GPS device of that sort is very similar to a cell phone, and there are—some of the companies—I don't know about OnStar in particular—that have that capability in the same way that some cell phone companies do.

Chairman CHAFFETZ. Ms. Guliani, can you give us your perspective on that?

Ms. GULIANI. I think that ——

Chairman CHAFFETZ. I am sorry, your microphone.

Ms. GULIANI. You know, one of the things that's been particularly concerning to us is, you know, as I understand it, part of the reason that the Department of Justice believes that a probable cause standard is not the appropriate one is this idea that, you know, individuals have voluntarily provided this information. And that's certainly not true in the cell phone contacts for most of us, you know, are not aware of the information that phone carriers collect, and when it comes to GPS information, don't really have an ability to turn that feature off.

And I think whether its OnStar, whether it's the medical devices of the future, the ability to turn that information off may not exist. And the idea that law enforcement can, you know, in some cases ping the device or remotely turn on the device and capture our location information when we are not aware, we wouldn't want it captured, and do so potentially without appropriate protections is very concerning and doesn't comport with what the Fourth Amendment would require in this context.

Chairman CHAFFETZ. I would assume that the gentleman from Wisconsin yields back, and then I will recognize myself and then Mr. Cummings as we wrap up here.

We have been talking a lot about the Federal, you know, the Department of Justice. Mr. Downing, the positions that you represent, is that true throughout all of the Department of Justice? Is it specific to just the criminal division, which you represent? I mean, are we to assume that this includes the DEA and the marshals and the FBI, et cetera?

Mr. DOWNING. The positions that I've been discussing apply across the board to all criminal investigations. I can't speak for national security investigations.

Chairman CHAFFETZ. Okay. I just want to make sure I understand the scope.

And what is also important for those listening to this hearing and members is that is just the Department of Justice. And the

concern is that other Departments have their own standards, their own way of collecting and securing these data.

As Ms. Duckworth talked about, one of my concerns is what are the standards? Because if you are going back to not having to use a warrant to gather historical information, there are no bounds on that. If you knew that some political group or organization was meeting at a certain location at a certain time, you could go get all that information and not have to get a warrant, correct, Ms. Guliani?

Ms. GULIANI. That's correct, and I think even more concerning is that there's no notice. So, for example, if you're in a situation where, you know, the Department of Justice or another law enforcement agency is collecting information about hundreds of individuals and what cell tower they connected to, it's not the case that after 90 days or the conclusion of the investigation that you'll be provided notification and able to challenge that conduct in court. And that's different than the approach taken, for example, by the wiretap statute. And so what we've essentially got is a situation where innocent people who have their information collected as a practical matter just don't have recourse to challenge this conduct in court.

Chairman CHAFFETZ. The ACLU did a very interesting report. I can't remember the date of it but I was fascinated by it. It is part of what compelled my interest in this topic where you did a survey across the Nation of the various law enforcement—I believe it was municipal, county, and State law enforcement. Can you generalize that?

And I would ask unanimous consent to enter into the record—although I don't have it here, I will get it in the next 2 days. Without objection, so ordered.

Chairman CHAFFETZ. But, Ms. Guliani, can you give us the framework of that survey?

Ms. GULIANI. Sure. We've done two surveys. One was we filed FOIA requests with law enforcement jurisdictions across the country to ask, you know, what—whether they're using—collecting location information, and if so, what standards apply. And what we found was, by and large, most law enforcement agencies were collecting this location information but that standards differed widely. So in some cases, jurisdictions such as those in Kentucky and Hawaii had voluntarily decided to follow a probable cause standard. In others, we found that jurisdictions were following a lower standard or not requiring a warrant.

As part of that report, one of the things that we found was that, despite Department of Justice policy that states that a warrant should be required for real-time prospective collection, in both New Jersey and Florida, it appeared that there had been cases where location information had been collected without a warrant. So that was one report we've done.

The second examination we've done is we've also conducted FOIA requests on the use of stingrays, you know, these cell-state simulators which can collect massive amounts of information.And what we found is, despite the fact that there are, you know, no Federal laws and no Federal guidance even concerning localities that receive Federal funds to purchase stingrays, but also the standard

varied widely. In some cases, law enforcement were not getting any court authorization. In other cases, even in cases where they received court authorization, they weren't informing judges, hey, this is what we're using, this is the impact of what it has. So judges were in some senses blindly, you know, signing orders.

And the third thing that we found was that there had been a concerted effort to keep these devices secret from both judges and defense attorneys and the public. And so the Department of Justice signs nondisclosure agreements with States and localities who purchase these devices, and those nondisclosure agreements say that information cannot be released.

And there may be cases where, in lieu of releasing information to a judge, the State or locality is suggested to drop the case or offer a plea bargain. And that was particularly concerning to us because, as we see it, the courts represent a way to provide oversight of the use of these devices, and to the extent that we are—there is a concerted effort to keep them secret from even these entities, that is a loss to the American people.

Chairman CHAFFETZ. So coming back, Mr. Downing, the Department of Justice has these nondisclosure agreements, these cell-site simulator nondisclosure agreements with State and local law enforcement. Is that something you can provide to this committee?

Mr. DOWNING. Yes, we can provide those. I would note, though, that the approach that we've taken particularly following the cell-site simulator policy is to make clear that we're not trying to conceal and nor should that policy be implied to conceal the fact that a cell-site simulator was used and that, of course, there's always an obligation of candor to the court. At this point, the FBI is actually looking again at those nondisclosure agreements and is in the process of revising them and trying to clarify what the approach is now.

Chairman CHAFFETZ. Why the change?

Mr. DOWNING. Well, I don't know that I have all the factors, but certainly when the environment has changed, there's a certainly a lot more information publicly available about these devices. And when the Department did an analysis that—of looking at this whole situation, we decided to institute the policy in the end, and now we're trying to make sure that all of our practices are consistent with that policy.

Chairman CHAFFETZ. I now recognize the ranking member.

Mr. CUMMINGS. Ms. Guliani, as I was just listening to you, it sounds like different standards or no standards all over the place, is that right?

Ms. GULIANI. That's exactly right. There's different standards among States. There's different standards, as you've heard, between types of location information, and there's different standards that appears from even how you collect that information, whether it's a stingray or whether it's through a phone carrier.

Mr. CUMMINGS. So would you agree that we have a serious equal protection issue here?

Ms. GULIANI. I think there are serious concerns that, you know, depending on where you live or the type of technique being used, that you will have a different standard apply, which is one of the reasons we believe it's so important that we have legislation or at

a minimum that the average American has information from the Department of Justice as to what standard actually applies, you know, what standard applies when they're collecting historical location information, historical location information from a phone carrier versus the information that might be collected from, say, a phone app. Those are all missing pieces where the public and it appears in some cases the Members of Congress have been left in the dark.

Mr. CUMMINGS. Mr. Downing, you know, in listening to the other members of the committee and the chairman, it is good that we were able to reach an agreement, but if I were another member, I would be very upset. I am being frank with you. I mean, we all represent approximately the same amount of people, and I think we made reasonable arguments that we are entrusted with all kinds of very sensitive information.

And I am hoping that we can—I know we reached our agreement, but I hope that we can revisit that because I think it is unfair to members, but particularly with something as sensitive as this. It affects almost every single person, am I right, Ms. Guliani

——

Ms. GULIANI. Almost every ——

Mr. CUMMINGS.—in this country?

Ms. GULIANI. Almost every American has a cell phone.

Mr. CUMMINGS. And we represent them. And I think the public would be alarmed if they knew that there was such a memo apparently giving guidance and their Members could not see it. I mean, it just strikes me as just—something is not right there. And that is after—you know, the chairman will tell you, we try to reach a balance, but it seems to me like this is kind of not balanced. But thank you all for your testimony. I really appreciate you.

Chairman CHAFFETZ. As we conclude here, I just want to kind of go down the panel, just take 30 seconds or so if you have any concluding thought. I wasn't able to let all panel members answer all questions, so if there is something you want to share verbally here, and again, we would always welcome your ongoing communication and input and thoughts.

But let's start with Mr. Downing and kind of go down the line, and then we will conclude this hearing.

Mr. DOWNING. Just in closing, I've heard a lot of talk about whether there's a need for legislation. Obviously, we don't have a position—obviously—we don't have a position on particular legislation, but I would encourage the members of the committee to think about the different kinds of location information there are and to consider whether there are different balances that need to be struck between those different kinds, taking into account the needs of public safety and the justice system. And we look forward to working with the committee as that process moves forward.

Chairman CHAFFETZ. Look, we have a duty and an obligation to help keep the public safe, but I would also argue that we are different in the United States of America. We are more open and transparent and critical. And part of my frustration is not the good work that you and so many of the men and women at the Department of Justice do. It is just that in order to try to craft the right solution, if we don't see all the facts, we are going to come to the

wrong conclusion. And Congress is notorious for coming up with wrong conclusions. So we are trying to get it right, and having the maximum information helps us to get there. And that is the spirit with which we approach this. So thank you personally for your commitment to this country and all that you do, and thanks for being here today.

Mr. Doucette?

Mr. DOUCETTE. Thank you, Mr. Chairman.

One of the questions that was asked during the course of today's hearings was dealing with who should act, whether it should be Congress or the courts, and who can act most quickly in order to deal with the changing technology. I think the answer is clearly that the—this particular body needs to—can act more quickly as the technology change. But that's not my original thought. That's Justice Alito in his concurrence, and United States v. Jones certainly suggested that.

That concurrence also brought up the concept that Mr. Hice was asking the questions about the mosaic theory, and that's certainly the topic of a law review article written by Professor Orin Kerr of the George Washington University School of Law. It's a fascinating article. The problem that is raised by the mosaic theory and that Professor Kerr raises is that, just as Mr. Larkin has pointed out, at what point in time does what is a—not a violation of a Fourth Amendment become a violation of the Fourth Amendment?

And I think that obviously if Congress is going to act and should act in this particular matter and can act in a number of different ways saying that historic cell tower information needs a probable cause determination or doesn't need a probable cause determination or finds the middle ground that Mr. Larkin was suggesting perhaps as far as his second alternative is that maybe at some point in time, whether it's 5, 10 days, what has been justified by a reasonable and articulable suspicion, current burden of a probable cause determination, that would aid us tremendously in guiding law enforcement and guiding the courts as to how to imply the standard for historic cell tower information.

I thank you for the opportunity to address this body.

Chairman CHAFFETZ. Thank you. And again, thanks for your good work and thanks for your expertise in being here today. I do appreciate it.

Mr. Larkin?

Mr. LARKIN. Three brief points. First, several members asked what is the adverse effect from a search warrant requirement? I think the right answer to that is we don't know. We don't know in individual cases because no individual police office or agent is going to be able to say the reason I couldn't make an arrest was I had to use a probable cause standard rather than a reasonable suspicion standard. Plus, at a macro level, we don't have anybody collecting that information on individual cases. So we really don't know the answer to what is the adverse effect from a search warrant requirement.

Second, with respect to the post-Jones memo, there isn't a good argument why DOJ shouldn't share it. It's, I think, a historic artifact. I was at DOJ for 9 years, and the executive branch and DOJ tend to look at Congress as not being part of the government. Con-

gress has always taken a position that the attorney-client privilege, for example, doesn't apply between the branches because it's all one government. The same is true here, and certainly as your colleague said, if you can get information dealing with the government's nuclear capabilities, you can get information dealing with stingrays.

Finally, your colleague from Wisconsin, I think ——

Chairman CHAFFETZ. Yes.

Mr. LARKIN.—asked about OnStar. OnStar is a private company. The relationship OnStar has with a customer, whether it's Ford or John Doe who buys a Ford with OnStar, is not governed by the Constitution. There may be Federal statutes that regulate to whom OnStar can give that location information, but the Constitution doesn't come into play at all. So if there's no statute limiting what OnStar can do, OnStar can give that information to the New York Times if it wants. So what happens when you regulate the government is different than private parties.

Chairman CHAFFETZ. Well said. And again, thank you, Mr. Larkin, for your expertise and your participation here today. We do appreciate it.

Mr. LARKIN. Thank you, sir.

Chairman CHAFFETZ. Ms. Guliani?

Ms. GULIANI. Well, thank you very ——

Chairman CHAFFETZ. Microphone.

Ms. GULIANI. Thank you very much for having this hearing.

I would underscore, you know, the points I made earlier. I think that now the time is ripe for a congressional action here and for legislation and for holding law enforcement to the same standard that applies to information in a variety of other contexts, you know, whether it is entering your home or getting a letter in a probable cause standard.

I would say, though, in the interim, as we wait for such legislation, I know that members of the committee will continue to press, and I hope that they will press the Department of Justice to release its policies publicly. I appreciate the fact members of this committee will now have an opportunity to see the Jones memos. That's an opportunity that all Americans should have.

And we should also understand exactly what standards are governing collection of location information. And to the extent that the Department of Justice can release a policy, similar to what it did with stingrays, release a public policy so that Americans can understand what standard applies, and we hope that that policy will have a probable cause standard. And we think that it should have a probable cause standard to comport with the Fourth Amendment.

And without such actions, I think we risk being in a place where simply due to modern technology, the fact that I want to use a cell phone or I want to have a GPS system in my car that somehow I'm entitled to less privacy, somehow my life is an open book in a way that the Founders didn't intend. And, you know, given these technological realities, I certainly hope that Congress will press the Department of Justice to take these actions.

Chairman CHAFFETZ. Thank you. You have been very insightful and very helpful on this, Ms. Guliani, and I do appreciate your par-

ticipation and your insight, your help with this committee. So thank you so much for being here.

Ms. GULIANI. Thank you.

Chairman CHAFFETZ. Thank you all. The committee stands adjourned.

[Whereupon, at 12:12 p.m., the committee was adjourned.]

○