AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

# ECPA REFORM AND THE REVOLUTION IN LOCATION BASED TECHNOLOGIES AND SERVICES

## HEARING

BEFORE THE

SUBCOMMITTEE ON THE CONSTITUTION, CIVIL RIGHTS, AND CIVIL LIBERTIES

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JUNE 24, 2010

**Serial No. 111–109**

Printed for the use of the Committee on the Judiciary

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

U.S. GOVERNMENT PRINTING OFFICE

57–082 PDF WASHINGTON : 2010

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

## COMMITTEE ON THE JUDICIARY

JOHN CONYERS, JR., Michigan, *Chairman*

HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
WILLIAM D. DELAHUNT, Massachusetts
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO PIERLUISI, Puerto Rico
MIKE QUIGLEY, Illinois
JUDY CHU, California
TED DEUTCH, Florida
LUIS V. GUTIERREZ, Illinois
TAMMY BALDWIN, Wisconsin
CHARLES A. GONZALEZ, Texas
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SANCHEZ, California
DANIEL MAFFEI, New York
JARED POLIS, Colorado

LAMAR SMITH, Texas
F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
DARRELL E. ISSA, California
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM ROONEY, Florida
GREGG HARPER, Mississippi

PERRY APELBAUM, *Majority Staff Director and Chief Counsel*
SEAN MCLAUGHLIN, *Minority Chief of Staff and General Counsel*

---

## SUBCOMMITTEE ON THE CONSTITUTION, CIVIL RIGHTS, AND CIVIL LIBERTIES

JERROLD NADLER, New York, *Chairman*

MELVIN L. WATT, North Carolina
ROBERT C. "BOBBY" SCOTT, Virginia
WILLIAM D. DELAHUNT, Massachusetts
HENRY C. "HANK" JOHNSON, JR., Georgia
TAMMY BALDWIN, Wisconsin
JOHN CONYERS, JR., Michigan
STEVE COHEN, Tennessee
SHEILA JACKSON LEE, Texas
JUDY CHU, California

F. JAMES SENSENBRENNER, JR., Wisconsin
TOM ROONEY, Florida
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio

DAVID LACHMANN, *Chief of Staff*
PAUL B. TAYLOR, *Minority Counsel*

# CONTENTS

JUNE 24, 2010


Page

OPENING STATEMENTS

The Honorable F. James Sensenbrenner, Jr., a Representative in Congress from the State of Wisconsin, and Ranking Member, Subcommittee on the Constitution, Civil Rights, and Civil Liberties ..... 1
The Honorable Henry C. "Hank" Johnson, Jr., a Representative in Congress from the State of Georgia, and Member, Subcommittee on the Constitution, Civil Rights, and Civil Liberties ..... 3
The Honorable Jerrold Nadler, a Representative in Congress from the State of New York, and Chairman, Subcommittee on the Constitution, Civil Rights, and Civil Liberties ..... 5
The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, Chairman, Committee on the Judiciary, and Member, Subcommittee on the Constitution, Civil Rights, and Civil Liberties ..... 6

WITNESSES

Mr. Matt Blaze, Associate Professor, University of Pennsylvania
Oral Testimony ..... 12
Prepared Statement ..... 17
Mr. Michael Amarosa, Senior Vice President for Public Affairs, TruePosition
Oral Testimony ..... 31
Prepared Statement ..... 33
Mr. Richard Littlehale, Assistant Special Agent in Charge, Technical Services Unit, Tennessee Bureau of Investigation
Oral Testimony ..... 56
Prepared Statement ..... 59
Mr. Marc J. Zwillinger, Zwillinger Genetski, LLP
Oral Testimony ..... 65
Prepared Statement ..... 68
The Honorable Stephen Wm. Smith, United States Magistrate Judge, Southern District of Texas
Oral Testimony ..... 76
Prepared Statement ..... 78

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Prepared Statement of the Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, Chairman, Committee on the Judiciary, and Member, Subcommittee on the Constitution, Civil Rights, and Civil Liberties ..... 7

APPENDIX

Material Submitted for the Hearing Record ..... 105

# ECPA REFORM AND THE REVOLUTION IN LOCATION BASED TECHNOLOGIES AND SERVICES

---

**THURSDAY, JUNE 24, 2010**

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON THE CONSTITUTION,
CIVIL RIGHTS, AND CIVIL LIBERTIES,
COMMITTEE ON THE JUDICIARY,
*Washington, DC.*

The Subcommittee met, pursuant to notice, at 10:11 a.m., in room 2237, Rayburn House Office Building, the Honorable John Conyers, Jr., (Chairman of the Committee on the Judiciary) presiding.

Present: Representatives Nadler, Conyers, Johnson, Chu, and Sensenbrenner.

Staff present: (Majority) David Lachmann, Subcommittee Chief of Staff; Stephanie Pell, Counsel; and Art Baker, Minority Counsel.

Mr. CONYERS. The Subcommittee will come to order. Obviously, I am not the Chairman of this Subcommittee, but I think through common agreement with the Members that are here, we will not detain this distinguished group of panelists any longer.

This is a very important continuation of discussions that the Constitution Subcommittee has been engaged in, and it essentially revolves around cell phone technologies and how they have changed, but how the law hasn't changed. And we are trying to see if we can come together to sort out some of the differences in views that are coming out of the court. And, of course, I think very few of us can anticipate the technologies that are evolving so rapidly.

I would like to invite the former Chairman of the Judiciary Committee, Jim Sensenbrenner, the Ranking Member of this Committee, to begin our discussions.

Mr. SENSENBRENNER. Thank you very much, Mr. Chairman. And as you know, I have to give a statement on the floor a little bit after 10:30, so I appreciate your giving Republicans the first word this time. And, you know, this is somewhat unprecedented, and again, I appreciate your indulgence.

Today's hearing is the second in a series of hearings to examine the need to update the Electronic Communications Privacy Act of 1986, or ECPA for short. This hearing addresses cell phone site information and other location based technologies.

A collection of civil liberty organizations and telecom companies have proposed a series of principles for ECPA reform, including law

enforcement access to cell phone and cell site location information should require a warrant based on probable cause for both prospective and retrospective location data.

Second only to the advent of personal computing, this is a technical revolution with mobile communication devices. Industry trade groups estimate that at the end of 2009 there were over 285 million wireless subscriber connections and over 2 trillion annualized minutes of cell phone use. Almost 23 percent of U.S. households today are wireless only.

As I have said before, at the intersection of all the new technological developments and capabilities are the privacy rights of the public, the economic interest in expanding commerce, the public policy of encouraging the development of even better technologies, and the legitimate investigative needs of law enforcement professionals.

As cell phones have created greater efficiency for consumers, they also have created greater efficiency for criminals. Fortunately, they also provide new ways for law enforcement to investigate crimes.

There seems to be confusion, or at least a difference of opinion, as to exactly what location information is acquired by which technology. Some technologies may only identify the general area in which the target is located, and others can be more precise. It is important for this Committee and Congress to clarify the true nature of these technologies before we embark on reforms to ECPA.

There also seems to be confusion in the courts, or a difference of opinion, on what portions of ECPA apply to these technologies and under what standard cell location information should be aquired. Considering that ECPA was enacted in 1986, well before the proliferation of cell phones and other technologies, I think it is fair to say that the statute does not speak specifically to these issues.

At a fundamental level, traditional pen register and trap and trace data are the telephone numbers dialed from—or the telephone numbers dialed to from that particular telephone. In Smith versus Maryland, 1979, the Supreme Court ruled that an individual has no reasonable expectation of privacy in the information gathered by these pen and trap devices.

As the Internet and cell phone technology advanced, Congress expanded the pen/trap statutes to include certain non-contact information from e-mails and cell phone calls. In enacting the Communications Assistance to Law Enforcement Act of 1994, or CALEA, Congress specifically instructed that a person's location information cannot be acquired solely pursuant to a pen register.

The Stored Communications Act, an act that is a part of ECPA, governs law enforcement requests for various types of stored information. Under an intermediate standard of specific and articulable fact, courts have widely held that the government can use the second communications act—Stored Communications Act; I am sorry—to acquire subscriber records, including retrospective cell location data.

However, the Third Circuit Court of Appeals is currently considering the application of the statute to retrospective cell site location information. The United States has appealed the denial of an order for historical information, even though the government complied

with the provisions of the statute, then based their application on specific and articulable fact showing that the information is relevant to an ongoing criminal investigation.

From co-mingling of the pen and trace statutes and the Stored Communications Act has evolved a hybrid order for requests of certain prospective cell site information. Some courts have accepted this theory and some have not, opting instead to require the government to obtain a warrant to enter Rule 41 of the Federal Rules of Criminal Procedure.

While there may very well be a need to clear up the confusion in the area of obtaining prospective cell site location information, it does not necessarily follow that the appropriate remedy to any ambiguity would be a Rule 41 search warrant based upon probable cause.

I thank the witnesses today, and I look forward to their testimony.

Let me say this is a very complicated area. It is not one that I think reeks of partisan divisions. I think we all know that a 24-year-old original law and a 16-year-old second law is way out of date compared to where the technology is at. And in order to clear this up for everybody, whether it is the courts, the law enforcement, the cell phone providers and everybody else, Congress needs to be very professional in doing what needs to be done to bring this up to date and know that haste may make waste. Thank you.

Mr. CONYERS. Thanks, Jim Sensenbrenner, for your opening comments.

And I now turn to Hank Johnson, himself a former magistrate in the Atlanta court system, and presently the Chairman of the Courts and Competition Subcommittee in Judiciary.

You are welcome to begin whenever you want, Chairman Johnson.

Mr. JOHNSON. Thank you. Thank you, Mr. Chairman, for holding a very important hearing.

Looks like my mic is not working, so I will just speak loudly.

This important hearing will give Members the opportunity to examine the Electronic Communications Privacy Act with respect to location based technologies such as cell phones and smart phones. The Electronic Communications Privacy Act provides the standards for law enforcement access to the electronic and wireless technology we use.

Specifically, this hearing will give Members the opportunity to hear from witnesses about reform under the Act and issues relating to historical and real-time location data. This hearing is timely, as mobile communication devices have evolved from being little more than a convenience for the wealthy to a basic necessity for most Americans. Cell phones have transformed the way we communicate and work with each other on a daily basis. In today's society it is more common for one to have a cell phone rather than a traditional landline phone.

According to 2009 Wireless Association report, there were approximately 277 million cell phone service subscribers in the United States last year. That is about 90 percent of the overall population. Whenever the subscribers have their cell phones on, the phones can automatically scan for cell towers and register location

information with the network. This has led to substantial privacy concerns, as cell site data may be collected without a person's knowledge.

Further, some data provides the ability to track all of a person's movements on a relatively precise and continuous basis. When it comes to law enforcement and national security, the value of a person's location at a particular moment in time cannot be overstated. Criminal investigators can use this information to find a child that has been kidnapped or to apprehend a dangerous criminal.

While the benefits of technology to aid law enforcement are great, it is important to remember that Americans have privacy rights. The founding fathers recognized that citizens need privacy for their persons, houses, papers and effects. While technology has been advancing at the speed of light, that basic principle the framers had in mind when they drafted the Constitution has not changed. Therefore, it is important to have a balance between user privacy expectations and law enforcement needs.

I want to deviate from my prepared remarks to let you know about a recent experience that I had. This week while I was here in Washington, I got a call from my scheduler over here at the Capitol, who told me that she had heard from my dealership that my car had registered—sent back a message that it needed—it was time for an oil change. And so I had the OnStar technology in the car, but I did not know that whatever data recorder is in the car would notify the dealership that the car itself needed some topping off of the oil.

And that is a sobering to me to know that someone sitting up at a computer terminal can see where I am, where my car is—at least where my car is—and what kind of condition it is in. They probably know how fast I drive it. And can that information be shared on a commercial basis without my knowledge? Those are some of the issues that we will be facing in the future.

The ability to monitor communications has grown enormously. As technology continues to expand, Congress should adjust laws accordingly to keep up with modern technology. And by the way, when I get home, the first thing I am going to do is look at that OnStar contract and see exactly what it provides for and what it does not provide for.

It has come to Congress' attention that the standards governing law enforcement access to historical and real-time cell site data regarding location information may be the most confusing area of the Act's application to wireless technology. With more than 500 Federal magistrate judges serving in district courts around the country, there is no room for confusion when it comes to the Electronic Communications Privacy Act. If courts are issuing conflicting decisions with different standards regarding law enforcement access to this wireless location data under the Act, Congress should step in and act accordingly.

I am anxious to hear from the witnesses today, as I have a number of questions. Should Congress step in and reform the Electronic Communications Privacy Act? If so, how should the Act be reformed to strike the proper balance between consumer privacy and law enforcement? What should law enforcement officers have to provide cell phone providers in order to obtain access to historical

and real-time data? Would it be premature for Congress to legislate, as there are unresolved Fourth Amendment issues?

I hope our witnesses can shed light on these questions, and I look forward to hearing from the witnesses. And I yield back the balance of my time—and would request a working microphone.

Mr. NADLER. [Presiding.] Thank you. You might try the one on the other side.

Let me just say before I read my opening statement that Mr. Johnson's opening statement raises some interesting possibilities. I didn't know that the car told the dealership when it was thirsty. I am pretty sure pretty soon it may be telling the insurance company that you are not replacing the brake fluid often enough or whatever, and this raises real questions about your car communicating with other entities without your even knowing about it and perhaps influencing your legal liabilities or rights.

Today's hearing is the second in which this Subcommittee will consider the statutory framework Congress established in the 1986 Electronic Communications Privacy Act, ECPA, in light of the enormous technological advances in electronic communications and 24 years since ECPA's passage.

While the first hearing was a general introduction to several ECPA reform issues that should be examined, this hearing will focus specifically on advances in cellular location based technologies and related services and how such technologies, while enriching our lives, can provide more precise and, to many of us, sensitive information about where we may be located at any given time.

So today we continue our examination of whether ECPA still strikes the right balance between the interests and needs of law enforcement and the interests of the American people in privacy. If we conclude from this examination that the balance of interests between law enforcement and personal privacy must be struck more finely, we will take the necessary legislative action. If we embark on that course, we must bear in mind the exigencies and complexities of the security environment in which law enforcement must act.

Moreover, if we act, we must do so with the full knowledge that any legislative changes to ECPA must nevertheless sustain the public's confidence in the security of their communications, or it can harm both the robust market for cell phones and the rapid innovation that is fundamental to that market's health. Because ECPA inevitably involves the interaction of all these important and complex considerations, we are taking the time through a series of multiple hearings to educate ourselves carefully and fully before beginning to engage in any legislative action.

This Subcommittee's exploration of where the appropriate balance may lie with respect to location information must surely include a lesson in location based technologies and services. After all, when ECPA was passed back in 1986, approximately 8 years before the GPS system was fully activated for public use, the only options one had for locating oneself on the road was still a road atlas or gas station. Now, as we will see, the GPS is supplemented by an array of different location technologies and the myriad applications they support.

We are honored to have certain witnesses here today, who are experts in these technologies. They can give us the necessary background to embark upon an understanding of how they work, what types of information and records they can generate and store, and how they can be of assistance to law enforcement in appropriate circumstances.

This initial educational effort is in my view not only warranted, but essential before we undertake any effort at amending or otherwise reforming ECPA. After we hear the terrain described, we will move on to other questions today—namely, how is ECPA currently being applied to these location based technologies and services by the courts?

Without stealing his thunder, we have one very distinguished witness here today, who will tell us in the most respectful way, I am sure, that Congress needs to give better guidance to the courts with respect to the standards governing law enforcement access to certain types of location based information. He is a magistrate judge working, as we say, in the trenches, who has grappled with how to apply ECPA to law enforcement requests for various types of location based information.

In many respects, at least for the moment, the testimony and discussions today may raise more questions than they answer. Since we are to hear about technologies both existing and those that are foreseeable that are revolutionary, certainly, by 1986 standards, I want to acknowledge that our task will be a challenge to find the appropriate balance between privacy and law enforcement interests, to protect the public while preserving consumer privacy and confidence, to support rapid technological innovation yet discern standards for law enforcement access that will not become outdated with each new generation of technology every 2 or 4 years.

As I indicated, this journey will at least initially take the form of a dialogue, and this Subcommittee needs the assistance and input of all stakeholders—law enforcement, private industry and civil liberties groups alike—in order to have any hope of getting this right. We look forward to speaking with you formally or informally and seeing you at future hearings.

The Chair will now recognize the distinguished Chairman of the full Committee for an opening statement.

Mr. CONYERS. Thank you, Chairman Nadler. I am going to put my statement in the record, and I will make just a couple observations.

[The prepared statement of Mr. Conyers follows:]

**Statement of the Honorable John Conyers, Jr.**
**for the Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services**
**Before the Subcommittee on the Constitution, Civil Rights and Civil Liberties**

**Thursday, June 24, 2010, at 10:00 a.m.**
**2237 Rayburn House Office Building**

The growth of cell phone technologies has provided all of us with new and innovative ways of communicating and accessing information. And, most Americans consider these technologies to have generally enriched their lives.

The growth and improvement of cellular services has also provided law enforcement agencies with new, more precise ways to locate and track those committing criminal activity.

Of course, with improvements in investigative tools – particularly tools that can reveal very personal details about our lives – come increased pressure upon our civil liberties.

Maintaining these interests in proper equilibrium is one of the core tasks of the Judiciary Committee as a whole and, particularly where Fourth Amendment questions arise, of the Subcommittee on the Constitution.

Congress passed the Electronic Communications Privacy Act in 1986 to regulate access to our electronic communications by law enforcement agencies.

Nearly 25 years ago, when this Act became law, few of us even

had cell phones. Now, cell phones play an integral, necessary part of our everyday lives.

This hearing is the second in a series of hearings where the Constitution Subcommittee will examine the Electronic Communications Privacy Act and determine what reforms should be made to strike the balance I've alluded to in light of these technological innovations.

We must ensure that law enforcement can investigate and prosecute crimes vigorously so that it can protect the public in this new environment.

At the same time, however, we must do our part to protect the public's interests in privacy and security by ensuring that law enforcement does not get access to private information without first meeting an appropriate legal standard.

As this hearing examines the Electronic Communications Privacy Act Reform with respect to location based information and services, I would like to raise several key issues for consideration.

**First**, has the emergence of new, varied and more accurate location based technologies rendered the analysis of traditional privacy protections associated with location data irrelevant or outdated?

For example, are GPS-enabled cell phones that people carry around electively best treated as being analogous to traditional tracking instruments that law enforcement secretly attaches to a vehicle?

Are there meaningful legal distinctions that can be drawn between different types of location based technologies and services?

**Second**, how are courts applying the Electronic Communications Privacy Act to current location based technologies?

Has the rapid success and acceptance of location based technologies and services outpaced the Electronic Communications Privacy Act in spite of the most gallant efforts by courts to try and adapt the statute to innovation?

Is there any danger in these continued gallant judicial attempts to pour new technological wine into old legal skins?

**Third**, does the continuing development of new, even more precise location based technologies and services require us to consider legal standards that are technology neutral so that our laws do not become outdated or even obsolete with each new generation of technology?

I understand that we will hear today from witnesses who are experts in these location based technologies and can give us a general background necessary to begin our consideration of what changes to the law may be appropriate in an age where technology will always be advancing.

These are important questions we must ask in the interests of both law enforcement and the public if we are to make the Electronics Communications Privacy Act work for both in this new age.

We will take our time, through the hearing process, to educate ourselves carefully and fully about a range of issues pertaining to reform of the Electronic Communications Privacy Act.

It will be a difficult task and I want to thank my good friends Mr. Nadler and Mr. Sensenbrenner for embarking upon it today, and to thank all our witnesses for helping us to determine the scope of this undertaking by contributing their testimony and expertise.

Mr. CONYERS. The first is that what our distinguished judicial witness did is extremely important; in meeting this Committee under your guidance to begin this evaluation of the relationship between the incredible outpouring of technology and the fact that our laws sometimes are not keeping up with it.

In addition, we have the problem of not being able to anticipate what new technology is coming out in the first place, so it is a sort of built-in problem. Do we try to process the congressional role in the normal way, or do we try to anticipate what is going to happen?

But I think the basic thing that Judge Smith has pointed out and that reinforces the importance of this hearing is that the courts are in disarray themselves, and understandably so. We have been looking at the 1986 law, and essentially it was created to govern law enforcement access to electronic and wire communications. It created different standards, some that are very high—what is a super warrant, anyway, for wiretapping—and some that are very low. What is a subpoena for telephone toll records?

And so this law, written before the technology existed, has understandable problems. But it is to the credit of this Committee that we have embarked on this discussion. This is the second of a series, and it sure won't be the last.

And it is in this spirit that I commend all five of you distinguished witnesses, experts, in coming here to help us unravel this problem today. I thank you for your presence.

Mr. NADLER. And I thank you.

Without objection, all Members will have 5 legislative days to submit opening statements for inclusion in the record. We will now turn to our panel of witnesses.

Our first witness is Matt Blaze, who is an associate professor of computer information science at the University of Pennsylvania, who serves as director of the distributed computing laboratory and conducts research on computer security, cryptography, network communications and surveillance technology. Much of his research focuses on methods to strengthen critical infrastructure against criminals and other unauthorized eavesdroppers and to help ensure that authorized surveillance systems work as intended in the rapidly changing environment in which they must be reliable.

Prior to joining the faculty at Penn, he worked for 12 years on the research staff at AT&T Labs in New Jersey. Professor Blaze earned his Ph.D. in computer science from Princeton, a master's degree from Columbia, and his undergraduate degree from the City University of New York.

Our second witness, Michael Amarosa, is senior vice president of public affairs at TruePosition, a location based technology company. Prior to joining TruePosition, Mr. Amarosa spent 24 years with the New York City Police Department in various managerial capacities, including 3 years as deputy commissioner for technological development, where he was directly responsible for the design and implementation of the city's E-911 system.

Mr. Amarosa is also chairman of the E-911 Institute, an organization that provides administrative and policy support to the congressional E-911 Caucus. Mr. Amarosa received his J.D. cum laude

from the New York Law School, a master's degree in public administration from NYU, and his B.A. from St. Peter's College.

Mark Zwillinger—I skipped somebody; oh, I am sorry—Richard Littlehale is an assistant special agent in charge of the Tennessee Bureau of Investigation Technical Services Unit. In this capacity he coordinates and supervises the use of advanced and covert technologies in support of law enforcement operations, and he is a Federal task force officer with an FBI joint cyber crime task force. Mr. Littlehale is a graduate of Bowdoin College and received his J.D. from Vanderbilt Law School.

Mark Zwillinger is a founding partner of Zwillinger Genetski LLP, where for 10 years his practice has focused on issues related to the Electronic Communications Privacy Act, the Wiretapping Communications Act, surveillance law and privacy. Previously, Mr. Zwillinger ran the privacy and security practice groups at Sonnenschein Nath & Rosenthal and at Kirkland & Ellis. Prior to that he served 3 years as a trial attorney in the computer crime and intellectual property section of the criminal division of the Department of Justice. Mr. Zwillinger earned his J.D. magna cum laude from Harvard Law School.

And finally, Judge Stephen Smith has served for the last 6 years as United States magistrate judge for the Southern District of Texas, Houston Division. Before his appointment to the bench, he practiced law for 25 years in the Houston office of Fulbright and Jaworski LLP. Judge Smith earned his B.A. cum laude from Vanderbilt University and graduated from the University of Virginia Law School.

I think we have two witnesses from Vanderbilt at some point. I am pleased to welcome all of you. Your written statements in their entirety will be made part of the record. I would ask that you summarize your testimony, or try to, in 5 minutes or less, which will be liberally construed. To help you to stay within that——

We don't have the timing. Do we have the timing thing? Yes.

To help you stay within that time limit, there is a timing light at your table. When 1 minute remains, the light will switch from green to yellow and then red when the 5 minutes are up.

Without objection, the Chair is authorized to call a recess of the hearing at any point, which we will endeavor to do only in case there are votes on the floor.

Before you begin, it is customary for the Committee to swear in its witnesses, if you would please all stand and raise your right hand to take the oath.

Let the record reflect that the witnesses answered in the affirmative.

You may be seated. We will now hear from our first witness. Professor Blaze is recognized.

## TESTIMONY OF MATT BLAZE, ASSOCIATE PROFESSOR, UNIVERSITY OF PENNSYLVANIA

Mr. BLAZE. Thank you, Mr. Chairman, for the opportunity to talk to the Committee today about the technology of wireless communications and tracking and wireless communications systems. It is a great honor to be here, and I am humbled by the task of trying

to distill what is in fact not just a very complex legal area, but a very complex and often confusing technological area.

Wireless technology, as we all know at the risk of gross understatement, has since 1986 exploded in popularity and undergone numerous generational changes that have completely changed the landscape not only of how we communicate and interact with each other, but of how the underlying technology works and how we think about it.

So what I would like to discuss first of all is the way cellular telephone networks work and are structured. The cellular telephone, unlike the traditional wire line telephones that we grew up with, uses the radio to communicate with the wired telephone network instead of a cable connected to your home or office.

This is essentially by itself a revolution in the way we think about the telephone, because it is no longer fixed to a particular location. We carry our phones with us now. Rather than thinking about the telephone located in a place that we call, we think about the person we want to call, because we expect them to have their telephone with them.

We can move around with these devices usually anywhere in the country, or almost everywhere in the country. And we expect our telephones to work, and largely they do. I was surprised to discover my telephone worked in the D.C. Metro on my way here this morning.

Cellular providers accomplish this by deploying a network of relatively closely spaced local radio base stations, those ubiquitous cellular telephone towers that we see in neighborhoods and alongside highways that are each responsible for completing telephone calls made by cell phones in their immediate area.

Cell phones, as they move and as they are turned on, discover the base station with the strongest radio signal and perform a registration process identifying themselves, establishing that the user has a valid cell phone service, and identifying the local base station that is best equipped to process the call by virtue of the strength of its radio signal.

Now, it is very important that coverage be contiguous, so essentially what cellular providers do is divide their coverage area, essentially the United States for most of the cellular providers that are there today, into a mosaic of local base station service areas that are called, in the terminology of the industry, sectors. So the base station with which a phone communicates covers an area called the local sector that it has good radio coverage for.

Now, when you move from sector to sector or when you place a call, cellular phone companies keep track of that so they know where incoming calls should be routed, which base station they should send the call to to have your phone ring. When you place the call, they know that you already have established that you have a valid account and have paid your bill and so forth. So cellular——

Mr. NADLER. On a technical point, when you move around with your phone in your pocket, they know where it is only if you make the phone call, or just because it is there emitting a signal?

Mr. BLAZE. No, any time the telephone is on, the phone periodically will check the signal strength of the local base station, send

it a message saying essentially, "Can you hear me? I am in your sector. Please register me." And the phones periodically do this. They do this when they are turned on. They do this as they move from place to place.

And in order for you to be able to receive incoming calls, it is very important that the phone company, this wireless company, keep track of which sector you are in, because that is how the switching equipment knows which base station to send an incoming call to cause your telephone to ring. So any time the phone is on, any time it moves around, whether it is actually making or receiving a call, the wireless provider is tracking the current base station with which a phone is associated. And that has been a central part of how the network works.

Now, how do we track phones? What kind of location tracking technology is available in this world of everyone carrying around a wireless handset? Well, the most prominent location tracking technology, the one that is most visible to the end user, is called GPS, which makes use of the global position system satellites originally put up by the U.S. military that allow a device with a satellite receiver and a view of the open sky to calculate very precisely its own location.

Mr. NADLER. Excuse me. And your cell phone in your pocket has that capacity to talk to the satellite?

Mr. BLAZE. Well, many cell phones do, but not all do. And in fact, although GPS technology is the most prominent location tracking technology for the end-user, it is actually not the most important technology for the surveillance and tracking point of view.

GPS has high accuracy. The latest generation of equipment can precisely locate something to within about 10 meters of accuracy, less under some circumstances. And it can be done by a device by itself with no other infrastructure than the ability to receive the satellite signals.

So we have GPS mapping systems in cars and so on. And the latest generation of telephones often include a separate GPS receiver and some mapping software and other software that can emulate the functions of, for example, a car GPS receiver.

So from the user's perspective, we often think of GPS as being the equivalent of location tracking. And we might think that if we don't have a GPS receiver on our telephones, that no one might know where we are. But in fact that is not true. GPS is actually not used by the cellular telephone network for tracking at all. And law enforcement use of GPS for surreptitious surveillance with cell phones is less important than other kinds of telephone-based tracking when we are talking in the context of wireless communication.

Now, the most basic kind of wireless tracking with a cell phone is to simply keep track of which sector the telephone is located in at any given moment. As phones move from place to place, as I mentioned, they register their location with the local base station.

The wireless company keeps track of that. It has to, because if it doesn't, it won't know how to get calls to you. And so if we keep track of which sector a phone has registered with, we effectively know where it is within the service area of that sector.

Now, a natural question to ask is, "Well, how accurate does this allow us to locate the phone? How big a radius might the phone

be in when it is registered in a particular sector, as phones do continuously when they are on?" And the answer is today is very different from what it was 25 years ago.

In the original cell systems, which were analog, not widely used, very expensive, and there weren't that many cellular customers, the incentive for the wireless service provider was to try to get by with as few base stations as possible that would adequately cover the service area in a way that would satisfy their customers. There weren't very many customers of cell phones in the earliest systems, and so really the limiting factor of how far apart base stations could be was the distance that the radio signals would travel.

But that meant that a sector might be several miles in diameter, up to 10 or sometimes even 15 miles in diameter in the early cell phone systems in areas with wide-open terrain and relatively few users. So knowing that sector location in early cell phone systems only allowed you to locate, you know, a city or a neighborhood in which a phone was located.

But cell phone systems have become so explosively popular, compared with the way we thought about them 25 years ago. There have been other factors that have resulted in the sector size steadily shrinking.

There are a limited number of simultaneous users that can be served by a cellular base station. When cellular technology wasn't as popular and was very expensive, this wasn't much of a factor. The ability of radio signals to penetrate the area was the limiting factor.

But today the limiting factor in how far apart space stations can be is the number of customers they have to serve. And as this technology has exploded, the number of customers in any given area has gone explosively up, particularly in urban and densely populated areas.

At the same time we as cellular users have more choices. There is more competition, and we have become more demanding of our cellular service providers, and we expect our phones to work in more and more places. We expect the coverage to be more and more reliable. As I mentioned earlier this morning, I discovered my phone was able to receive a call to my surprise in the Metro subway.

Being able to provide service over a continuous area requires, again, that we include sectors that cover dead spots and that are able to provide good signal coverage everywhere we go. Those ubiquitous advertisements—"Can you hear me now?"—reflect cellular service providers' competition with one another to provide base stations that cover more and more service area more and more densely.

So the effect is that the size of a sector today is far smaller than it was 25 years ago because of the natural evolution of the technology.

Mr. NADLER. Could you sum up, perhaps? In particular, tell us how big a sector is these days.

Mr. BLAZE. Right. So the largest sectors can still be several miles in diameter in rural areas, sparsely populated areas. But the latest technology has trended toward what are called variously microcells, picocells and femtocells that are designed not to serve an area of

miles in diameter, but rather to serve a very, very specific location, such as a floor of a building or even an individual room in a building such as a train station waiting room or an office complex or hotel or even a private home.

So as we have moved toward very small sector locations, we can, if a user is in one of these very small sectors, essentially determine the location——

Mr. NADLER. Exactly where he is—exactly where he is.

Let me ask one question, and I have to ask you and continue on to the next witness. It is physically necessary for the system to operate for the system to know where your cell phone is in order to route the calls there. And obviously, the smaller the area, the fewer the competing calls, and that is why it gets smaller and smaller, with obvious implications for accuracy of telling us.

What is the technological necessity and what is the practice of retaining this information? In other words they need to know where you are now so they can route the call. Do they need to know where you were an hour ago or a day ago? And do they retain this information? And if so, why?

Mr. BLAZE. Well, every service provider—I should say I am not speaking for any service provider, and every service provider will have its own practices—but in general, service providers record everything essentially forever. This information is extraordinarily valuable for business, marketing and technical purposes. It tells them where their network needs to be improved, were dead spots are, and how their customers use their phones.

[The prepared statement of Mr. Blaze follows:]

PREPARED STATEMENT OF MATT BLAZE

**House Committee on the Judiciary**

**Subcommittee on the Constitution, Civil Rights, and Civil Liberties**

**Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services**

**Testimony of Professor Matt Blaze**

**June 24, 2010**

## 1. Introduction and Background

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

I am currently an associate professor of computer and information science at the University of Pennsylvania in Philadelphia, where I serve as director of the Distributed Computing Laboratory and conduct research on computer security, cryptography, network communication, and surveillance technology. Prior to joining the faculty at Penn, I was for 12 years a member of the research staff

at AT&T Labs (previously known as AT&T Bell Labs) in New Jersey. I have a PhD in computer science from Princeton University, a Masters degree from Columbia, and I completed my undergraduate studies at the City University of New York.

A focus of my research is on the properties and capabilities of surveillance technology (both lawful and illicit) in the context of modern digital systems and communications networks. This research aims to strengthen our critical infrastructure against criminals and other unauthorized eavesdroppers and to help ensure that authorized surveillance systems work as intended in the rapidly changing environments in which they must reliably collect evidence and investigative intelligence. Sometimes, this work has led to surprising observations about real-world surveillance systems. For example, in 1994, I discovered weaknesses in the NSA's "Clipper" key escrow encryption system that led to that system's abandonment before it was widely deployed. More recently, my graduate students and I found previously undiscovered vulnerabilities in analog telephone wiretaps used by law enforcement, and we identified ways for law enforcement agencies to harden their CALEA intercept systems against a variety of surveillance countermeasures.

There is perhaps no more ubiquitous symbol of our highly connected society than the cellular telephone. Over the course of only a few short decades, mobile communication devices have evolved from being little more than an expensive curiosity for the wealthy into a basic necessity for most Americans,

transforming the way we communicate with one another, do business, and obtain and manage the increasing volume of information that is available to us. According to recent estimates, there are today more than 285 million active wireless subscriber accounts in the United States. Many households now forgo traditional "landline" telephone service, opting instead for cellular phones carried by each family member. Wireless carriers have strained to keep up with the explosive demand for cellular service, in many areas deploying new infrastructure (most visibly cellular antenna towers) as quickly as they can find places to put it.

As difficult as it may be to imagine modern life without the cell phone, it is sometimes easy to forget how rapidly the technology has come about and how quickly new laboratory ideas in wireless communication can advance into the products and services that we take for granted. Over the last 25 years the mobile telephone has transformed from an analog voice-only service (originally available in only a few markets) into a high-bandwidth, always-on Internet access portal. "Smartphones", such as the latest iPhones and Android devices, act not just as voice telephones but as personal digital organizers, music players, cameras, email readers, and personal computers, in a package that fits in our pocket. We now carry our phones with us wherever we go, and we expect them to have service wherever we happen to be.

Many of the most important and innovative new applications and services that run on mobile devices take advantage of the ability to quickly and

automatically detect the user's location to provide location-specific information and advice. At the same time, cellular providers calculate where phones in their networks are located (and how they move) to manage various network functions and to plan where new infrastructure is required.

## 2. Wireless Location Technologies

Unlike conventional wireline telephones, cellular telephones use radio to communicate between the users' handsets and the telephone network. Cellular service providers maintain networks of radio base stations (also called "cell sites") spread throughout their geographic coverage areas. Each base station is responsible for making connections between the regular telephone network and nearby cell phones when they make or receive calls. Cell phones periodically identify themselves to the nearest base station (that with the strongest radio signal) as they move about the coverage area. If a phone moves away from the base station with which it started a call and nearer to a different base station, the call is "handed off" between base stations without interruption. Phones will generally work any time they are within radio range of at least one base station, which allows users to use their phone at any location in their provider's geographic coverage area.

There are two different technological approaches for calculating the location of a cell phone. In one approach, the user's phone calculates its own location

using special GPS satellite receiver hardware built in to the handset. In the other, the cellular system calculates the location of the phones that are active in the network, using the normal cellular radio interfaces and without explicit assistance from the users' devices.

### 2.1 Handset-based GPS

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

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

make use of a phone's GPS location might be offered by the cellular carrier or by a third party, internet-base entity.

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

### 2.2 Network-based location

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

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

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

### *2.2.1 Sector identification*

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

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

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

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

way to make service more reliable in more places under varying radio conditions is to add base stations that cover "dead spots". This reduces the size of a sector's coverage area even further.

As a result, the number of cellular base stations has been growing steadily, with a corresponding decrease in the geographic area served by each. According to the most recent Cellular Telecommunications Industry Association (CTIA) study, there are more than three times as many cellular base stations today as there were ten years ago. Indeed, this trend has been accelerating in recent years, with the deployment of the latest generation of smaller and smaller-scale cellular base stations (called, variously, "microcells", "picocells" and "femtocells") designed to serve very small areas, such as particular floors of buildings or even individual homes and offices.

The effect of this trend toward smaller sectors is that knowing the identity of the base station (or sector ID) that handled a call is tantamount to knowing a phone's location to within a relatively small geographic area. In relatively unpopulated areas with open terrain, this may be an area miles in diameter. But In urban areas and other environments that use microcells, this area can be quite small indeed, sometimes effectively identifying individual floors and rooms within buildings.

### 2.2.2 *Enhanced location with time- and angle- of arrival*

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

A variety of "off-the-shelf" products and system upgrades have recently become available to cellular providers that use enhanced time- and/or angle-of arrival calculations to collect precise location information about users' devices as they move around the network. Current commercially available versions of this technology can pinpoint a phone's location to an accuracy of within 50 meters or less under many circumstances, and emerging versions of the technology can increase accuracy even beyond that. This is accomplished without special hardware is required on the users' phones, and accurate locations can be tracked in this way even when no calls are being made or received, as long as the user's phone is turned on and is within the coverage area. (Whether locations are routinely tracked and recorded at times other than when calls are made or received depends on the policy of the particular carrier).

Although these enhanced location technologies are not yet universally available in every network, wireless carriers are deploying them because they provide information that is extremely valuable in managing their networks and businesses. By tracking more precisely where each mobile device is located within a sector (and the direction it is moving), a carrier can better identify where new infrastructure is required, where old infrastructure is redundant, and how and where their customers use different wireless services.

While each carrier has its own data collection and retention practices, carriers typically create "call detail records" that include the most accurate location information available to them. Historically, before more advanced location techniques were available, carrier call detail records typically included only the cell sector or base station identifier that handled the call. As discussed in the previous section, the base station or sector identifier now carries with it more locational precision than it once did. But as even more precise location information becomes available, these records can now also include the customer's latitude and longitude along with the sector ID stored in cellular carrier databases. Some carriers also store frequently updated, highly precise, location information not just when calls are made or received, but about every device as it moves about the networks. Maintaining such detailed records about the locations of phones as they move from place to place makes good engineering sense, and we should expect this trend to continue as part of the natural progression of technology. Once the infrastructure to collect it is installed, the cost of collecting and storing high resolution location data about

every customer is relatively small, and such information is extraordinarily valuable for network management, marketing, and developing new services.

## 3. Cell Phone Location and Law Enforcement Surveillance

As noted above, even on networks that do not employ time-of-arrival or angle-of-arrival location enhancements, the sector location by itself identifies the location of a surveillance target with increasing specificity as cellular sectors become smaller and smaller and as microcells, picocells, and femtocells are deployed to provide denser coverage. In legacy systems or in rural areas, a sector ID might currently specify only a radius of several miles, while in a dense urban environment with microcells, it could identify a floor or even a room within a building. How precise sector identity is depends on the particular location of the target and on the layout of the particular carrier's network.

Most carriers' systems use a variety of large and small sector configurations. A mobile user, in the course of his or her daily movements, will periodically move in and out of large and small sectors. Even if the network only records cell tower data, the precision of that data will vary widely for any given customer over the course of a given day, from the relatively less precise to the relatively very precise, and neither the user nor the carrier will be able to predict whether the next data location collected will be relatively more or less

precise. For a typical user, over time, some of that data will likely have locational precision similar to that of GPS.

As cellular carriers roll out better location technologies in the course of their business, the location information sent to law enforcement (as transmitted from the carrier's call database in (near) real time in response to a wiretap order) is becoming become more and more precise. The current base station or sector ID paradigm is becoming less important to carriers, and as networks improve, sector data is increasingly being linked to or supplanted by an accurately calculated latitude and longitude of the customers' handsets.

In the past, when cell sectors were widely spaced and before the availability of the enhanced network-based location technologies now being deployed by wireless carriers, it may have technically sound to distinguish between location based on the cellular network (at presumably low accuracy) and that based on GPS (at high accuracy). Today, however, this distinction is increasingly obsolete, and as cellular networking technology evolves, it is likely to become effectively meaningless. As microcell technology and enhanced location techniques becomes more widely deployed in cellular networks, the information revealed by through the cell sector identifier pinpoints, under many circumstances, a user's location to a degree once possible only with dedicated GPS tracking devices. It is no longer valid to assume that the cell sector recorded by the network will give only an approximate indication of a user's location. The gap between the locational precision in today's cellular

call detail records and that of a GPS tracker is closing, especially as carriers incorporate the latest technologies into their networks.

As the precision provided by cellular network-based location approaches that of GPS-based tracking technology, cellular location tracking can have significant advantages for law enforcement surveillance operations compared with traditional GPS trackers. New and emerging cell location techniques can work indoors and in places not typically accessible to GPS receivers. Cell phone location information is quietly and automatically calculated by the network, without unusual or overt intervention that might be detected by the subject. And the "tracking device" is now a benign object already carried by the target -- his or her own telephone.

Mr. NADLER. Thank you. Thank you very much. I am sorry we went over here, but we have to get a basic education in the basics here so we know what we are—so at least we think we know what we are doing.

Our next witness is Mr. Amarosa.

**TESTIMONY OF MICHAEL AMAROSA, SENIOR VICE PRESIDENT FOR PUBLIC AFFAIRS, TRUEPOSITION**

Mr. AMAROSA. Good morning, Mr. Chairman and Members of the Subcommittee. My name is Michael Amarosa, and I am the senior vice president of TruePosition. It is a privilege to appear as part of this Subcommittee's examination of the Electronics Communication and Privacy Act.

Wireless technology plays an ever-increasing role in the daily communications of Americans, including during emergency situations. Of the 300,000 emergency calls to 911 daily, over half are now from wireless phones. This shift has the ability to locate wireless calls, the core element of our Nation's emergency response 911 structure.

Expeditious and effective emergency response has been at the center of my professional career. I spent 24 years working in public safety, and it was my honor to manage the largest 911 center in the Nation out of the New York City Police Department. During that tenure we completed major upgrades of the system and infrastructure that we needed to support the NYPD's mission.

Since leaving the PD, my role with TruePosition has given me the opportunity to work with a range of agencies in tackling ongoing and heightened national effort to bring modern technology to support emergency response, preparedness and investigations.

Long before wireless technology became prominent, policymakers and emergency response officials embraced the critical need to quickly locate individuals facing an emergency. The faster help arrives, the more likely lives are to be saved.

This premise underlies the FCC's mandate that the wireless operators provide public safety agencies with location information in an emergency situation. The requirement, as you know, is known as Enhanced 911. It dictates that the location of the wireless 911 calls must be transmitted to the appropriate emergency call center.

TruePosition's very existence has evolved from the wireless location mandate. We are the leading provider of location determination solutions. Currently, two technologies address the FCC's location accuracy requirements. They are GPS, which was discussed earlier, and Uplink Time Difference of Arrival.

Both of these technologies use what we know about radio waves. We are able to measure the distances from a known point such as a cell phone to an unknown point such as satellites and transmitters, because we know radio waves travel at constant velocity, and are able to make calculations to locate the phone from that point.

UTDOA differs from GPS, and the network base works in virtually any environment. It is not affected by obstructions such as tall buildings or concrete walls. It is able to locate all mobile phones, including those that are not GPS-enabled. Its accuracy is very high. It typically falls within 50 meters of that accuracy level.

Technology is extremely useful in law enforcement situations as well. Police used UTDOA recently to rescue a woman kidnapped in Hamilton County, Ohio, who was locked in the trunk of a vehicle. GPS was not an option, because it could not penetrate the metal trunk. A UTDOA location platform allowed police to constantly monitor the victim's location and apprehend the kidnappers.

In addition to serving 911 calls, wireless location technology has evolved in several public and private sector applications, including locating victims suffering from Alzheimer's, autistic children. It can be used to locate contraband cell phones in prison environment as an alternative to prison jamming.

Wireless technology has revolutionized communication. Unfortunately, it is also being used by criminals and terrorists. In the 2004 Madrid bombings, terrorists used improvised explosive devices to attack morning commuting trains, killing 191 people and wounding over 1,800. Mobile phones were used to detonate these IEDs. High-accuracy technology is our crucial element in preparedness, investigation and response to these dangers.

TruePosition's UTDOA technology delivers two key important elements in a mission-critical location—high accuracy and high reliability. It can provide information relating to the details of criminal conduct and be an important tool in preventing tragedy. It can present an additional dimension to the comprehensive information picture that intelligence and law enforcement officials use on a regular basis.

TruePosition's security solutions capture and analyze wireless data, including current activities, mobile events and interactions. The technology can help identify and track any mobile device in a real-time mode in any environment with high accuracy and reliability. It can be deployed in such areas as border security, critical infrastructure protection, and law enforcement to aid in forensic intelligence.

Location technology has contributed to saving lives and personal property. To allow for the continued use and growth of this life-saving technology, I urge that any government action in this area of wireless technology remain technology neutral. I commend the Subcommittee on its efforts to bring the ECPA up to date and appreciate very much the opportunity to appear before you today and welcome any questions, Mr. Chairman.

[The prepared statement of Mr. Amarosa follows:]

**PREPARED STATEMENT OF MICHAEL AMAROSA**
**SENIOR VICE PRESIDENT, TRUEPOSITION, INC**

**Before the**

**COMMITTEE ON THE JUDICIARY**
**SUBCOMMITTEE ON THE CONSTITUION,**
**CIVIL RIGHTS AND CIVIL LIBERTIES**
**HOUSE OF REPRESENTATIVES**

**Electronic Communications Privacy Act**

**June 24, 2010**

Good morning Chairman Nadler, Ranking Member Sensenbrenner and Members of the Subcommittee. My name is Michael Amarosa and I am Senior Vice President of TruePosition, Inc. It is a privilege to appear as part of the Subcommittee's examination of the Electronic Communications Privacy Act and the state of technology since it was last amended.

My role today is to provide background and history addressing the technical elements of wireless location technology, in particular network based location technology. Wireless location capability is the core element of the Nation's emergency response 9-1-1 structure. Long before wireless technologies became prominent, the Congress, the Federal Communications Commission (FCC), State and local legislatures and regulators, telecommunications carriers, those who operate the Nation's 911 Centers and police, fire and emergency medical officers (EMS), embraced the critical need to locate the individual facing an emergency expeditiously. The faster help arrives, the more likely lives are saved.

The investment and work TruePosition and other technology companies, including the wireless carriers, have committed to locating individuals confronting an

emergency flow directly from this important public policy. Beyond emerging as an important factor in the quality of emergency response, location capability now contributes to preparedness and investigation responsibilities.

Expeditious and effective emergency response has been at the center of my professional career. I spent 24 years working in public safety. It was my honor to manage the largest 911 center in the Nation, that of the New York City Police Department (NYPD), as Deputy Commissioner for Technological and Systems Development. The NYPD sought to bring to public safety technologies that would speed police, firefighter and emergency medical service response to the citizen needing help. During my tenure at the NYPD, we undertook and completed major upgrades of the systems supporting 911 and the equipment and infrastructure needed to support NYPD's mission. This effort encompassed obtaining the necessary funding, determining and designing the system upgrades, and deploying the improvements. The experience reflects a microcosm of the ongoing and heightened national effort to bring modern technology to support emergency response, preparedness and investigation. Since leaving the NYPD, my role with TruePosition has given me opportunity to work with a range of agencies, large and small, urban, rural and suburban. There remains a critical need to bring modern technology to important government responsibilities.

My purpose here today is to provide insight to the technical characteristics of wireless location technology to assist your examination of the Electronic Communications Privacy Act. I present no stance with regard to what amendments to the law should be examined. In providing technology and services, TruePosition's foremost

principle is fidelity to the laws Congress enacts. Our presence here today seeks to contribute to this important precept.

**TruePosition, Inc.**

TruePosition, headquartered in Berwyn, Pennsylvania, is the leading provider of location determination and intelligence solutions for public safety and national security worldwide. TruePosition offers a portfolio of industry-leading location technologies, future-proof platform products, innovative applications, and comprehensive networking and systems services to enable the creation of carrier-grade location solutions for private enterprise and government agencies to protect citizens, combat crime, and save lives. TruePosition has offices in North America, the European Union and Asia. It is a subsidiary of Liberty Media Corporation. EmFinders, Inc. and Rosum Corporation are subsidiary entities of TruePosition.

**Enhanced 9-1-1 Location Requirements**

The first step toward speeding emergency response was recognizing the value of a universal emergency telephone number. The United States and Canada adopted the emergency services number 911 in 1968. In the wireline environment, telephone companies know the addresses of most landline phones. Providing that information to the dispatchers at the 911 call center so they could promptly direct emergency response to the location of the incident became a priority in the national 911 system.

Yet, if a person called from a wireless phone, the public safety agency had to rely on the caller to provide an accurate location of the emergency. The most often heard question asked by emergency communications personnel was "where is your emergency?" With wireless calls expanding, the challenge is maintaining the standard

established in the wireline environment. Of 300,000 calls made to 911 daily, over half are now from wireless phones, and approximately half of those – with the relative number rising – are made from indoor environments.

Relying on the caller to provide the location for directing emergency response is fraught with risk. The delay associated with determining where the individual is stifles and often precludes determining even what the emergency is. The standard of emergency dispatch is to provide the most effective resources in the most expeditious way possible; time is unforgiving. Those calling for emergency services are unsettled and distressed even in familiar surroundings. The trauma of an event delays response or misdirects it and the error is not inconsequential. Police, fire, EMS and other emergency service agencies have documented where accident victims lost their lives because emergency responders did not know the location of the caller.

It is this background- location capability being a fundamental element of speeding emergency response- that led the FCC to mandate wireless operators to provide public safety agencies with location information in the event of an emergency. The requirement, known as Enhanced 9-1-1 (E 9-1-1) dictates that wireless calls to the emergency 911 number must be located and the location sent to the nearest or most appropriate emergency call center and only to the call center.

The FCC specified the accuracy required for locations on a statistical basis and provided a timeline for deployment. It left the choice of technology to meet the mandate's requirements up to the wireless carriers. An initial deadline of year end 2005 for national deployment of the E 9-1-1 wireless location system was met by major carriers. Those carriers unable to meet the accuracy standard were required to seek a

waiver of the FCC rules. Currently, the FCC is examining various changes to the system to improve location accuracy and effectiveness of the E 9-1-1 system.

The commitment to emergency response and deployment of wireless location is attributed to several factors. Congress consistently emphasized the importance of E 9-1-1 and the FCC pursued the goal with focus. Police, fire, EMS and other emergency response agencies and their associations advocated the importance of defined requirements and reliable performance. Just as important is the private investment by wireless carriers in their networks and the public investment by state and local government in individual 911 centers.

TruePosition's very existence evolves from wireless location technology. We made substantial commitments of resources, prior to any mandate, to develop technologies able to provide the location of persons using mobile phones to call for help. The effort has required understanding and respecting wireless carriers and their network as well as their customers and public safety agencies. We value our work with the public safety community and with carriers, both large and small, to bring about pervasive E 9-1-1.

TruePosition continues to commit significant resources to provide location technology to the ever-evolving generations of mobile devices. With carriers now promoting wireless broadband services, it is crucial that citizens and public safety officials can continue to rely on location technology. As manufacturers, service providers, software and application developers and ancillary equipment sources move to shape the standards and protocols of the future, location technology must be at the forefront.

**Wireless Location Technologies**

Currently two location geolocation technologies are capable of addressing the FCC's location accuracy requirements and are installed nation-wide. US CDMA carriers use a handset based technique known as Global Positioning System (GPS/AGPS). US GSM carriers use a network based technique known as Uplink-Time-Difference of Arrival (U-TDOA). Both approaches possess a fall back geolocation technique as well in the event the primary one cannot determine the location of the handset.

Both of these methods involve determining the location of a point in a coordinate system by measuring the distances from the point of unknown location to three or more points of known location. GPS uses space-based satellites; U-TDOA uses radios located at cell sites on the ground. Graphically, in two dimensions, the location of the unknown point can be visualized as the common intersection of three circles whose centers are at the location of the known points and whose radii are the measured distances. Radiolocation uses the properties of radio waves to measure the distances from the unknown point to the known points. The specific property utilized is the velocity of radio wave propagation. Radio waves propagate, i.e. travel, at a constant velocity. Therefore, the distance between two points can be determined by measuring the time it takes a radio wave to travel between the two points and multiplying by the velocity of propagation of radio waves to derive the distance.

GPS uses this property of radio wave propagation to permit the determination of the location of a GPS receiver, the cell phone/handset. The GPS is comprised of at least 24 satellites constantly orbiting the earth in six low earth orbits. Each satellite possesses a very accurate time clock that is synchronized with the time clocks in all of the other GPS

satellites. Each satellite transmits at least one civilian signal with its own unique signature, i.e. code, with its time of transmission and location of the satellite embedded into it. GPS receivers on the surface of the earth with an unobstructed or minimally-obstructed view to a number of GPS satellites receive the transmissions from them and note the time of reception with respect to their local clock. Typically, at least four GPS satellites uniformly distributed about the sky must be received to accurately solve for the latitude, longitude, elevation and time offset between the GPS receiver's local clock and the GPS satellites' clocks.

TruePosition's U-TDOA is a network-based technology that relies on multilateration and uses equipment installed in the mobile operator's network. Because it is network-based, U-TDOA can pinpoint the location of any mobile phone – current or future, in any environment. It allows the system to:

- Locate all mobile phones and devices, regardless of age or air interface - even those that are not GPS-enabled
- Locate so-called "gray market" mobile phones and devices – that is, those phones and devices not sold by carriers or their authorized dealers that GPS cannot locate
- Locate roaming mobile phones and devices that may not be interoperable with carriers' GPS systems
- Locate mobile phones and devices in any environment (indoors, in-vehicle, urban, suburban, rural, etc.)
- Locate mobile phones and devices with very high accuracy (typically under 50 meters) and reliability

Like GPS, U-TDOA is also a time based geolocation technique in that it measures the time of travel of radio waves. Specifically, the difference in the time it takes the radio wave to travel from the handset to Location Measurement Units (LMUs)

located at the base/transmitting facilities of the wireless carrier is the information utilized for UTDOA geolocation. The radio wave it measures is the same signal the handset uses for signaling and communications on the network. It measures the time of travel to multiple auxiliary receivers collocated with the base stations. These auxiliary receivers, the LMUs, are very accurately time-synchronized to each other and at any given moment, a handset may be communication with upwards of 30 LMUs. A minimum of three LMUs must receive the handset's signal to uniquely determine the location of it. Reception of the handset by more than 3 LMUs also enhances the accuracy of the location estimated. TruePosition has deployed over 100,000 LMUs.

U-TDOA system determines a wireless phone's geographical location by collecting and processing the RF signals transmitted by the phone. When a signal is transmitted -- when a phone call is placed -- the system gathers information about the signal from nearby mobile base stations. The data are transmitted to a processor that analyzes the information and computes the position of the caller by using TruePosition's patented Time Difference of Arrival (TDOA) algorithms. For a 911 call, the system then determines the location of the call and delivers the information so that the appropriate 911 center can dispatch assistance.

Unlike GPS, U-TDOA provides accurate and reliable geolocation of handsets even when they are indoors. This occurs for two reasons. First, the distances between the transmitter, i.e. the handset, and receiver, i.e. the LMU, is much less than with GPS, which relies upon satellite signals, so there is much less loss due to spherical spreading of the propagating radio wave. Second, and more significant, the power output of handsets can be varied and are controlled by the wireless network and dynamically adjusted many

times per second to assure reliable communications. Thus, when the loss between the transmitter and receiver increases because of attenuation by building materials, the wireless network commands the handset to increase it output power to compensate for this additional attenuation in order to achieve reliable communications. Thus, if a handset can communicate with its wireless network from indoors then U-TDOA can reliably and accurately geolocate it.

Differences between GPS and U-TDOA are important. U-TDOA is challenged in extreme rural areas, where there are long distances between carrier base stations. When satellite visibility is seriously blocked – such as in urban canyons or the insides of buildings – the GPS system is not able to produce a location. GPS cannot reliably and accurately provide caller location originating in many common buildings. In addition, unlike with U-TDOA, GPS devices can be deactivated – that is, the ability to locate them disabled – by the user.

**Expanded Use of Location Technology**

Location technology has evolved to serve beyond locating 911 calls. There are now expanded applications serving both the private and public sector. A network technology using television broadcast signals has been developed.[1] There are applications to locate lost persons and to safeguard and secure property whether it is in

[1] Rosum location technology is based on time difference of arrival where a device makes timing measurements of broadcast television signals. This technology is particularly applicable to urban and indoor scenarios, because TV signals are broadcast at a very high power level to enable them to penetrate buildings. These signals are also wide band 6 MHz bandwidth, which also facilitates accurate timing measurements. The technology requires that the TV broadcast signals be synchronized, or that a monitoring network be deployed across the coverage area to create timing calibration information of the TV signals. The technology also requires that a TV band antenna and tuner be included in the wireless device to make these timing measurements and requires that the TV broadcast antenna locations surround the devices to be located. Rosum technology has not yet been deployed in mass market.

storage or in transit.[2] It has emerged as an element of confronting and eliminating what corrections officials state is a growing challenge of illicit cell phones in prison. Jamming alone is neither effective nor risk free in eliminating illicit cell phone use in correctional institutions. Effective prevention can evolve by implementing network location and other wireless technologies. Location technology's importance in supporting law enforcement and national security missions is also recognized.

**Law Enforcement and National Security**

Today, the global environment must confront dangers that are all too real. Wireless technology has revolutionized communication — creating a level of convenience and connectivity never seen before. Unfortunately, this revolution also has a dark side, as criminals and terrorists continuously use wireless technology to coordinate their activities. High accuracy location technologies, those able to meet mission critical requirements, are a crucial element in the preparedness, investigation and response to these dangers.

Terrorists and criminals need modern communications. They use wireless communications extensively to recruit, train, plan and prosecute their crimes and atrocities. They also depend on these communications for all other aspects of their lives. To avoid possible detection, they use multiple anonymous pay-as-you go mobile phones and swap SIM cards and handsets. While wireless technology has revolutionized

[2] TruePosition's EmFinders,™ is a technology company dedicated to the rapid location and recovery of wandering or missing adults and children that uses existing U-TDOA network based cellular telephone location technology. The EmFinders EmSecQ is a small, affordable, watch-like wireless device without buttons or a screen and is under the secure and remote control of the EmFinders operations center. It is worn by individuals with medical impairments like Autism, Down syndrome or Alzheimer's disease. The device can only be activated at the request of a caregiver who has reported the individual missing to the police. A call from the EmFinders device is a pre-screened 911 call.

communication, it also provides tangible assistance to those assaulting the lives, property and values of citizens. Terrorists also use this technology to initiate attacks such as detonating improvised explosive devices (IEDs).

As events demonstrate, these incidents are a serious test to the social and economic stability of all nations. In the Madrid bombings, terrorists attacked the morning commuter trains, killing 191 people and wounding over 1,800 people. Mobile phones were used to detonate the IEDs. In Lahore, 12 terrorists attacked the Sri Lankan cricket team, killing 6 policemen and wounding 7 players. Mobile phones were used to organize and execute the attack. In Mumbai, 10 terrorists attacked two hotels, killing 164 people and wounding over 300 people. Mobile phones were used to receive orders from their leaders and coordinate the attack.

Properly implemented to protect the rights and expectations of the innocent citizen, wireless location technology has emerged as a critical implement in the preparedness and investigation responsibilities of national security and law enforcement agencies. Location technology provides the ability to detect and locate criminal and terrorists' activity in real time.

TruePosition's U-TDOA technology delivers two key requirements of mission critical location-high accuracy and high reliability. It can provide information relating to the details of the criminal conduct and be an important tool in preventing tragedy. It can present an additional dimension to the comprehensive information picture that intelligence and law enforcement officials need. While it can be implemented passively on existing networks, it is not possible without core location accuracy standards in place.

Described discretely, TruePosition location security solutions allow for automatic notifications based on desired criteria, such as the geographic zone of activity, specific communications patterns or particular users. Unlike GPS, it does not demand a special handset or device, and cannot be disabled by the user. U-TDOA technology allows for locating multiple devices in real time with high accuracy. The information obtained can be viewed in a map-based graphic format, also in real time. It includes alerting capability with regard to specific geographic areas and users. It is transparent to the device user and the network and embraces high standards to gain access and control to the capability.

The technology provides analysis capability of historic location and calling activity information. It can compile current activities, mobile events and interactions with other devices. By compartmenting information, it allows government agencies to pool resources and provide safe shared and secure access to definitive information relating to the size, detail, location and activity of illegal conduct.

Location technology has emerged as an important instrument in discerning details of criminal activity and to provide insight addressing the expanse of the conduct. It promotes the ability to analyze dangers and risks on a continuous real time basis.

**Conclusion**

TruePosition continues to work closely with large and small public safety agencies and the dedicated associations and individuals that represent them, to best integrate accurate location into the 911 communications centers. We also work closely with wireless carriers in their significant cooperative effort toward the goal of universal

E 9-1-1 deployment. With heightened national security and law enforcement demands, we work with these agencies in carrying out their critical mission requirements. TruePosition values and safeguards these important responsibilities.

This completes my statement. TruePosition appreciates very much the opportunity to appear before the Subcommittee and stands ready to provide further information today or in the future.

**ATTACHMENT**

TruePosition

LOCATION ACCURACY- THE NEED FOR INDOOR TESTING

*Ex Parte* Presentation

Federal Communications Commission

PS Docket 06-117

June 11, 2010

# SUMMARY

- FCC should require a testing protocol that encompasses indoor accuracy reflecting consumer use
- Increased accuracy evolves from clarity of rules, enforcement and investment in existing technology
- AGPS cannot reliably and accurately provide caller location originating in many common buildings

# E9-1-1 Should Reflect Consumer Behavior
# Indoor Testing is Critical

- "We-- including the general public – need to know how well the E-9-1-1 systems are doing in terms of the overall accuracy with which they are locating wireless callers. Specifically, it is important to know how well they are actually performing in operational systems in the field…"
  - *Statement of Professor Dale N. Hatfield, Committee on Commerce, S*cience and Transportation, US Senate (April 4, 2007)
- States report (Alabama, Texas, Virginia, Washington, Massachusetts, Delaware, and Michigan) that percentage of wireless calls range from 52% to 72% of all calls received by PSAPs
- J.D. Power 2009 study shows that 52% of all wireless calls are made indoors
- Wireless expansion to broadband services furthers the intensity of indoor use

# Location Accuracy Test Results

- Test Results should be submitted to the Commission in a format inviting comparison
- Results should be publicly available
- Centralized approach permits more consistent and discerning examination of progress and the environments encountered
- Affords PSAPs and Commission ability to gauge progress , enforce standards and structure remedies

# Location Technologies
# AGPS and UTDOA

- TruePosition 's *White Paper (attached)* analyzes the two location technologies used by US carriers and the ability of each to locate indoor callers
  - As radio waves travel at a constant velocity, the distance between two points can be measured. Location is determined by examining the time lapse between two points of the travelling signal
- The AGPS handset signals from satellites is one of the two geolocation technologies
- The visibility of the receiver handset to a minimum number of satellites is crucial
  - When satellite visibility is seriously blocked,-- urban canyons or inside a building, the AGPS system is not able to produce a location
- AGPS cannot reliably and accurately provide caller location originating in many common buildings

# Location Technologies
# A-GPS and U-TDOA

- UTDOA, the other US market geolocation technology, determines location by comparing time difference of the cell signal reaching each Location Measuring Unit (LMU) installed in the network's base stations
- U-TDOA technology works very well in urban, suburban, and indoor environments , UTDOA is network-based and deployed continent-wide
- UTDOA suffers in extreme rural conditions where cell sites are arranged in a "string of pearls" configuration
- Accuracy increases as number of LMUs increase, a function of carrier investment
  - Accuracy influenced by signal- to- noise ratio of the received signal, the bandwidth of the transmitting signal and the time available to process the information from multiple antennas
  - Where LMUs are not densely deployed , in-building performance is degraded as compared to more fully deployed network

# Record Affirms that AGPS is Not A Universal Solution

- *"Nevertheless, AGPS cannot today, nor in the foreseeable future, meet the E911 Phase II accuracy requirements in each and very PSAP on a PSAP-by-PSAP basis"*
- *"While these hybrid [A-GPS and AFLT] approaches can be highly beneficial to maximize yield, even employing currently available hybrid solutions will not guarantee that the Phase II accuracy requirements can be met in each and every PSAPS not only because of the difference in size among the PSAPs, but also because within PSAPs there are some challenging environments in where performance can be below the norm"*
  - *Comments of Qualcomm, PS Docket 07-114 (July 5, 2007) at page 6*
- *"Because of the inherent limitations of GPS satellite visibility, however, Verizon Wireless has also deployed technology as Advanced Forward Link Trilateration ("AFLT") which uses Time Difference of Arrival ("TDOA")* [**so does GPS**] *based on the triangulating of signals among the handset and multiple cell sites that assist GPS or independently serve as default locations. [...] However, the AFLT portion of the solution cannot achieve the GPS derived accuracy levels [...]"*
  - *Comments of Verizon Wireless , PS Docket 07-114 (July 5, 2007) at page 18*
- "In their comments, Verizon Wireless, Sprint Nextel, and QUALCOMM all described the technical features of AGPS solutions and how AGPS works in particular circumstances. These parties demonstrated that, in many PSAP jurisdictions throughout the country where certain topologies predominate, such as urban canyons and heavily forested areas, PSAP-level compliance with the current accuracy rule will be technically infeasible."
  - *Ex Parte of the Rural Carrier Association and Verizon Wireless. PS Docket 07-114 (August 31, 2007)*

# Legacy, 3G and Future Networks Require More than AGPS

- AGPS does not work in environments from which most E911 calls are made
- FCC should reject proposals allowing AGPS as a universal technology , particularly in transitory environments
- Poor indoor AGPS performance, the increasing numbers of E9-1-1 calls from indoors and the number of subscribers transitioning to advanced networks would actually decrease the number of callers able to be located

# UTDOA AGPS Comparison

## Performance of UTDOA

Source: Comments of TruePosition, PS Docket 07-114, CC Docket 94-102 and WC Docket 05-196 (August 20, 2007) at page 6

| Metric | Metric Definition | Rural Outdoor | Suburban Outdoor | Urban Outdoor | Dense Urban Outdoor | Indoor Low Penetration | Indoor High Penetration |
|---|---|---|---|---|---|---|---|
| Accuracy 67 percent (m) | 67th Percentile Error In Meters | 50 to 500+ | 65 | 65 | 65 | 77 | 90 |
| Accuracy 95 percent (m) | 95th Percentile Error in Meters | 300 to 1000+ | 180 | 180 | 180 | 210 | 270 |

# UTDOA AGPS Comparison

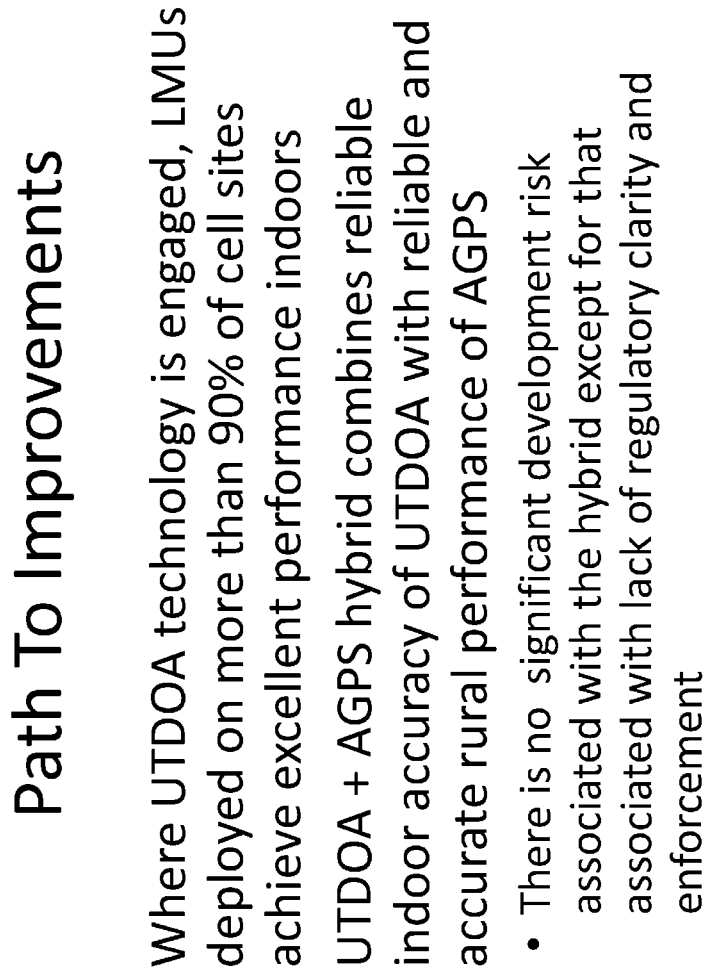
Performance of AGPS

Source: Comments of TruePosition, PS Docket 07-114, CC Docket 94-102 and WC Docket 05-196 (August 20, 2007) at pages 14-15

a—indicates that the technology failed to produce a location more than 33 percent of the time, preventing a 67th percentile accuracy from being computed

b– indicates that the technology failed to produce a location more than 5 percent of the time, preventing a 95th percentile accuracy from being computed

| Metric | Metric Definition | Rural Outdoor | Suburban Outdoor | Urban Outdoor | Dense Urban Outdoor | Indoor Low Penetration | Indoor High Penetration |
|---|---|---|---|---|---|---|---|
| Accuracy 67 percent (m) | 67th Percentile Error in Meters | 14 | 20 | 25 | 8995 | 67 | a |
| Accuracy 95 percent (m) | 95th Percentile Error in Meters | 80 | 284 | b | b | 1000 | b |




---

Mr. NADLER. Thank you.

I will now recognize Mr. Littlehale.

**TESTIMONY OF RICHARD LITTLEHALE, ASSISTANT SPECIAL AGENT IN CHARGE, TECHNICAL SERVICES UNIT, TENNESSEE BUREAU OF INVESTIGATION**

Mr. LITTLEHALE. Chairman Nadler, Ranking Member Sensenbrenner and honorable Members of the Subcommittee, my name is

Richard Littlehale. I am the assistant special agent in charge of the Technical Services Unit of the Tennessee Bureau of Investigation, and I have spent the better part of 15 years using communications records to protect the people of Tennessee.

I am grateful to the Subcommittee for giving me the opportunity to share my perspective on how location information derived from communications technologies can be invaluable in the most critical of law enforcement investigations. I offer testimony here today on my own behalf, based on my own experience.

As communications technology evolves, so must the laws that govern it. And there is always room for clarification. That said, I believe that the balance struck between privacy and public safety in the existing ECPA framework is in a broad sense a reasonable one, and I would respectfully call your attention to some risks inherent in upsetting the current paradigm.

I cannot overstate the value of location evidence to law enforcement. It can help find a kidnapped child, apprehend a dangerous fugitive or prevent terrorists from following through on a violent plan. We are not just talking about cell site information either. Imagine a pedophile grooming a potential child victim using a chat application on a smartphone. Law enforcement must be able to quickly generate and serve process on however many service providers are necessary to find that subject before the unspeakable happens.

The current legal framework distinguishes between network transactional location records stored and recorded by the service provider in the ordinary course of its business and demand-based location information generated solely based on a law enforcement request.

This information is reasonable, because it is—this framework, rather, is reasonable, because it is consistent with other ways location information can be obtained and used by law enforcement and because it is consistent with the view that information voluntarily turned over to a third party enjoys less privacy than those things we keep from the outside world.

A person's location at a particular time can be derived from any number of sources other than mobile devices. A bank will have records of a customer's use of a credit card or ATM card in their possession that would show exactly when and where that particular card was used. A transportation authority might have records of when a commuter passed by a particular tollbooth based on the information provided by their commuter pass.

Those records can currently be obtained with a subpoena in most cases. Should that standard change? Even the law of tracking devices permits installation and monitoring without probable cause under some circumstances.

Complexity is hardly foreign to the Constitution. The same piece of property—a person's suitcase, say—may be governed by completely different legal standards when it is laying on a closet shelf, in the trunk of a car, or passing through a border checkpoint.

If we suppose that a blanket standard is necessary, we must consider the consequences of rounding up to probable cause in all cases. Location information can be used to good effect in many instances where law enforcement may not have developed probable

cause. Further, the time required to generate a search warrant and have it signed may itself hamper law enforcement's efforts to move quickly in an investigation.

I fully acknowledge that the above argument could also be used in favor of relaxing the search warrant requirement completely in order to make law enforcement more efficient in all investigations. Of course, such a thing would be foreign to our bedrock legal principles. In this case, however, the present balance of judicial supervision and law enforcement efficiency has existed for some time and should not be abandoned without a demonstrated need.

Finally, even a blanket standard is going to have trouble covering everything in this area. Imagine our pedophile with a smartphone again. Say he is using the WiFi in a coffee shop, and that activity generates information that can be localized to that particular shop at a particular time. That is information location information far more accurate than a cell sector. Would it require a search warrant to get that information from the shop's Internet service provider?

Generating a search warrant for each and every child exploitation lead will slow the processing of those leads. If that is acceptable, then so be it. But it is a downstream effect that must be considered.

And what about broader locations? Are we only talking about cell sites? What if I just want to know what market your phone is using, what city you are in? That is location information.

We must also remember that legal barriers are not the only ones that keep communications records out of law enforcement hands. In many instances we are unable to utilize evidence that would be of enormous value in protecting the public, because the technologies used to carry and store that information are not accessible to us, no matter what legal process we obtain.

Encryption, smartphone, countermeasure applications, and a dizzying variety of communication streams are walling off more of the evidence we need at a steadily increasing rate. If the law enforcement community does not successfully bridged this gap with legal reform, training, solutions development and funding, then our ability to protect the public using this information will degrade at the same breakneck pace.

Whenever our society moves forward with the privacy versus public safety debate, we should be mindful that any redefinition of law enforcement access to the information it needs, whether by altering legal barriers or allowing private corporations to elect new technological barriers, may well come at a price.

Admittedly, we cannot let extreme situations rule the law. But neither should we ignore the fact that they exist. What seems like a small change in abstract setting may seem less so when I am standing on your doorstep at 4 in the morning, and your child is missing, and every second counts.

Thank you for giving me the opportunity to share one law enforcement perspective on the need for caution as we open dialogue on ECPA reform. I encourage you to seek the input of a wide range of law enforcement experts as you move forward on this critical issue. And I look forward to your questions.

[The prepared statement of Mr. Littlehale follows:]

PREPARED STATEMENT OF RICHARD LITTLEHALE

**Before the**

**Committee on the Judiciary**

**Subcommittee on the Constitution, Civil Rights and Civil Liberties**

**Rayburn House Office Building**

**Washington, D.C. 20515**

**HEARING ON ECPA REFORM AND THE REVOLUTION IN LOCATION BASED TECHNOLOGIES AND SERVICES**

**June 24, 2010**

**Written Testimony**
**of**
**Richard Littlehale**
**Assistant Special Agent in Charge**
**Technical Services Unit**
**Tennessee Bureau of Investigation**

**Chairman Nadler, Ranking Member Sensenbrenner, and honorable Members of the Committee,** my name is Richard Littlehale, and I am the Assistant Special Agent in Charge of the Technical Services Unit of the Tennessee Bureau of Investigation. We are the high-tech investigative unit of Tennessee's statewide criminal investigation agency. One of my unit's most important responsibilities is to help law enforcement agencies at all levels of government across Tennessee use communications records in support of their criminal investigations. I have personally used these techniques for the better part of fifteen years in support of everything from fugitive investigations to efforts to recover abducted children.

I am grateful to the Subcommittee for giving me the opportunity to share my perspective on how location information derived from communications technologies can be invaluable in the most critical of law enforcement investigations. I offer testimony here today on my own behalf, based on my own experiences.

## Utility of Location Evidence

The value of evidence of a person's location at a particular moment in time cannot be overstated. A criminal investigator can use the information to find a kidnapped child, apprehend a dangerous fugitive before they can harm the public, or prevent a terrorist from following through on a violent plan. Technology-based evidence is particularly valuable to law enforcement because the evidence is drawn from reliable, unbiased sources that maintain the evidence for some period of time – typically as business records in the ordinary course of the services they offer.

The various records created when a mobile device like a cellular phone interacts with its network have become a tremendous resource for law enforcement. Particularly when used in concert with traditional investigative techniques, cell phone location information frequently permits law enforcement an opportunity to find and rescue a victim or apprehend an offender in a matter of hours -- whereas other methods may consume many days and may not prove fruitful at all. Take the case of a carjacking-kidnapping victim who has a cellular telephone with her, but is unable to use it to call 911 as her assailant speeds away with her held hostage. A witness to the crime reported the license number to the police, and they used that information to identify the victim. A call to a friend or relative reveals the cell phone number. Interaction with the cellular service provider will allow law enforcement to determine a cell site that the phone recently hit, sending patrol cars to the area to look for the car. Without that evidence, the police department would have only the witness's location as a reference point for a search.

Cell site information is certainly one of the most useful location-based forms of evidence available to law enforcement, but it is by no means the only one. Increasingly,

law enforcement is required to develop location information from other methods of communication. Suppose, for example, that a pedophile is grooming a child in an internet chat room in an effort to get that child to travel to meet with him so that he can victimize the child. Suppose further that the pedophile uses a computer that is part of a particular network to access the chat room in question. A series of subpoenas to service providers will allow law enforcement to identify the subject's "virtual" location on the network (in the form of an IP address) so that the pedophile can be identified and located (by resolving the date and time of the IP assignment to a particular subscriber account and service address) – resulting in the child being spared from unspeakable harm.

**Legal Requirements to Obtain Communications Records**

At this point, it is useful to separate the issues of updating language to deal with new technologies and fundamentally altering the level of proof needed by law enforcement to access information. Generally speaking, the law enforcement community believes that the balance currently struck by ECPA and related statutes and case law is an appropriate balance. Any change to that balance should be broadly discussed and carefully considered, as it will have substantial and far-reaching secondary consequences. Having said that, there is certainly room to discuss the matter, and as communications technology evolves, so too must the laws that govern it.

***Why the current legal framework makes sense***

At present, law enforcement generally distinguishes between network *transactional* location records (ordinary records of communications captured, stored and recorded by the service provider in the ordinary course of its business as a necessary incident to providing the services they provide) and *demand*-based location information (manufactured information generated solely based on a law enforcement demand pursuant to lawful emergency or court authorization). Because the latter is not a record that already exists, it is commonly believed to require a higher standard of proof because it is more invasive.

Cell site location records are routinely generated in the normal course of a cellular provider's business. They indicate nothing more that which piece of the telephone company's equipment (the particular cell tower and sector) that a particular customer's cellular handset was communicating with on a particular call event began or concluded. Those records would be created whether or not law enforcement would later attempt to obtain them or to receive them contemporaneous with their creation; and they would be kept for a certain period of time and then discarded or archived.

Contrast this with a demand-based location request. In that instance, at law enforcement's direction and based on lawful emergency or court authorization, the

service provider causes a more precise location record to be generated – one that would not otherwise exist at all. That record would not have been created "but for" the law enforcement demand; as a result, it is reasonable and prudent to suggest that a higher level of proof be met for that information to be turned over.

This framework is reasonable because it is consistent with other ways location information can be obtained and used by law enforcement and because it is consistent with the view that information voluntarily turned over to a third party enjoys less privacy than those things we keep from the outside world. It is worth considering that a person's location at a particular time can be derived from any number of sources other than mobile devices, sometimes in very precise ways. A bank will have records of a customer's use of a credit or ATM card in their possession that would show exactly when and where that particular card was used. A transportation authority might have records of when a commuter passed by particular tollbooths based on the information provided by their electronic commuter pass. Those records can currently be obtained with a subpoena in most cases – and when they relate to communications records, Congress has already acted to afford them greater protections under ECPA's existing framework. Should that standard change? If not, how can the inconsistency be explained, if the purpose of reform is to bring clarity and consistency to the law?

***Why not always require probable cause?***

If governing law is changed to require probable cause for any type of location information, there will be a reduction in the effectiveness of this technique for law enforcement. First, location information can be used to good effect in many instances where law enforcement may not have generated probable cause sufficient to satisfy the warrant requirement. Further, the time required to generate a search warrant and have it signed, even in cases where probable cause exists, may in-and-of itself hamper law enforcement's efforts to move quickly in an investigation.

I fully acknowledge that the above argument could also be used in favor of relaxing the search warrant requirement completely in order to make law enforcement "more efficient" in *all* investigations. Of course, such a thing would be foreign to our bedrock legal principles. In this case, however, the present balance of judicial supervision and law enforcement efficiency has existed for some time, and should not be abandoned without a demonstrated need for an increase in privacy and a demonstrated pattern of abuse – presently nonexistent -- by government officials. Time is always a factor in investigations; and the more important the investigation, the more important time can become.

Take as an example a recent case that my unit worked in Tennessee. Local, state, and federal law enforcement agencies were engaged in a massive (and, thankfully, successful) search for a 4-day-old infant abducted after a stranger stabbed his mother and left her for dead. During a five-day period, my unit obtained communications

records through 15 pen register orders, 9 search warrants, and 377 administrative subpoenas and Sec. 2703 "specific and articulable facts" orders. When you are talking about that volume of process, any change in the type of process required will have an impact on how rapidly law enforcement can process leads and resolve the case, and in a case of this type, every minute counts.

This is not to say that law enforcement cannot continue if the standard for location information is elevated to probable cause. It will, however, mean some decrease in the number of leads we can pursue; and in some cases, it will inevitably prevent us from obtaining records that will be helpful and will result in some measurable – albeit unknowable – harm to the public. If the privacy trade-off is worth it in the eyes of lawmakers, then law enforcement will adapt. What is critical is that everyone involved takes steps to understand the full downstream consequences of what may appear to be minor changes to governing law, so that they may be considered in the proper context.

In addition, adopting a probable cause standard for cell site location information may not fully answer the question. Suppose for a moment that Congress adopts a probable cause standard for cell site location information. How that standard was drafted would raise a new set of issues outside of the cellular network. Suppose a customer with a "smart-phone" accesses the wireless access point of a coffee shop with the phone's Wi-Fi capability, and that generates an internet protocol address that can be localized to that particular shop at a particular time. That is location information far more accurate than a cell sector, but at no time is that information traveling over the phone company's network. Instead, the information could be obtained from the coffee shop's internet service provider. Would that require a search warrant? If so, generating a search warrant for each and every lead passed on to law enforcement of an individual who may be attempting to victimize a child over the internet will have a significant slowing effect on the processing of child exploitation leads. If that is acceptable, so be it, but it is a downstream affect that must be considered.

## The Technology Gap

I would be remiss in any discussion of the utility of technology-based evidence if I did not point out that legal barriers are not the only ones that keep communications records out of law enforcement hands. In many instances, we are unable to utilize evidence that would be of enormous value in protecting the public because the technologies used to carry and store that information are not accessible to us, no matter what legal process we obtain.

The gap between what law enforcement is legally entitled to access under current law and what is actually available is already wide -- and it is growing wider all the time. Encryption, smart-phone countermeasure applications and a dizzying variety

of communications streams are walling off more of the evidence we need at a steadily increasing rate. If the law enforcement community does not successfully bridge this gap with legal reform, training, solutions development, and funding, then our ability to protect the public using this information will degrade at the same breakneck pace.

As Congress moves forward with discussions of how it might simplify the legal requirements for obtaining communications records, and whether or not to change the standards law enforcement must meet to get the records it wants, the technology gap has a place in the discussion. I would urge that Congress ensure that whatever level of process it decides is appropriate, that steps are taken to guarantee that law enforcement will be able to access the required communications technologies once that process is obtained.

**Conclusion**

A robust debate about balancing personal privacy and security is beneficial to all Americans, but the people and their representatives must be able to make an educated judgment about what they are giving up and what they are getting. There is no question that a growing number of personal details about all Americans...location, communication, the sundry details of lives lived in the modern world...lie in storage and move in transit across a vast landscape of devices. Just as there is no question that the people living those lives have an interest in preserving the privacy of that information, there can be no question that some of those devices hold the keys to finding an abducted child, apprehending a dangerous fugitive, or preventing a terrorist attack. Whenever we move forward with the privacy/safety debate, we should be mindful that any restriction of law enforcement's access to that information, whether by redefining legal barriers or allowing private corporations to erect new technological barriers, may well come at a price, and some of that price could be paid by our most vulnerable citizens. We should be sure we are willing to require them to pay it.

As an American law enforcement officer, I know that I am a guardian of a free society, a society that embraces in its founding law the decision to elevate the rights of the individual above incremental increases in public safety. Ours is also a society that requires an open exchange of ideas on topics critical to the public interest, and today's topic is such an issue. As I hope to have shown, redrafting the laws governing law enforcement access to communications records raises significant implications for law enforcement's ability to protect the public. I urge the members of this committee to ensure that the law enforcement community is given the opportunity to continue to share its perspective on the potential human implications of any proposed reform of the Electronic Communications Privacy Act, so that all the competing factors may be balanced appropriately.

Mr. NADLER. Thank you.

Mr. Zwillinger is now recognized.

**TESTIMONY OF MARC J. ZWILLINGER, ZWILLINGER GENETSKI, LLP**

Mr. ZWILLINGER. Thank you, Mr. Chairman.

I am very pleased to be here today to discuss ECPA reform generally and location data specifically. I have been working with ECPA for over 13 years—first, as a DOJ attorney who used to teach prosecutors and agents how to acquire electronic evidence, and for the last 10 years as a lawyer, helping ISPs and wireless providers respond to the government's request for data. As a result, I can tell you three things about ECPA. First, it is complicated.

Second, it has done a fairly good job over the past 20 years in striking the right balance between law enforcement needs and user privacy. But now it is definitely in need of reform to bring its privacy protections into the modern age of cloud computing, social networking and mobile networks.

One area where ECPA no longer functions well is with regard to location data. This morning I want to focus——

Mr. NADLER. Excuse me. Could you tell me what you—tell us what you mean by cloud computing?

Mr. ZWILLINGER. The storage of data as opposed to locally on your computer in your possession, out in the network on the Internet in the cloud.

Mr. NADLER. Thank you.

Mr. ZWILLINGER. With regard to location data, ECPA is not functioning very well anymore. And I would like to focus on three of the issues I put forth in my written statement—one, the type of location data that raises privacy concerns; second, the discrepancy between acquiring real-time data and historical data; and third, to answer Mr. Johnson's question, the reason why Congress should not wait for the courts to resolve these issues.

First, as to location data generally, of course, Mr. Littlehale is right. Law enforcement obtains a wide variety of records that provide insight into a person's past location. For example, a landline call or a credit card receipt can shed light on where a person was at a given moment in time. But when those transactions occur, it is reasonably clear that some record is being made of that event, and only limited information about an individual's movements is disclosed.

The type of location data that concerns us here has the opposite characteristics. It may be collected without a person's knowledge, and it allows the tracking of a person's movements on a relatively precise and continuous basis. This type of tracking is much more persistent and much more intrusive than the disclosure that I bought a coffee at Starbucks at 9 o'clock this morning.

This is why it is also a mistake to think about ECPA reform solely in the context of relatively imprecise cell site location information, because whatever the limitations are on cell cite limitation today, cell tower data will rapidly evolve into the more precise and consistent information that is being supplied by GPS technology.

Second, as to getting historical data versus prospective data, the existing statutory framework clearly distinguishes between the

two. As to past location data, the application of ECPA is fairly straightforward. Location data, at least for calls, is properly considered a record or other information pertaining to a subscriber or customer, which the government may get under Section 2703(d) of the Stored Communications Act using the specific and articulable facts standard that is explained in Judge Smith's chart.

But the framework for real-time data is not anywhere near as clear. On their face you would think that the pen register and trap and trace statutes would allow the government to access location data under a relatively low standard that requires a court to issue a pen and trap order whenever a government agent certifies that the location information is relevant and material to an ongoing investigation.

But when Congress passed CALEA in 1994, it precluded law enforcement from relying solely on pen/trap authority. The government's workaround, which you have heard about, has been to combine the authority of a pen/trap order with the historical request for data under Section 2703(d). But this doesn't work.

An order under 2703(d) can only provide access for historical records, not prospective data. It is not a surveillance statute, and there are no provisions in 2703(d) that contemplate future surveillance or provide limitations on the duration and minimization and monitoring. So it can't be the additional authority that Congress needed in 1994 when it said that law enforcement could not rely solely on pen/trap.

So how can it be that there are different rules for obtaining information about where I was an hour before an order was signed compared to an hour after an order was signed? Those rules are entirely different and clearly to this date unresolved.

Some courts have tried to fix this discrepancy by creatively applying the tracking device statute found in 18 USC 3117 to apply to both types of data, but as I described in my written testimony, I don't think the tracking device statute can apply to a consumer's own electronic devices.

But the fact that courts are trying to do so is strong evidence of the need for Congress to step in and harmonize the before and after rules for the same set of information and to set a properly robust standard for the government to meet before it obtains precise location data.

Finally, as to Mr. Johnson's question, I don't think Congress should expect that the problem will be resolved by the courts anytime soon. First, the application of the Fourth Amendment to location data is uncertain. Even if every device that emitted location information was considered a tracking device, the Fourth Amendment alone would not necessarily mandate a prior warrant to collect information from these devices.

In fact, in *Knotts* and *Karo,* the leading Supreme Court cases, the court suggested that a warrant is only required when the data from a tracking device reveals information about private spaces. Certainly, cell phones may be carried into private spaces, but not always in private spaces.

And second, just last week in the *Quon* case, the Supreme Court deliberately shied away from extending Fourth Amendment protections to rapidly evolving technology.

So in conclusion, I don't think Congress should share the court's reluctance to address privacy concerns created by modern technology. Competing claims over privacy rights are being litigated on a daily basis. And as everyone struggles to apply a 1986 law to technology that is becoming more precise in its ability to pinpoint location, the time is ripe for Congress to set out clear and sustainable rules that better balance user expectations and law enforcement needs in light of modern technology.

Thank you for the opportunity to testify today.

[The prepared statement of Mr. Zwillinger follows:]

PREPARED STATEMENT OF MARC J. ZWILLINGER

**Written Statement of Marc J. Zwillinger**

**Partner**

**Zwillinger Genetski LLP**

**before the**

**U.S. House of Representatives Committee on the Judiciary**

**Subcommittee on the Constitution, Civil Rights, and Civil Liberties**

**Hearing on**

***ECPA Reform and the Revolution in Location Based Technologies and Services***

**June 24, 2010**

Chairman Nadler, Ranking Member Sensenbrenner and Members of the Subcommittee, thank you for the opportunity to testify about ECPA reform, and specifically about issues relating to historical and real-time location data. By way of background, I served as a Trial Attorney in the United States Department of Justice Computer Crime and Intellectual Property Section from 1997-2000, and for the last ten years I have been representing companies, including internet service providers, social networking companies, and wireless providers on issues related to electronic surveillance and the Electronic Communications Privacy Act. As part of that work, I have litigated surveillance-related issues in district and appellate courts across the United States. I also teach a course in cybercrime law as an adjunct professor at the Georgetown University Law Center in Washington, D.C. I have also been involved in the Digital Due Process Coalition for the last 2 years. I am testifying today solely in my individual capacity and not on behalf of any clients or the Digital Due Process Coalition.

Let me begin by saying that as someone who spends nearly every day dealing with complicated issues arising under ECPA, I believe that ECPA is in need of reform, especially to bring the privacy protections for both transactional and stored communications into the modern age of cloud computing, social networks and mobile devices. And while today's discussion of location-based data is important, the uncertainty of ECPA's application to content stored in the cloud and its flat prohibition on access to contents in civil matters and for criminal defendants provides even more justification for amending ECPA. In many ways, ECPA has done remarkably well in striking the right balance between law enforcement needs and users' privacy interests for the past 25 years. Unfortunately, there are several specific areas where ECPA's balance no longer works effectively. This has happened for the very reason that the Supreme Court recently noted in *Quon*, "rapid changes in the dynamics of communication and information transmission are evident, not just in the technology itself but in what society accepts as proper behavior." *City of Ontario, California, et al. v. Quon*, Dkt. No. 08-1332, slip. op at 11 (June 17, 2010).

Before examining how the statutory regime applies to location-based data, it is important to define the types of location-based information that are driving the concern about ECPA reform. Law enforcement certainly may obtain a broad array of information that provides knowledge about a person's location at a given moment in time. For example, law enforcement can use a record of a landline phone call, an in-person credit card transaction, or use of a rechargeable fare card for public transportation to pinpoint a person's location at a particular time. Traditionally, law enforcement has obtained these records for use in criminal investigations without causing significant privacy concerns. Presumably, this is for two reasons: (1) it was clear to the person engaging in such transactions that his or her interaction at that point in time was being recorded; (2) the transactions provide information about an individual's location at a specific moment in time, but do not provide a stream of continuous location data that could be used to track his or her specific whereabouts.

Consequently, the types of data that do raise serious privacy concerns under existing law are those that have the opposite characteristics: (1) information that may be collected without the subject's knowledge, like cell-site data that is collected even when a call is not in progress; and (2) data that provides the ability to track all of a person's movements on a relatively precise and continuous basis. This information tends to appear most often in electronic form and is maintained and collected by providers covered by ECPA. With regard to this type of location data, ECPA's statutory framework is profoundly unsatisfying. It creates a different set of rules for historical and prospective location data, and it fails to provide clear guidance for situations in which the government seeks to track an individual's precise movements, leaving the answer to the general application of Fourth Amendment principles and significant variation across jurisdictions.

To explain why legislation is appropriate, I will first examine how the DOJ currently obtains historical location data including Cell Site Location Information, also known as CSLI. Next, I will discuss how DOJ seeks to obtain prospective location data. Finally, I will conclude by pointing out the flaws in DOJ's approach and the benefits of legislative reform.

**Historical Location Data:**

Most of the established precedent on location-based data relates to law enforcement requests for historical CSLI. There should be no real question that the Stored Communications Act ("SCA"), 18 U.S.C. § 2701, *et. seq.* currently governs the government's authority to obtain this type of data. The SCA describes the circumstances in which an electronic communications provider can disclose records or other information pertaining to a subscriber or customer (with the exception of the contents of the subscriber's communications). As the SCA makes clear, every piece of information maintained by an electronic communications service provider must fit into one of the four categories of data described by the statute: (1) contents of communications in electronic storage; (2) contents of wire or electronic communications in a remote computing service; (3) records or other information pertaining to a subscriber or customer; or (4) basic subscriber information of the type described in 18 USC § 2703(c)(2). Of those categories, nearly every bit of non-content transactional information a provider maintains falls into the 3rd category – "records or other information pertaining to a subscriber or customer," all of which is obtainable though an order issued pursuant to 18 U.S.C. § 2703(d).

For historical location data to be available to the government under the provisions of 18 U.S.C. §2703(d) only three things have to be true: (1) the provider has to be a "provider of electronic communication service"; (2) the data has to be "a record or other information pertaining to a subscriber or customer of" an electronic communications service; and (3) the data may not be "content" information, which is defined by the SCA as "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8). For the most part, location data that accompanies a call does not provide information related to the substance of the communication, rather it is ancillary data conveyed so that the wireless telephone can connect with the nearest cell tower. It is not the content of the communication.

This may not continue to be the case, however, with regard to new location-based Internet services, which, unlike cell site location data, are designed to track location data, either because the user voluntarily enters their location in text-based fields (like on Facebook) or specifically authorizes the transmission of GPS information so that the user can get directions through Google Maps or connect with friends (as on Foursquare). In these instances, there is certainly an argument that the uploaded and/or transmitted location data is in fact the "content" of the communication because it is not information necessary for the connection of some other communication, but is rather information the user intentionally transmits to a third party (directly or through an application) because communicating the location information itself is the purpose of the transmission.

This is why thinking about location data only in the context of cell tower data is misleading and should not be the paradigm through which Congress views ECPA reform. But in the specific context of information collected by wireless service providers as an integral step in providing wireless service, the information should be obtainable through the use of an Order under 18 U.S.C. § 2703(d), which requires the government to proffer "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."

**Real-Time Location Data:**

The current process through which the government may obtain real-time or prospective location data, whether for cell sites, or otherwise, is more complicated and uncertain, especially because it implicates statutes beyond ECPA. The starting point for understanding this process is the language of the pen register/trap and trace ("PRTT") statutes,[1] which, on their face, allow the government to obtain an order to get access to "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted," and/or "dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." 18 U.S.C. §§ 3127(3) and (4). If this were the only relevant authority, the analysis for cell site location data would likely end here, because the location data transmitted by a cell phone at the outset or receipt of a call has been held to fall within this definition. Again, if we consider location-based data provided by other devices, such as GPS or navigation devices whose main purpose is to transmit location data, it is not at all clear that the PRTT statutes would continue to apply.

Where they do apply, however, the showing applicants must make in order to obtain a PRTT order is less than the showing they must make under the 2703(d) standard for historical location data, at least with regard to devices that send or receive electronic communications. Under the PRTT statutes, to obtain a pen/trap order, applicants must only identify themselves and the law enforcement agency conducting the investigation and certify their belief that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the agency. *See* 18 U.S.C. § 3122(b)(1)-(2). So long as the application contains

[1] 18 U.S.C. § 3121, *et seq.*

these elements and the issuing court has jurisdiction over the offense being investigated the court is required under the statute to authorize the installation and use of a pen/trap device anywhere in the United States. *See* 18 U.S.C. § 3122(a); 18 U.S.C. § 3127(2)(A).

Under the SCA and PRTT, it appears that prospective location data (at least with regard to devices that send or receive electronic communications) receives less protection than historical location data. However, the analysis extends beyond the scope of these statutes. When Congress passed the Communications Assistance for Law Enforcement Act ("CALEA") in 1994, it included a provision now codified at 47 U.S.C § 1002(a)(2), which states that "[w]ith regard to information acquired solely pursuant to the authority of pen registers and trap and trace devices, such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)." Absent this prohibition, it is likely that the pen register and trap and trace statutes alone would be sufficient to authorize the collection of location data. Therefore, it is CALEA, and not ECPA, that precludes the collection of location data from cell phones under the standard for Pen Registers and Trap and Trace devices. It does not necessarily preclude their use for location information derived from other types of devices that are not subject to CALEA.

Given CALEA's language, the government has struggled to come up with an alternative theory for obtaining location data on a prospective basis without first obtaining a warrant under Rule 41 of the Federal Rules of Criminal Procedure. Given the state of Fourth Amendment jurisprudence, this is an understandable impulse because current Fourth Amendment case law suggests that a prior warrant may not be necessary to track an individual's location in purely public spaces.[2] The government's preferred method is to combine the authority of a pen register and trap and trace with the authority previously described under 18 U.S.C. 2703(d) for obtaining historical location data. The government's theory is essentially that by combining the authority to obtain prospective data under the PRTT statutes with the greater judicial showing necessary for historical data under the § 2703(d) standard, the government avoids the CALEA prohibition against "solely" relying on the authority of the PRTT statutes. This theory has been rejected by many courts, but accepted by some, as an acceptable method for obtaining prospective location data.[3]

---

[2] Thus, law enforcement has not been required to obtain a search warrant before affixing a GPS tracking device to the outside of an automobile that is parked on a public street. *United States v. Pineda-Moreno*, 591 F.3d 1212 (9th Cir. 2010) (placement of tracking device on exterior of vehicle while parked in defendant's driveway, while on public streets and while in a parking lot did not violate Fourth Amendment); *United States v. Garcia*, 474 F.3d 994 (7th Cir. 2007) (installation of a battery-power GPS device on the exterior of a vehicle does not implicate Fourth Amendment rights); *United States v. McIver*, 186 F.3d 1119 (9th Cir. 1999) (installation of a magnetic GPS device and magnetic beeper on the outside of a vehicle does not constitute a search under the Fourth Amendment).

[3] *See e.g. In re Applications of the United States for Orders Authorizing the Disclosure of Cell Cite Information*, 2005 WL 3658531 (D.D.C. Oct 26, 2005); *In re Application of the United States for Orders Authorizing Installation and Use of Pen Registers and Call Identification Devices*, 416 F. Supp.2d 390 (D. Md. 2006); *cf. In re Application of the U.S. for an Order for Disclosure of Telecommunications Records*

This theory has also been embraced by the Department of Justice in the 2009 Version of the Manual for Searching and Seizing Computers and Obtaining Electronic Evidence, published by the DOJ's Computer Crime and Intellectual Property Section. The manual states:

> The rationale behind this "hybrid" use of the Pen/Trap statute and § 2703(d) is as follows. Cell-site data is "dialing, routing, addressing, or signaling information," and therefore 18 U.S.C. § 3121(a) requires the government to obtain a pen/trap order to acquire this information. However, the Communications Assistance for Law Enforcement Act of 1994 ("CALEA") precludes the government from relying "solely" on the authority of the Pen/Trap statute to obtain cell-site data for a cell phone subscriber. 47 U.S.C. § 1002(a). Thus, some additional authority is required to obtain prospective cell-site information. Section 2703(d) provides this authority because, as discussed in Chapter 3, supra, it authorizes the government to use a court order to obtain all non-content information pertaining to a customer or subscriber of an electronic communication service.

Yet, despite the DOJ's endorsement, this theory is flawed. Its principal failing is that an order granted under Section 2703(d) cannot provide law enforcement with the authority to obtain prospective information; its reach is limited instead to historical records. There is not a single provision of the SCA that contemplates prospective surveillance, nor are there ancillary provisions that address the duration or scope of prospective monitoring activities. In contrast, such provisions are found in every other statute that contemplates future monitoring. Thus, it is apparent that §2703(d) as written was not intended to, and cannot, provide the requisite supplemental authority necessary under CALEA to permit law enforcement to capture real-time location based data. As a result, the hybrid theory must fail as a matter of statutory construction, leaving a Rule 41 Warrant (or a Title III Order) as the sole method of obtaining prospective location data.

In addition to the statutory construction argument, district courts have cited other reasons for rejecting the hybrid theory. For example, some courts have asserted that that cell phones are "electronic or mechanical device[s] which permit[] the tracking of the movement of a person or object" and therefore should be considered "tracking devices" under 18 U.S.C. § 3117(b). This is turn, they argue, would mean that cell site location information would be explicitly excluded from the definition of "electronic communications" under 18 U.S.C. 2510(12), and consequently that neither prospective nor historical location data could be provided to law enforcement under the authority of §2703(d). As applied to either prospective or historical data, this theory has two problems. First, it assumes that any device that a consumer chooses to carry that reports location information becomes a tracking device under

---

*and Authorizing the use of a Pen Register and Trap and Trace,* 405 F. Supp. 2d 435 (S.D.N.Y. 2005); *In re Application of the U.S. for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; and (2) Authorizing Release of Subscriber Information and/or Cell Site Information,* 411 F. Supp. 2d 678 (W.D. La. Jan. 26, 2006).

federal law whenever the government seeks to have access to the information it provides – and there is simply no text or legislative history to support that conclusion. The tracking device statute is designed to cover tracking or homing devices surreptitiously installed by the government. The government may need to seek prior judicial authorization under Rule 41 to surreptitiously install a tracking device on a person or that person's property, but getting records for a device that the consumer voluntarily owns and operates appears to be a separate issue.

Second, and perhaps more importantly, the Stored Communications Act does not exclude tracking device communications from the category of information that can be provided pursuant to 18 U.S.C. § 2703(c). Once an entity is deemed to be a provider of electronic communications – that is a provider that allows users to send and receive either wire or electronic communications – it must provide "records and other information pertaining to [its] subscriber[s] to or customer[s] of such service (not including the contents of communications)" whenever it receives a Court Order issued under 2703(d). Nowhere in this section is it written that these records or other information must themselves be records of electronic communications. In fact, many are not. Further, while Congress chose to explicitly exclude the contents of communications from the records to be provided, it did not provide an exception for communications that may reveal location information. Whereas a provider that solely provides communication services to tracking devices might not be an eligible recipient of a 2703(d) Order, entities that provide tracking device services in addition to other communications services are certainly obliged to provide location-based data when the statutory prerequisites are met.

The search for creative solutions – such as leaning on tracking device provisions – by both privacy advocates and courts is strong evidence of an emerging desire to ensure that reasonably precise real-time and historical location-based information is treated similarly under the law and that a properly robust standard must be met before this type of data is obtained. This makes sense, because information on where an individual has traveled for the hour before a request is made has the same level of intrusiveness as to the information about where the same individual is going to be for the next hour on a real-time basis. But, given the current state of the law, Congressional action is needed to bring about this result.

Without legislative intervention, courts will continue to issue conflicting decisions with differing standards and exacerbate uncertainty amongst law enforcement agencies and providers as they struggle to apply a 1986 law to technology that is only becoming more precise in its ability to pinpoint location and provide an ever expanding universe of information. Further, Congress cannot wait and expect that courts will sort out this problem through proper application of Fourth Amendment doctrine. This is partly because of the Private/Public line that courts have drawn in Fourth Amendment jurisprudence. Even if all devices that provide location-based information were deemed to be "tracking devices" under existing law, the Fourth Amendment would not necessarily require a prior warrant to get information from these devices. The Supreme Court has held that the Fourth Amendment Warrant requirement is applicable only where the information provided by a tracking device reveals information about a person's activities in the interior of constitutionally-protected private spaces, rather

than a public space.[4] So, government would not necessarily need a warrant – either historically or prospectively – to obtain location data about an individual whenever he ventures into a non-constitutionally protected space, but would likely need a warrant when the device is transmitting information from a private space. Such jurisprudence makes it difficult to determine the appropriate standard in advance in all circumstances without statutory guidance. Moreover, we certainly cannot expect the courts, especially the Supreme Court, to address the issue with any alacrity. When presented this past month with an opportunity to apply the Fourth Amendment to text messages sent by public employees, the Court declined indicating that:

> [It] 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 Amendment implications of emerging technology before its role in society has become clear. *City of Ontario, California, et al. v. Quon*, Dkt. No. 08-1332, slip. op at 10 (June 17, 2010).

Nor would a court-devised solution be necessarily preferable. Addressing this issue legislatively has benefits both for law enforcement and for privacy rights. For users, amending ECPA to cover this issue would allow Congress to also cover the ancillary issues raised by such surveillance, such as the appropriate duration for orders, need for record-keeping, immunity for providers who comply with orders, emergency disclosure and consent exceptions, and other types of issues found in the prospective monitoring statutes. As for Law Enforcement, a Congressional solution would recognize that the entirety of Fourth Amendment doctrine need not be imported into the new statute and could allow the government more flexibility on issues of particularity and minimization, than if this issue were covered by the Fourth Amendment.

In conclusion, Congress should not mimic the Court's reluctance to move Fourth Amendment doctrine into the 21st century, but instead should take it as a call to arms. Competing claims over privacy rights are contested daily; and in some ways the need for legislative action is even greater now than it was in 1986 when ECPA was originally passed. As the courts and law enforcement struggle to keep pace with rapidly evolving technology and the accompanying expanding universe of information available from service providers, the time is ripe for Congress to set forth clear and sustainable ground rules that balance user expectations and law enforcement needs.

Thank you for the opportunity to testify today. I would be pleased to continue to work with the Committee as the ECPA reform process moves forward.

---

[4] *United States v.* Karo, 468 U.S. 705 (1984) (finding once a beeper has been taken inside a private residence law enforcement must acquire a warrant to monitor it); *United States v. Knotts*, 460 U.S. 276, 282 (1983) (finding that when officers monitor a "beeper" to assist them in conducting surveillance of a vehicle's movements along public roadways, they are not conducting a Fourth Amendment search, as there is no reasonable expectation of privacy on a public road).

Mr. NADLER. Thank you.

And I will now recognize Judge Smith.

**TESTIMONY OF THE HONORABLE STEPHEN WM. SMITH, UNITED STATES MAGISTRATE JUDGE, SOUTHERN DISTRICT OF TEXAS**

Judge SMITH. Thank you, Mr. Chairman, Ranking Member, Members of the Subcommittee. I am honored by your invitation to appear at today's hearing. I am a United States magistrate judge, but I am testifying on my own behalf this morning, not on behalf of any group or organization. But it is testimony informed by hands-on experience with ECPA over a number of years.

Ordinarily, your Committee would probably be better served by hearing from a Supreme Court justice or Court of Appeals judge steeped in the law, able to give a full exposition of its strengths and flaws based on years of experience and observation. But on this topic, cell phone tracking, that would not be possible. Very few appellate courts have dealt with ECPA in any respect over the years, and as Exhibit B to my written testimony shows, not a single one to date has dealt with the question of legal standards or compulsory government access to cell site location information.

Ponder this fact. For nearly a quarter-century, magistrate judges have been issuing tens of thousands of these orders under a fiendishly complex statute without any substantial guidance from a higher court. And I can't think of another area of law in which that could be said. You know, FISA, perhaps—Foreign Intelligence Surveillance Act—but then FISA is a special case and was understood to be a departure from routine law enforcement for everyday crime.

I believe that is an unhealthy state of affairs for our democracy. First, without a functioning system of appellate review, the process of refinement, clarification of statutory ambiguity and uncertainty cannot take place. And this is especially unfortunate for a statute as complex as ECPA.

A more serious concern is that a basic check on judicial as well as prosecutorial power has been removed. Without the discipline of appeal, every magistrate judge essentially becomes a law unto himself or herself answerable to no one. And law enforcement is able to channel their ex parte applications to a judge known to have a more accommodating view of the law.

Now, this does not happen with respect to ordinary search warrants. The cause of this unhealthy state of affairs, in my opinion, is the regime of secrecy that has enveloped——

Mr. NADLER. Excuse me. Why does this not happen with ordinary search warrants?

Judge SMITH. Well, because ordinary search warrants are issued pursuant to a warrant under the statute under Rule 41, and under that rule the party whose house is being searched gets notice, receives a copy of the warrant. Typically, they are not sealed.

Mr. NADLER. It is not ex parte.

Judge SMITH. Right. It is not—well, it is ex parte, but before the search is carried out, the person whose home is being searched——

Mr. NADLER. Gets notice.

Judge SMITH [continuing]. Gets notice.

Now, the cause of this unhealthy state of affairs, as I said, is the regime of secrecy. Under ECPA gag orders and permanently sealed cases prevent law-abiding citizens from finding out whether and to what extent their electronic lives have been intruded upon by government. Again, this does not happen when law enforcement searches your home or your office or your car.

The difference boils down to notice. Now, without notice, and this can be pre-acquisition or post-acquisition, but without notice, due process of law becomes a dead letter.

So I applaud the Committee's efforts to reform ECPA to face the new technological advances of the 21st century, but the problem with 20th-century ECPA is not just that it failed to anticipate new technology. Few of us back then could have imagined the cell phone of today and what it can do.

The problem is that it is an overly complex statute that was allowed to operate almost entirely in the dark, off the radar screen of the general public as well as appellate courts. Thus, the balance that it struck, at least in my view, between privacy and law enforcement has been eroded. And few seemed to notice, at least until now.

Now, your task will be to strike a new balance that will be sustainable for our time and time to come. My prescription for sustainability is twofold—more bright lines and more sunshine. I believe the principles endorsed by the Digital Due Process Coalition go a long way toward the former goal. I think my written remarks suggest some ways to accomplish the latter.

In closing, I want to thank this Committee for inviting the views of one of the hundreds of magistrate judges who wrestled in the trenches, as you say, with this statute for years. And with that, I would be glad to answer any of your questions. Thank you.

[The prepared statement of Judge Smith follows:]

PREPARED STATEMENT OF THE HONORABLE STEPHEN WM. SMITH

Before the
Committee on the Judiciary
Subcommittee on the Constitution, Civil Rights, and Civil Liberties
2237 Rayburn House Office Building
Washington, D.C. 20515

HEARING ON ELECTRONIC COMMUNICATIONS PRIVACY ACT REFORM
AND THE REVOLUTION IN LOCATION BASED
TECHNOLOGIES AND SERVICES

June 24, 2010

Written Testimony of
United States Magistrate Judge
Stephen Wm. Smith

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

I am honored by your invitation to testify at today's hearing. I am a U.S. Magistrate Judge for the Southern District of Texas, sitting in Houston. While this testimony is my own, and not offered as the official position of any group or organization, it is a view from the trenches shared by many of my fellow magistrate judges across the country. Before reaching the substance of my testimony, it might be helpful to outline the role of magistrate judges in handling law enforcement requests under ECPA.

## 1. Role of Magistrate Judges in Electronic Surveillance[1]

There are over 500 federal magistrate judges serving in district courts around the country. In addition to civil matters, our responsibilities on the criminal side generally include almost everything except conducting felony trials. We conduct initial appearances, appoint counsel for indigents, set bail conditions, hold detention hearings, issue criminal complaints and arrest warrants, take grand jury returns, handle extradition requests, misdemeanor trials, competency hearings, and suppression motions. One of our chief functions is to issue search warrants and other orders in aid of criminal investigations. These include electronic surveillance orders for pen registers, trap and trace devices, tracking devices, 2703(d) orders for telephone and e-mail account records and activity. That is where our experience with ECPA comes in.

Although different districts may handle it differently, in most districts there is at least one magistrate judge on criminal duty at all times, ready to take a call 24 hours a day, 7 days a week. In the Houston division we have 5 magistrate judges, and we rotate the criminal duty among ourselves every two weeks. While on duty we carry either a beeper or dedicated cell phone to allow instant access by law enforcement. It is not uncommon for a magistrate judge to be contacted at night or on a weekend to issue electronic surveillance orders in cases of emergency, such as a kidnaping or alien smuggling. With rare exceptions, ECPA orders pertain to ordinary crimes and criminals, not national security or terrorism cases.

The process is *ex parte*, meaning only one party – law enforcement – appears before the magistrate judge. Since this is at the criminal investigation stage, no

---

[1] For purposes of my testimony, "electronic surveillance" includes pen registers, trap and trace devices, tracking devices, cell site information ("CSI"), stored e-mail, telephone and e-mail activity logs, and customer account records from electronic service providers. Wiretap orders, which are issued only by district judges, are not included.

defendant has yet been charged so no defense counsel is there to challenge the government's request. Likewise, no representative of the electronic service provider or the target phone's subscriber is present. In fact, the orders routinely contain gag orders precluding the service provider from advising their customers that the government is accessing their cell phone or e-mail account records. The public rarely learns about these orders, even long after issuance, because they are routinely placed under indefinite (*i.e.*, permanent) seal.

Actual data on the number of electronic surveillance orders issued under ECPA is not readily available, as far as I know.[2] However, some idea can be gleaned from a recent survey by the Federal Judicial Center.[3] This study, which looked at the prevalence of completely sealed cases in federal court, surveyed every federal case filed in all federal courts during 2006. It found that of the 97,155 criminal matters handled by magistrate judges that year, 15,177 were completely sealed from public. The vast majority of those were warrant-related applications.

Another data point is provided by a local survey of such orders issued by our court in Houston from 1995 through 2007. According to that survey, Houston's five magistrate judges issued a total of 4,234 electronic surveillance orders, or about 325 every year.[4] Considering that this volume was generated by less than 1% of the federal magistrate judges in the country, it is safe to conclude that the 2006 total in the FJC study was not a fluke. A reasonable estimate is that the total number of electronic surveillance orders issued at the federal level each year substantially exceeds 10,000.[5]

---

[2] ECPA requires the Attorney General to report to Congress the number of pen registers applied for annually. *See* 18 U.S.C. § 3126. However, there is no separate reporting requirement for tracking devices under § 3117 or location information obtained under § 2703(d).

[3] The study is available online at: www.fjc.gov/public/pdf.nsf/lookup/sealcafc.pdf/$file/sealcafc.pdf.

[4] *See In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders,* 562 F.Supp.2d 876, 895 (S.D. Tex. 2008).

[5] This does not include the number of such orders issued by state courts.

## 2. In Pursuit of Hidden Elephants[6]

I took the bench in 2004, having no background in criminal law. In fact I had never heard of a trap and trace device until I was confronted with an application for one on my first day of criminal duty. The application also asked for something called "cell site information." Reluctant to sign what I did not understand, I turned to the United States Code and encountered ECPA for the first time. The experience was frustrating: the terminology was unfamiliar, the organization not intuitive, and the syntax far from straightforward. The casenotes accompanying the statute shed no light; they cited only a handful of lower court decisions not particularly relevant to my questions. No appellate court had ever addressed the issue. I asked my colleagues on the bench, and found they were just as puzzled as I was. I tried to look at sample orders from other courts, but found that they were sealed. I met (several times) with the AUSAs, who basically argued that their request should be granted because other judges had done so.

Still unsatisfied, I plunged into the legislative history of ECPA, reading every committee report and law review article I could find. I contacted law professors who had written about ECPA, as well as a former Congressional staffer who had helped draft the law and subsequent amendments. I met with our local U.S. Marshals, who gave me a tour of their local electronic surveillance shop and a demonstration of the technology. I called various service providers to get their perspective. I then spent several months drafting a memo, setting out my tentative conclusions and supporting analysis. I sent the memo to our local U.S. Attorney, asking him exactly what was wrong with my analysis and why. He forwarded the memo to DOJ, which responded months later with a detailed rebuttal, advocating what has since come to be known as the hybrid theory. Unpersuaded, I issued my first opinion on cell site information in October 2005.[7]

***Prospective CSI.*** From my research, I came to understand that ECPA authorized various criminal investigative tools under four different legal standards.

---

[6] "[Congress] does not, one might say, hide elephants in mouseholes." *Whitman v. American Trucking Ass'n,* 531 U.S. 457, 468 (2001) (Scalia, J.).

[7] *In re Application*, 396 F.Supp.2d 747 (S.D. Tex. 2005). This was actually the second published decision on the topic. Magistrate Judge James Orenstein had issued a decision reaching the same conclusion two months earlier, although the government did not make the hybrid argument in support of that application. *See In re Application of the U.S.*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005).

Generally speaking, the more intrusive the investigative tool, the greater the legal process necessary to access it. Visualize it as a 4-story courthouse: pen registers and trap/trace devices are on the ground floor, having the least demanding standard ("certified relevance");stored communications and account records are on the second floor, accessible with "specific and articulable facts";[8] tracking device warrants are on the third floor, covered by the familiar Rule 41 "probable cause" standard; wiretap orders are on the top floor, with their "super-warrant" requirements. A chart illustrating this "Electronic Surveillance Courthouse" is attached as Exhibit A.[9]

The essential difficulty, of course, is that ECPA does not explicitly refer to "cell site" or other location information from a cell phone. In the case before me, the Government sought compelled access to a full range of cell site information (CSI) on a prospective basis.[10] My basic approach was to determine which floor of the courthouse was the best fit for this type of request. Because the Government's stated purpose was to locate the target phone user in real time, the most obvious candidate seemed to be the third floor, for tracking devices. The statutory definition of a tracking device is very broad and unqualified, and could easily be read to encompass the unlimited CSI sought here.[11] Moreover, none of the other categories of electronic surveillance seemed to fit. The pen register standard was ruled out by a proviso in a 1994 statute known as CALEA.[12] The wiretap standard did not apply because CSI does not reveal the contents of a communication. The Stored Communications Act (SCA) standard did not seem to apply for two reasons: the definition of "electronic

---

8 This is an oversimplification, but sufficient for our purpose. *See* 18 U.S.C. § 2703.

9 Again, this chart oversimplifies in several respects. For example, it ignores the complicating distinction between communications held in a remote computing service and those held in electronic storage by an electronic communications service provider. It also excludes non-judicial processes such as administrative and grand jury subpoenas.

10 The application sought "the location of cell site/sector (physical address) at call origination (for outbound calling), call termination (for incoming calls) and, if reasonably available, during the progress of a call," in addition to "the strength, angle, and timing of the caller's signal measured at two or more cell sites, as well as other system information such as a listing of all cell towers in the market area, switching technology, protocols, and network architecture." 390 F. Supp. 2d at 749.

11 *See* 18 U.S.C. § 3117(b) ("the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object.").

12 The Communications Assistance to Law Enforcement Act, 47 U.S.C. § 1002(a)(2).

communication" specifically excludes information from a tracking device;[13] and the structure of the SCA was inherently retrospective, allowing access to documents and records already created, as opposed to prospective real time monitoring. I concluded that there was "no reason to treat cell phone tracking differently from other forms of tracking under 18 U.S.C. § 3117, which routinely require probable cause."[14]

Other magistrate judges soon began to weigh in with published decisions of their own. Many agreed with me, some did not. The first opinion with a contrary view was issued in December 2005 by Magistrate Judge Gabriel Gorenstein in the Southern District of New York.[15] He held that a limited form of prospective CSI[16] could be obtained under the SCA standard of specific and articulable facts, a lesser showing than probable cause. His opinion accepted the Government's hybrid theory and provided what remains its most cogent expression to date. In essence, that theory argued that a lesser standard for obtaining this information could be implied from a combination of provisions in three separate statutes.[17] Even as he was adopting the hybrid theory's conclusion, Judge Gorenstein declared the result "unsatisfying,"

---

13 18 U.S.C. § 2510(12)(C).

14 396 F. Supp.2d at 757. The opinion closed by expressing hope "that the government will seek appropriate review by higher courts so that authoritative guidance will be given the magistrate judges who are called upon to rule on these applications on a daily basis." *Id.* at 765. Unfortunately, with a single exception in five years, that plea has fallen on deaf ears.

15 405 F. Supp. 2d 435 (S.D.N.Y. 2005).

16 His order "contemplates the production only of: (1) information regarding cell site location that consists of the tower receiving transmissions from the target phone (and any information on what portion of that tower is receiving a transmission, if available); (2) tower information that is tied to a particular telephone call made or received by the user; and(3) information that is transmitted from the provider to the Government." 405 F. Supp. 2d at 450.

17 I have compared this analysis (perhaps uncharitably) to a three-rail bank-shot: The first rail is the Pen Register Statute (as amended by the 2001 Patriot Act), asserted to be the exclusive means by which law enforcement might acquire non-content signaling information such as cell site data. The second rail is the 1994 CALEA statute, which provides that location information such as cell site data cannot be obtained "solely pursuant" to a pen/trap order. This was interpreted to mean that, while a pen/trap order is still a necessary condition for compulsory disclosure of cell site data, it is no longer sufficient, and must be combined with some additional authority. According to the Government, this authority is found in the third rail, otherwise known as the SCA, which allows Government access to cell phone customer records upon a showing of "specific and articulable facts."

given the lack of clear guidance from Congress.[18] Finally, he emphasized that his ruling was restricted to a limited form of CSI yielding only generalized location data.[19]

A spate of magistrate judge opinions followed in the next three years, and eventually even a few district judges weighed in. Surveying the published opinions, it is fair to conclude that the majority held that probable cause is the appropriate standard for government access to prospective cell site information. A minority of published decisions, following Judge Gorenstein, allow access under the lesser "specific and articulable facts" standard. Significantly, each of these opinions also restrict their holdings to limited CSI; not one reported decision has ever allowed access to unlimited (*i.e.*, multi-tower, triangulation or GPS) location data on anything other than a probable cause showing.[20] A chart of all published decisions to date concerning prospective cell site information is attached as Exhibit B.

***Historical CSI.*** A later round of published decisions centered on the question of government access to historical cell site data. The first wave of CSI decisions, even those requiring probable cause for prospective location information, had assumed or suggested that historical location information was not materially different from other forms of account records or customer information in the hands of the phone company, and therefore obtainable under the lesser standard of SCA § 2703(d). Although not the first decision to challenge that consensus, the most prominent was issued in 2008 by Magistrate Judge Lisa Pupo Lenihan on behalf of all magistrate judges sitting in the Western District of Pennsylvania.[21] Judge Lenihan reasoned that the text and legislative history of ECPA and its amendments warranted no "distinction between real-time ('prospective') and stored ('historic') cell-phone-derived

---

18 405 F. Supp. 2d at 442.

19 *Id.* at 449-50.

20 Most magistrate judges have not taken the time to issue published opinions on this question, so the possibility exists that published opinions are not a representative sample of magistrate judge opinion as a whole. Indeed, some standard government applications make the claim that "the silent majority of magistrate and district courts that routinely grant pen/trap/cell orders under the combined authority of Pen/Trap and SCA continue to do so without resort to publishing decisions affirming their current practice thus permitting the minority view to appear more pervasive than it is."

21 534 F. Supp. 2d 585 (W.D.Pa. 2008).

movement/location information."[22] Her decision is currently on appeal before the U.S. Court of Appeals for the Third Circuit. It is the first and to my knowledge the only time the Government has appealed any district court ruling on cell phone tracking. A listing of decisions addressing the standard for historical cell site information is included on Exhibit B.

Uncertainty over cell phone location information is hardly the only difficulty magistrate judges have encountered in dealing with ECPA. For example, there is the issue of post-cut-through dialed digits;[23] many others could be added. Those matters are beyond the scope of today's hearing, so there is no need to address them here. But when the Subcommittee does decide to take up those matters we hope that you will again afford magistrate judges the opportunity to offer you the benefit of our experience.

### 3. A Modest Prescription: Simplicity and Transparency

ECPA was passed in 1986 as a laudable attempt to balance the privacy rights of citizens and the legitimate interests of law enforcement, given the communications technology of that day. In reforming and updating ECPA for the 21st century, the task of finding the appropriate balance belongs first of all to the political branches. Obviously, there are important First and Fourth Amendment concerns to be weighed. As a judicial officer, I do not presume to advocate for either side of that debate. That said, from a magistrate judge's perspective, there are two systemic flaws in the existing statutory scheme that ought not be preserved in the next.

***Undue complexity***. The new statute should clearly specify the types of information available and the legal showing required for government access. To the extent distinctions must be made, legal standards should not be tied to a particular device or form of technology, which is probably on the road to obsolescence as you debate it. That type of standard inevitably presents judges with the most vexing of interpretive choices, forcibly fitting the round peg of tomorrow's technology into the square hole of yesterday's.

As a matter of logic, the legal standards for government access to location information should be geared to the level of intrusion into citizens' privacy. But in

---

22 Id. at 601.

23 *See In re Application of U.S.*, 622 F. Supp. 2d 411 (S.D. Tex. 2007) (Rosenthal, D.J.); *In re Application of U.S.*, 515 F. Supp. 2d 325 (E.D.N.Y. 2007) (Azrack); *In re Application*, 441 F. Supp. 2d 816 (S.D. Tex. 2006) (Smith).

my view the temptation to draw fine distinctions for different ways of monitoring cell phone location ought to be resisted. Even as to existing technology, those distinctions can be difficult to draw in the abstract. CSI comes in a wide variety of forms, offering differing tracking capabilities: Is there a meaningful distinction between CSI from a single urban tower and that from multiple rural towers? Between registration information or call-identifying information? What about "pings" or calls initiated by law enforcement? Should a different standard apply for location information pertaining to third parties calling or called by the target phone? How does one calibrate the relative degree of intrusion of such monitoring techniques, given that the precision of the location information obtained will vary from case to case, often depending on inferences drawn from other sources? For instance, when law enforcement already knows the business and residential addresses of the target (or the target's family, friends, and associates), a single phone call signal captured from a single tower may be all that's needed to reliably pinpoint a target's exact location at a given time.

Similar difficulties will plague any attempt to distinguish between historical and prospective cell phone information. How is "historical" to be defined – one second after transmission?[24] One hour? One day? One month? The case law to date has understandably sidestepped this knotty issue.[25] To avoid confusion, any dividing line will have to be explicit, and necessarily arbitrary. The term "prospective" is also ambiguous; although often employed as a synonym for "real-time," they are not really the same thing.[26] Real-time monitoring captures CSI the instant it is transmitted; it is the polar opposite of historical CSI. On the other hand, prospective CSI may be understood as referring to that generated anytime after the court issues its order. Thus, prospective CSI may well include not only real-time CSI, but also historical CSI generated while the order is in effect.[27] And what about historical CSI that is captured only at the instigation of law enforcement, and for which the provider has

---

[24] *See* Albert Gidari Jr., *Companies Caught in the Middle*, 41 U.S.F. L. Rev. 535, 544 (2007) ("In essence, [cell tower registration information] becomes historical, transactional information within a millisecond of when the provider receives it.").

[25] In my orders I take the position that "historical" CSI means any data existing as of the date of the order. This avoids the need to pick an arbitrary age limit.

[26] *See In re Application of the U.S.*, 402 F. Supp. 2d 597, 599 & n.5 (D. Md. 2005) (Bredar).

[27] Pen/trap orders typically expire after 60 days, although they may be renewed an unlimited number of times. 18 U.S.C. § 3123(c)(2).

no legitimate business reason to generate or maintain on its own. Should the standard to *create* CSI be different than that to *retrieve* CSI maintained in the ordinary course of business?

The task of drafting a rational, readily comprehended, easily administered statutory scheme to govern law enforcement access to electronic communications is daunting. Complicating that effort – by multiple distinctions based on predicted intrusion levels for different forms of location data – seems not only ill-advised, but also counter-productive. It's also likely to prove a waste of time in the wake of technology's inexorable advance.

***Undue Secrecy.*** As pointed out earlier, the vast majority of electronic surveillance orders are issued under seal. This of course is understandable – immediate disclosure of the target's name and number might defeat the purpose of the surveillance. The problem is the duration and extent of that secrecy.

Under ECPA, secrecy is achieved in two-ways: (1) gag orders preventing service providers from informing customers about law enforcement monitoring of their cell phone and e-mail usage; and (2) sealing orders denying public access to judicial orders.[28] Typically, electronic surveillance orders contain both types of provisions, but rarely impose an expiration period; instead, those orders remain in place "until further order of the court."[29] The catch is that there is no mechanism in place for the judge to revisit the sealing order. She does not retain jurisdiction over the case, which is not a "case" at all but an investigation that may or may not ripen into a real case. Other surveillance applications pertaining to that investigation will be given a separate case number and assigned to the judge on duty at the time.[30] The

---

[28] Pen register orders must be sealed, and must direct the provider not to disclose to anyone the existence of the order or the investigation, "until otherwise ordered by the court." 18 U.S.C. § 3123(d)(1) & (2). By contrast, the SCA does not require § 2703(d) orders to be sealed, and allows for "preclusion of notice" to others only if there is reason to believe the investigation would be jeopardized or other adverse consequences would result. 18 U.S.C. § 2705(b)(1)-(5). As a practical matter, the government routinely combines pen/trap applications with requests for customer information under § 2703(d), and so gets the benefit of the more restrictive pen register provisions.

[29] *In Re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 879-80 (S.D. Tex. 2008).

[30] In my court I have devised a protocol to deal with this problem: the order is initially sealed for 180 days, subject to extension upon a certification from the AUSA that the investigation is still active or that exceptional circumstances warrant the extension. *Id.* at 895.

upshot of this system is that, once sealed, an electronic surveillance order is likely to remain sealed long after the underlying investigation is closed, if not forever. This has been confirmed by a study of electronic surveillance orders issued by the Houston Division from 1995 through 2007. Out of 3,886 orders initially sealed "until further order of the court," 3,877 or 99.8% were still under seal as of April 2008.[31]

The brunt of such secrecy is not necessarily borne by the surveillance targets who are ultimately charged with a crime. After all, they are entitled to discover the nature and source of the prosecution's evidence, including electronic surveillance orders leading to arrest. Suppression motions are available in the event of a constitutional violation.[32] But not everyone caught up in the web of electronic surveillance is ultimately charged with a crime. Any target is likely to call or be called by family, friends, associates, or even total strangers who have no connection to a criminal enterprise. Yet by the fortuity of a single call, these by-standers may be swept up in a criminal investigation, their cell phone use monitored and their location tracked in real time. Unlike criminal defendants, however, these presumably law-abiding citizens will never find out. The phone company cannot tell them, and court-house records will disclose nothing. Ordinarily, a citizen whose house or office is searched is provided a warrant duly signed by a judicial officer, giving notice of the particulars of the search.[33] When a citizen wishes to challenge the legitimacy of a law enforcement search of his home pursuant to a warrant, the law affords due process for that purpose. But when searches are shrouded in permanent secrecy, as in most cases of electronic surveillance,[34] due process becomes a dead letter.

Such secrecy also has a pernicious impact on the judicial process of statutory interpretation. Any statute has its share of ambiguity and uncertainty, which is

---

31 *See* Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade,* 3 Fed. Cts. L. Rev. 177, 209-10 (2009) (hereafter *"Kudzu"*).

32 *See United States v. Forest,* 355 F.3d 942 (6th Cir. 2004).

33 These procedures are specified in Rule 41, which incidentally was amended in December 2006 to cover tracking device warrants. The rule does allow for deferred notice in special circumstances.

34 *See Kudzu, supra* at 208-211. There is also evidence of a trend toward permanent sealing of ordinary search warrants issued under Rule 41. *Id.* at 210. Until very recently, the sealing of a search warrant was regarded as an "extraordinary action" to be taken only in exceptional circumstances. *See* 3A Wright, King & Klein, Federal Practice and Procedure: Criminal 3D § 672, at 332-33 (2004).

resolved, case by case, through lower court rulings subject to review and correction by the courts of appeal and, ultimately, the Supreme Court. But this process of refinement and correction has not happened for ECPA. In a recent article I described this legal "black hole" for electronic surveillance orders:

> Due to a peculiar combination of circumstances, these sealed orders are entirely off the radar screen, not only for the public at large, but also for appellate courts. Consider a typical pen register order. The only affected party which might have an incentive to object – the targeted e-mail customer or cell phone user – is never given prior notice of the order; in fact, the electronic service provider is usually forbidden from disclosing its existence. The provider is compensated for most expenses in complying with the order; any uncompensated inconvenience hardly justifies an appeal. The government obviously has no reason to object when its application is granted; in the rare case of a denial, why risk an appeal that could make "bad law"? There are always other magistrate judges to try.
>
> Add a sealing order to this mix, and the outcome is a lacuna of law from which little light escapes. This is especially unfortunate because [ECPA] is fiendishly complex, made more so by the passage of the Patriot Act in 2001. Each year . . . busy magistrate judges issue hundreds of ex parte cell phone tracking orders with literally no appellate guidance concerning the proper showing for their issuance – probable cause versus something less. . . Thus, when it comes to marking the bounds of legitimate government intrusion into our electronic lives, each magistrate judge has effectively become a law unto himself. This cannot be a good thing.[35]

The case now before the Third Circuit is the exception that proves the rule. The first appellate court decision on the proper standard for government access to cell site data will be handed down nearly a generation after ECPA was passed, and nearly a decade after its amendment by the Patriot Act. At that rate, cell site data will likely be a quaint technological memory before the next appellate court can consider it.[36]

---

[35] *Kudzu, supra* at 211-12.

[36] One of the few appellate cases to deal with electronic surveillance in any respect illustrates the conundrum. *Warshak v. United States,* 532 F.3d 521 (6th Cir. 2008). The case arose after

Another consequence of this breakdown in the normal process of appellate review is "rent seeking"[37] on the part of prosecutors. Given the ambiguity and complexity of ECPA, reasonable judges will disagree on its application. Understandably then, prosecutors will tend to gravitate toward a judge who is known to view their requests less critically. The majority of electronic surveillance applications will thus be channeled to judges more inclined to grant them. The inevitable result of such electronic surveillance rent-seeking will be diminished privacy protection for the public as a whole. It may well be that a fully-informed public would not object to this trade-off in personal privacy for the sake of more efficient law enforcement. The problem is that, due to ECPA's regime of secrecy, the public is not fully informed, and can be only dimly aware of the depth and breadth of electronic surveillance carried out under current law.

***Possible Reforms.*** There are a number of ways to reduce secrecy and enhance transparency. Here are some that come to mind:

- elimination of automatic sealing for pen register orders;[38]
- use of less restrictive techniques such as redaction of target names, phone numbers, and other identifying information;
- clear standards and duration limits for sealing and non-disclosure orders;
- clear standards and limits on the number of renewal orders;
- post-acquisition notice of tracking orders to cell phone users;[39]
- more detailed, complete, and public reporting of electronic surveillance

---

a magistrate judge unsealed *ex parte* orders granting government access to plaintiff's e-mails under the SCA. A panel of the Sixth Circuit initially held unconstitutional parts of the SCA which permitted access to e-mail without prior notice or a probable cause warrant. 490 F.3d 455, 461 (6th Cir. 2007). The panel's decision was vacated and the case dismissed by the en banc court for lack of ripeness. Twenty-four years after ECPA, and one of its core provisions is not yet ripe for appellate review.

37 I hesitate to use the term "judge shopping," because I do not wish to imply that the AUSAs and law enforcement officers with whom I work are anything less than ethical and dedicated professionals. I would do the same in their shoes.

38 Some judges question the need for any judicial role in the issuance of pen/trap orders. Under ECPA the judge's role is a purely ministerial one of attesting to the prosecutor's certification that the requested order is relevant to an ongoing criminal investigation.

39 *See* FED. R. CRIM. P. 41(f)(2)( C).

orders by DOJ.[40]

Other commentators have suggested extending the Wiretap Act's exclusionary rule to all types of electronic surveillance orders under ECPA, as well as enhancing civil remedies and penalties for ECPA violations.[41] These ideas are also worth considering.

Whatever the details, the guiding principles for ECPA reform should be brighter lines and more light. Simplicity may not be entirely achievable in a statute dealing with complicated technology. Likewise, transparency is not practicable for every phase of a criminal investigation. But complexity and secrecy take hidden tolls in the form of diminished privacy protection, unchecked judicial power, and public confidence in the judicial system.[42] The 21st century version of ECPA must recognize these dangers, and take necessary measures to avoid them.

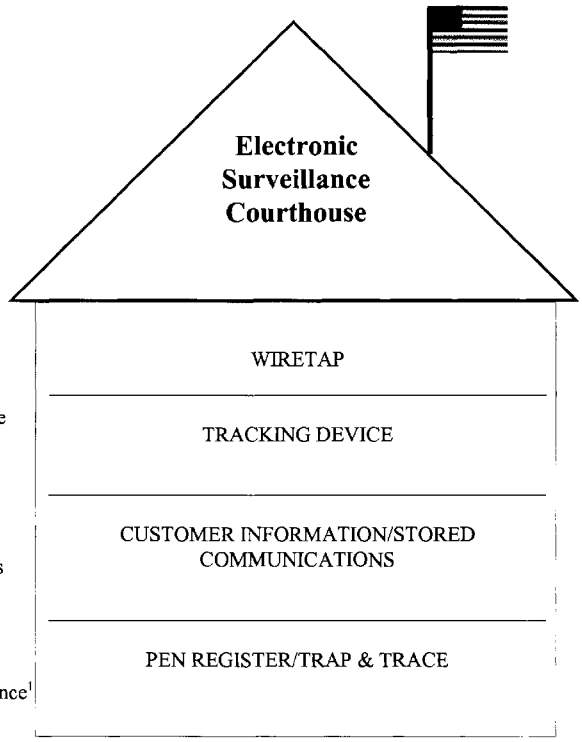
---

40 *See* K. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance,* 41 U.S.F. L. Rev. 589, 633-34 (2007).

41 *See* O. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would change Computer Crime Law,* 54 Hastings L.J. 805 (2003); S. Freiwald, *Online surveillance: Remembering the Lessons of the Wiretap Act,* 56 Ala. L. Rev. 9 (2004).

42 *See Richmond Newspapers Inc. v. Virginia*, 448 U.S. 555, 571-72 (1980) ("[E]specially in the administration of criminal justice, the means used to achieve justice must have the support derived from public acceptance of both the process and its results. . . . People in an open society do not demand infallibility from their institutions, but it is difficult for them to accept what they are prohibited from observing.").

## EXHIBIT A




| Floor | Access Key: |
|---|---|
| 4 | Super-Warrant |
| 3 | Rule 41 Probable Cause |
| 2 | Specific and Articulable Facts |
| 1 | Certified Relevance[1] |

[1] Not Pictured: Administrative Subpoena
Grand Jury/Trial Subpoena
Consent
Written Request Relating to Telemarketing Fraud

# EXHIBIT B

**Summary of Reported Cell Site Decisions**
**(as of June 1, 2010)**

## I. Prospective Cell Site Information (CSI)

### A. Applications Denied Without Probable Cause

#### 1. Unlimited CSI (multi-tower, triangulation, GPS)

- *CSI Houston I*, 396 F. Supp. 2d 747 (S.D. Tex. Oct. 14, 2005) (Smith)
- *CSI Washington I*, 2005 WL 3658531 (D.D.C. Oct. 26, 2005) (Robinson)
- *CSI Baltimore I*, 402 F. Supp. 2d 597 (D. Md. Nov. 29, 2005) (Bredar)
- *CSI Washington II*, 407 F. Supp. 2d 132 (D.D.C. Dec. 16, 2005) (Facciola)
- *CSI Washington III*, 407 F. Supp. 2d 134 (D.D.C. Jan. 6, 2006) (Facciola)
- *CSI Fort Wayne*, 2006 WL 1876847 (N.D. Ind. July 5, 2006) (Lee, D.J.)
- *CSI Milwaukee II*, 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006) (Adelman, D.J.)
- *CSI Corpus Christi*, 2007 WL 3342243 (S.D. Tex. Nov. 7, 2007) (Owsley)
- *CSI Pittsburgh*, 534 F. Supp. 2d 585 (W.D. Pa. Feb. 19, 2008) (Lenihan), *aff'd* 2008 WL 4191511 (W.D. Pa. Sep. 10, 2008) (McVerry, D.J.)

#### 2. Limited CSI (single tower, call -related)

- *CSI New York I*, 396 F. Supp. 2d 294 (E.D.N.Y. Oct. 24, 2005) (granting reconsideration of but adhering to result reported at 384 F. Supp. 2d 562 (E.D.N.Y. Aug. 25, 2005) (Orenstein)
- *CSI Milwaukee I*, 412 F. Supp. 2d 947 (E.D. Wis. Jan. 17, 2006) (Callahan)
- *CSI New York III*, 415 F. Supp. 2d 211 (W.D.N.Y. Feb. 15, 2006)(Feldman)
- *CSI Baltimore II*, 416 F. Supp. 2d 390 (D. Md. Feb. 27, 2006) (Bredar)
- *CSI New York IV*, 2006 WL 468300 (S.D.N.Y. Feb. 28, 2006) (Peck)
- *CSI Houston III*, 441 F. Supp. 2d 816 (S.D. Tex. July 19, 2006 (Smith)
- *CSI Baltimore III*, 439 F. Supp. 2d 456 (D. Md. July 24, 2006) (Bredar)
- *CSI Puerto Rico*, 497 F. Supp. 2d 301 (D.P.R. July 18, 2007) (McGiverin, D.J.)
- *CSI New York VII*, 2009 WL 159187 (S.D.N.Y. Jan. 13, 2009) (McMahon, D.J)

### B. Applications Granted With Less Than Probable Cause

#### 1. Unlimited CSI (multi-tower, triangulation, GPS)

No reported opinions.

**2. Limited CSI (single tower, call-related)**

- *CSI New York II*, 405 F. Supp. 2d 435 (S.D.N.Y. Dec. 20, 2005) (Gorenstein)
- *CSI Shreveport*, 411 F. Supp. 2d 678 (W.D. La. Jan. 26, 2006) (Hornsby)
- *CSI Charleston*, 415 F. Supp. 2d 663 (S.D.W. Va. Feb. 17, 2006) (Stanley) (granting the application to locate a non-subscriber, while rejecting the hybrid theory to locate subscribers)
- *CSI Houston II, 433* F. Supp. 2d 804 (S.D. Tex. Apr. 11, 2006) (Rosenthal, D.J.)
- *CSI New York V,* 460 F. Supp. 2d 448 (S.D.N.Y. Oct. 23, 2006) (Kaplan, D.J.)
- *CSI Sacramento* 2007 WL 397129 (E.D. Ca. Feb. 1, 2007) (Hollows)
- *CSI Houston IV*, 622 F. Supp. 2d 411 (S.D. Tex. Oct. 17, 2007) (Rosenthal, D.J.)
- *CSI New York VI*, 632 F. Supp. 2d 202 (E.D.N.Y. Nov. 26, 2008) (Garaufis, D.J.)

**II. Historical Cell Site Information**

**A. Applications Denied Without Probable Cause**

- *CSI Fort Wayne,* 2006 WL 1876847 (N.D. Ind. July 5, 2006) (Lee, D.J.)
- *CSI Pittsburgh,* 534 F.Supp.2d 585 (W.D. Pa. Feb. 19, 2008) (Lenihan), aff'd 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008) (McVerry, D.J. ). This case is currently on appeal to the Third Circuit.

**B. Applications Granted With Less Than Probable Cause***

- *CSI Boston*, 509 F. Supp. 2d 76 (D. Mass Sept. 17, 2007) (Stearns, D.J.) (reversing 509 F. Supp. 2d 64 (D. Mass. July 27, 2007) (Alexander, M.J.))
- *United States v. Suarez-Blanca*, 2008 WL 4200156 (N.D. Ga. April 21, 2008) (Baverman)
- *United States v. Benford,* 2010 WL 12666507 (N.D. Ind. March 26, 2010) (Moody, D.J.)

*Note: Other decisions have granted such requests without extended discussion.



---

Mr. NADLER. I thank you.

I thank all the witnesses. And we will start the questioning by recognizing myself for a while.

Professor Blaze, with regard to newer technologies that measure time and angle of arrival, you state that according to the policy of the carrier, a customer's location information might be routinely received by that carrier or not, even at times other than when calls

are made or received. What factors might it or does the carrier consider in electing whether to store such data or not?

Mr. BLAZE. Well, the important thing to understand is that, first of all, this technology is not yet fully deployed in every cell site, but carriers are embracing time of arrival and angle of arrival calculations not just to comply with E-911 mandates for providing location during emergency calls, but because it provides them with extremely important information for managing their network.

In particular, it tells them where their customers are located to resolution of typically about 50 meters. And it tells them where they move about, where——

Mr. NADLER. Why would they want to know within 50 meters where their customers are?

Mr. BLAZE. Well, it tells them where new infrastructure is needed, where old infrastructure is redundant, whether the expensive real estate for a tower is paying for itself properly or whether they can afford to move it to another location, whether microcells are required, and so on.

So it is very strongly in the interest of wireless carriers to collect this data as often as possible and as pervasively as possible, to store it effectively forever, and to analyze that data intensely just for the operation of its own business.

Mr. NADLER. Thank you.

Mr. Amarosa, I was struck by one thing you said. You said therefore the distance between two points—radio waves propagate at a constant velocity, obviously. Therefore, the distance between two points can be determined by measuring the time it takes the radio wave to travel between the two points and multiplying by the velocity of propagation of the radio waves to derive the distance.

That assumes you know what time it left. You know what time he received it. In order to know the distance, which is to say the time of propagation, you have to know the time it left the transmitter. How do you know that?

Mr. AMAROSA. Based on putting receivers on the cell sites, you take the differences in time that it hits all the different cell sites.

Mr. NADLER. Difference of time, so triangulate it by——

Mr. AMAROSA. Exactly. Exactly.

Mr. NADLER. You know the distance from here and the distance from here, and you can——

Mr. AMAROSA. Right.

Mr. NADLER. Okay. Thank you.

Now, also you state the TruePosition location technology used by GSM carriers can identify mobile phone devices typically within 50 meters. Fifty meters is how many feet?

Mr. AMAROSA. It is roughly about three feet a meter, so you are talking about 150 feet.

Mr. NADLER. So it is 150 feet. Is TruePosition able to provide this high degree of accuracy after the fact or only when requested prospectively by E-911 operators and law enforcement?

Mr. AMAROSA. The way the system works right now, you establish triggers in the system to locate. You don't locate every call. So the network couldn't handle the location of every call. Right now, the only way you do that is based upon the fact of either being

prior written consent or on any 911 situation where the call would come in.

And prior——

Mr. NADLER. Wait a minute. I thought from your testimony and Professor Blaze's that it automatically recorded every call, because that is how you get all this system information. In other words they automatically record not the call——

Mr. AMAROSA. They are not locating every call. The way the system works today is they are only locating those calls that have certain triggers. The triggers are the E-911 calls that are coming in. And that is the way we are providing location back to the carrier.

Mr. NADLER. But I thought in order to—well, let me ask Professor Blaze.

This seems to contradict what you were saying a moment ago about you need to know the location of all the calls to figure out how many cells you need, where, and so forth. Do you want to——

Mr. BLAZE. So the cellular carrier always records the cell sector location for every call and any kind of——

Mr. NADLER. Sector for every call, the specific location only where——

Mr. BLAZE. Specific location only when specifically requested. My understanding is that cell carriers do that, as Mr. Amarosa points out, on E-911 triggered calls and on phones under surveillance and also periodically on random phones to figure out what is going on.

Mr. NADLER. Okay. So——

Mr. BLAZE. As the technology becomes cheaper and more widespread, they can do it more and more often.

Mr. NADLER. So in other words—the question I was going to ask Mr. Amarosa next is can TruePosition technology be used by carriers to gather and potentially retain this high accuracy location information of all subscribers at all times? Or is this high accuracy information only collected and retained after an appropriate and valid legal request by authorities?

You answered the latter, and you also said it would be cost prohibitive to do the former. But Professor Blaze is saying that that cost prohibition will erode, and it is predictable sometime in the future that you may be able to and may in fact become standard to get this very sensitive location for all calls.

Mr. AMAROSA. I don't know if it will become standard. I think the capabilities will eventually exist, but whether it becomes standard——

Mr. NADLER. The capabilities will exist. It will get cheaper, and it may or may not become standard.

Mr. AMAROSA. Right.

Mr. NADLER. And thank you. So I mean, we have to worry about that as a possibility.

Now, can TruePosition's U-TDOA systems work in virtually any environment?

Mr. AMAROSA. Yes, they can.

Mr. NADLER. Because the radio waves will penetrate anything?

Mr. AMAROSA. The way the system will work, you have in-building capabilities that certain other technologies do not have. You have the ability, if you can make a call and if you look at your phone now, you will see that you have the ability to make a call

inside. We can locate that airway. It is not blocked by the diffraction of concrete walls——

Mr. NADLER. And that is because it is a stronger signal than it used to be, or what?

Mr. AMAROSA. It is because it is using radio waves, and that is not going back to the satellite. It is going to the transceiver where the transmitter is picking up and making that call to the——

Mr. NADLER. It is going to the cellular tower, you mean.

Mr. AMAROSA. Right. Exactly.

Mr. NADLER. And the radio wave that goes to the cellular tower is more powerful or more penetrating than the one that went to the satellite?

Mr. AMAROSA. Because of the fact that the GPS chip is where you are locating from, rather than from a radio wave.

Mr. NADLER. I am sorry.

Mr. AMAROSA. The GPS system is located based upon the chip in the phone, which is communicating with the satellite——

Mr. NADLER. Right.

Mr. AMAROSA [continuing]. As opposed to the radio wave, which is communicating with the base station receiver. And the radio waves can penetrate through buildings and concrete walls and steel structures.

Mr. NADLER. Yes, but the radio wave going to the chip, to the satellite, also has to penetrate that wall.

Mr. AMAROSA. And it doesn't. And it doesn't reach the satellite, because of the way the satellite systems work. You have to have an open sky capability and the ability to see the satellites——

Mr. NADLER. Okay. Because it is at a different angle, because it is going up as opposed to——

Mr. AMAROSA. Right. Exactly. You take, for instance, if you tried to use the GPS capability in the Wall Street area in New York City. Even though you just can't get through because of the narrowness of the streets.

Mr. NADLER. Thank you.

Mr. Zwillinger, we have heard much today about revolutionary location based technologies that give extremely precise information about where an individual or individuals may be at any given time.

Can any meaningful legal distinctions be drawn that should inform our review of the ECPA statute and its application to location based information? To your knowledge does DOJ draw distinctions with regard to location information derived from different location based technologies? Is that a sensible way to make a distinction based on what technology is used?

Mr. ZWILLINGER. Well, unfortunately, it has been the only one so far. Let me go through three possible ways to draw a distinction. You know, one way to draw a distinction is between historical and prospective data. And for reasons we talked about, that is not a rational distinction. It is the same invasiveness 5 minutes ago versus 5 minutes from now.

The second one is where the Fourth Amendment points, which is——

Mr. NADLER. Well, wait. Let me just challenge you on that. Where you are located right now might be important for an emergency use. You need a paramedic quickly, or, you know, you use

E-911, et cetera. Where you were may be important for evidentiary reasons, which is very different from an emergency response. So maybe you should make a rational distinction.

Mr. ZWILLINGER. Well, I think emergency is the distinction there, though. I mean, no ECPA reform would really do much to the emergency disclosure provisions that would allow you to make disclosures for an emergency. And E-911 is based on a consent theory that when you dial 911, you are consenting for disclosure. So I don't think making a distinction on that basis would cause a real-time prospective distinction. We need an emergency exception. We need the 911 capability. But I don't think that should drive the framework of ECPA.

So the second distinction is reasonably precise versus general location data. And this is a distinction, I think, DOJ does draw to some extent now, because my understanding is—and obviously, I am not there—that their guidance is if they are going to try to track GPS data, they suggest that districts use a Rule 41 warrant, although there are some notable cases where that isn't being followed.

But their theory, I believe, is that it is constitutionally based, that a GPS can give you information about being inside a structure, and cell site data isn't as precise. I think that is a very dangerous distinction. We have been hearing that today that this technology is evolving to be more precise, that the GPS technology is (a) being used for different applications and that providers may track more precise data. So I am not sure that is the way for ECPA——

Mr. NADLER. Well, we had that with the Supreme Court in the 1920's and 1930's, actually. And I think it was Justice Holmes who said the distinction of whether the bug is on the outside of the wall or the inside of the wall didn't make a heck of a lot of difference and that in fact he speculated—I think in 1928, he said someday it may be possible from across the street or a mile away to tell what is being said inside a room, and we should protect that privacy.

So do you think the distinction might be better whether you are inside a room or a place where we will at least impute to you a reasonable expectation of privacy than what you are saying, or where in your house you are is more private—is a greater expectation of privacy than whether you are in your house or in the car or at the University?

Mr. ZWILLINGER. Well, to some extent the Fourth Amendment does turn on that, which is one of the reasons I think Congress really needs to act here, because those aren't the distinctions that are meaningful to us in society. I mean, if I am continuously tracked everywhere I go all day, the fact that sometimes I am outside and sometimes I am inside doesn't give me comfort that it was okay to track me during those moments I was outside.

So, you know, to me when we are thinking about ECPA reform, we are thinking about where we want to raise the standard. It is not were you in the house at that moment? It is are we learning something about your continuous movement versus learning something about you at a given moment in time, like you bought a book at Barnes & Noble this morning.

Mr. NADLER. And which should have greater privacy consideration—your continuous movement or an information moment in time and why?

Mr. ZWILLINGER. I think continuous movement, because it is more invasive, and it is more intrusive to be tracked at every moment of the day all day than, as Mr. Littlehale pointed out, they get a credit card receipt, they know you were at a gas station. This has been the way it has been for a long time. It is an existing record. Nothing is being turned on. The providers aren't being enlisted to become government agents.

Mr. NADLER. So in other words, you make a phone call or receive a phone call, and you at that point have less expectation of privacy than just the fact that it is in your pocket as you move around.

Mr. ZWILLINGER. That is one way to look at it, yes.

Mr. NADLER. Okay. And you said the third basis.

Mr. ZWILLINGER. Well, I think I covered the status location versus continuous flow was the third basis I was thinking of.

Mr. NADLER. I am sorry?

Mr. ZWILLINGER. I said the static location versus continuous tracking is the third basis and one that I would ask the, you know, the Committee to think about.

Mr. NADLER. Okay. I have one more question for Judge Smith.

And you explained in your testimony that with regard to those magistrate and district courts that are granting access to prospective cell site data under 18 USC 2703(d), specific and articulable fact standard, they are only doing so for a limited cell site information.

Can you explain the distinction between limited cell site information and full range or unlimited location data in greater detail?

Judge SMITH. As I understand it, the difference between limited cell site information and what I call full cell site information is the difference between a single tower signaling, reflecting the beginning and end of a call, as opposed to all the signaling information that that may be derived from signals bouncing off of multiple towers in a given location.

In that circumstance that allows for the triangulation, more detailed, precise location pinpointing of the individual. And to date, as you correctly point out, I am not aware of any published decision by any of the magistrate judges, although we do disagree on the approach to the statute. I am not aware of any published decision in which a magistrate judge has allowed unlimited cell site information, GPS triangulation, on anything less than probable cause.

Now, that doesn't mean—and I have been advised in some applications that just because there aren't any published decisions doesn't mean we are not getting it. So I am not exactly sure where all my colleagues stand on this, because not everyone has taken the time to publish a written decision.

Mr. NADLER. Thank you.

I now recognize the gentleman from Georgia.

Mr. JOHNSON. Thank you, Mr. Chairman.

I want the witnesses to respond to this scenario. Bill is a law enforcement officer. Jane is his wife. Bill suspects that Jane is having an affair. Bill issues a subpoena or a—not issues, but he tenders a subpoena to a cell phone provider or a global positioning system

provider and requests information on the location right now of Jane.

Can that law enforcement officer be successful at acquiring that data, you know, where she is in real time right now? And what is the difference between him requesting that information versus the historical data—where has she been over the last 2 weeks or so? Can that happen? First of all, can you get that information, a law enforcement officer, without showing any kind of probable cause or reasonable suspicion, but just simply a subpoena, ongoing investigation?

If I could get a response to that, Mr. Amarosa? Mr. Littlehale? Mr. Zwillinger and Judge Smith? And I assume that we certainly have already heard from Professor Blaze about the fact that we compile that data, so if you would respond.

Mr. AMAROSA. Well, let me go first. We don't track individuals unless the trigger goes into effect, which is the 911 call. So we are not tracking—I forget her name—Mrs. Law Enforcement.

Mr. JOHNSON. Jane.

Mr. AMAROSA. Jane. We are not tracking her at this point in time. We don't maintain databases on calls that come into the system. If there was a call that comes into the system that is a non-911 call, we are not creating a location for it, so we wouldn't have it. We don't respond unless there is a lawful request, and it is——

Mr. JOHNSON. What is a lawful request?

Mr. AMAROSA. Well, what we are responding to is court orders.

Mr. JOHNSON. A court order.

Mr. AMAROSA. And the subpoena of the data——

Mr. JOHNSON. A blank subpoena or a subpoena issued by the court—blank.

Mr. AMAROSA. Well, I am not sure that this law enforcement officer has the authority to issue a subpoena.

Mr. JOHNSON. Okay. All right.

Mr. Littlehale?

Mr. LITTLEHALE. From my standpoint there are two issues. Obviously, what this individual has done is certainly a violation of that agency's policies, very likely a crime as well. I am not sure that the level of process required, if you assume a jealous officer who is willing to forswear his badge in order to track his wife, is going to make a difference, because he could just as easily swear out a false search warrant as he could—well, I say just as easily.

It certainly would take him slightly more time to fake a search warrant and go to a judge and get it signed. But he could just as easily do that as he could if he had the power to issue an administrative subpoena.

So the question is what safeguards does that particular department have in place? I can't speak for every department, but I can say from my department that would be difficult to do.

Mr. JOHNSON. Well, can it be done? Theoretically, it can be done, can't it?

Mr. LITTLEHALE. Theoretically, it could, yes.

Mr. JOHNSON. Okay. And you could get access to the cell phone record real-time where the person is located right now based on a subpoena.

Mr. LITTLEHALE. If that officer had a pretty good degree of sophistication in their use of electronic surveillance techniques and was willing to fake whatever process they needed to do and they were able to sneak around in their agency and use the right fax machines and that sort of thing, conceivably, yes. I would say it would be very difficult to do in my agency.

Mr. JOHNSON. All right. Okay.

Mr. ZWILLINGER. When you first started the question, I thought it was going to be a civil subpoena and the answer was going to be easy, because you can't get any prospective for the civil subpoena. But clearly, it is not. This is a law enforcement process.

I don't think subpoena would get this piece of data. A subpoena might get a call record, but if this is historical, it should be produced with a 2703(d) order, which is the specific and articulable facts standard order. And if this is future, then that is a question we have been debating today.

The government would try to get it with a hybrid pen register and 2703(d) order, and the esteemed judge to my left would decline it, and then they would have to come back with a warrant. But that is the open question. They would probably find a magistrate who would allow it. It shouldn't be a subpoena for prospective real-time cell location data, even under the current analysis of ECPA. It should be at a minimum a (d) order for historical data.

Judge SMITH. I agree with Mr. Zwillinger. I would hope that Bill in your hypothetical would not be able to get the information simply through a subpoena. It is possible that he may.

I think it would probably depend on whether or not the provider would feel like that is a sufficiently legitimate order. Most providers, at least as far as I know, have counsel that advise them on what they need to see. And typically, a simple subpoena as opposed to a court order directing the provision of this information under 2703(d) or Rule 41 would be required, so——

Mr. JOHNSON. Yes, even under FISA we had some situations where law enforcement officers were able to obtain data, promising that a subpoena would be submitted later.

Judge SMITH. This goes back—excuse me—this goes back a little bit to my point about no appellate oversight. Even if a judge issued this type of order without any sort of process or without any sort of probable cause or the lesser standard of specific and articulable facts, he may—he or she may be able to do it without any repercussions, because there is no appeal, basically.

Mr. JOHNSON. Yes, according to the Department of Justice, its policy is that Federal agents should seek a warrant based on probable cause before retrieving real-time GPS tracking information. However, Freedom of Information Act requests by the ACLU have uncovered at least two jurisdictions, Florida and New Jersey, that seek this information under a lesser standard.

Does DOJ policy bind the Federal agents or U.S. attorneys? And is it possible that this policy is being ignored in other jurisdictions, Judge Smith?

Judge SMITH. Well, I don't know exactly what DOJ's policy is. I will say that recently the majority of GPS precise tracking information requests that I have seen, they have gone under the Rule 41

standard. However, that has not been uniform. I have seen exceptions to that.

Mr. ZWILLINGER. Can I comment briefly on that? As someone who represents providers, I frequently get requests from and subpoenas and other legal process from U.S. attorneys' offices around the country, and I am the one typically telling them that, you know, that what you have done is in violation of DOJ policy. And sometimes I hear back, "Oh, do you mean those folks in Washington?" To which I say, "Yes, and you should call them." And they say, "Well, our boss is a U.S. attorney, and he has been confirmed by the Senate, and we will do things the way we do things."

So to rely on DOJ policy to prevent prosecutors from doing things that we would think that the law would prevent them from doing is somewhat dangerous, and it puts a lot of burden on ISPs and providers to make sure that government isn't doing what it shouldn't be doing.

Mr. NADLER. Thank you.

The gentleman's time has expired.

The gentlelady from California is recognized.

Ms. CHU. Yes, I would like to ask Mr. Zwillinger or Judge Smith, Newsweek reported that location tracking has caused serious harm, and they cited a case where an agitated Alabama sheriff called the phone company's employees, demanding that they release the real-time data on his daughter's whereabouts. He claimed that she had been kidnapped and that the cell phone company pinged her cell phone every few minutes to identify her location, but in reality there was no kidnapping. The daughter had been out on the town all night, and the father wanted to know where she was.

There was also a more sinister request that came from some Michigan police officers, who purportedly were concerned about a possible riot and then pressed another telecom company for information on all the cell phones that were congregating in an area where a labor union protest was expected.

So what ability do you have to challenge the use of prospective cell phone information, as in the case of the Alabama sheriff's daughter? What rights do you have to challenge a warrant for a regular tracking device, if you deem it illegal or improper?

Judge SMITH. Well, if you are charged with a crime and they attempt to introduce evidence obtained in that manner, a motion to suppress can be filed. And if the evidence was obtained in violation of the Constitution, a violation of the Fourth Amendment, there is a suppression remedy.

The difficulty is that not everyone charged with a crime is deemed subject to these orders. If you happen to call or are being called, have been called by the target phone, then you may be swept up in a criminal investigation, even though you are a pizza delivery guy or someone who has no contact, no contact with the criminal conspiracy.

And so as I said, that is the problem. Law-abiding citizens' privacy rights might be impacted. They will not know about it because of the gag orders imposed on the providers and because of the sealing orders that courts impose prohibiting this information from being released to the public.

Mr. ZWILLINGER. To add to that, the examples you have given are examples where the police officer or law enforcement officer claimed an emergency. And with regard to the disclosure of historical records, the discretion to disclose information based on emergency is with the provider. So providers that I represent might have forms that the agent will have to fill out to certify it is an emergency or to explain what the emergency is and why they should exercise this discretion.

For forward-looking data like a pen register or wiretap, there was no discretion with the provider. If the right official comes and says this is an emergency, the provider must provide the data for 48 hours until the order is given, and then must shut it off.

So there is not very much you can do in the situation where the right official claims an emergency and asks for forward-looking process except to not provide location data in response to a pen. But again, you are talking about an abuse of the emergency provisions, and there is very little that can be done.

Ms. CHU. So you are saying that with both the sheriff and with these Michigan police officers, they have to comply.

Mr. ZWILLINGER. They have to comply with a pen register request for forward-looking data for 48 hours. I have to admit I am not sure exactly what the request was made in the Michigan situation.

Ms. CHU. Well, it was for a labor union protest that was to be expected, so it was forward-looking.

Mr. ZWILLINGER. Yes. Yes. If the emergency provisions were properly invoked, then they would have to comply.

Ms. CHU. Okay. I would like to follow up on the DOJ policy. According to the Department of Justice, of course, it says that Federal agents have to seek a warrant based on probable cause before retrieving real-time GPS tracking information. However, Freedom of Information requests by the ACLU have uncovered at least two jurisdictions, Florida and New Jersey, that seek this information under lesser standards.

This clearly seems to indicate a depth of confusion about how to handle real-time data for cell phones. And why is there such a difference between the official policy and what is going on in the ground? And does the DOJ policy bind Federal agents or U.S. attorneys to get warrants in any way?

Judge SMITH. Congresswoman Chu, again, I am not an expert on DOJ policy. I would presume that that would provide substantial guidance to the U.S. attorneys' offices. But again, a lot of the requests are initiated by various law enforcement agencies—the DEA, the FBI. We get requests from Postal Service postal inspectors occasionally for this type of information.

So all I can tell you is it does not seem to me that the policy has been uniformly applied. Whether that is some kind of breach or not, I will not say.

And by the way, I do want to say that although we have discussed here some—some examples of apparently abusive conduct on behalf of law enforcement, in my experience, the people that I deal with, the agents that come before me and the A-USA attorneys that appear before me are dedicated, ethical professionals. I

think they are just as troubled by the confusion in this area as the judiciary is.

Mr. ZWILLINGER. I would just supplement that by saying that the fact that it is DOJ policy, there is not a statutory provision to point to to say that this is required. This is what we are discussing today about to what extent ECPA should cover this. So the guidance is coming from an anticipation of what the constitutional ramifications will be for not getting the warrant. And it seems that some people are making different decisions about that.

Ms. CHU. Thank you.

I yield back.

Mr. NADLER. I thank the gentlelady.

And that will conclude our questions this morning just in time for a vote.

The gentleman from Georgia?

Mr. JOHNSON. Thank you.

I do want to explain the fact that I have abundant respect and admiration for the law enforcement community. And, however, for the purposes of creating a picture of what can happen with someone—with a law enforcement officer in bad faith seeking this information helps us to understand the dilemma of good law enforcement officers seeking the same information.

So we don't want the worst-case scenario to be prevalent and possible as we move forward into the future. And so I only raised that example of police misconduct to help enlighten us as to what the stakes are for failing to act with this very important issue.

And I want to thank the Chairman for holding this hearing. And I look forward to working with you, Mr. Chairman, as we peer into the future of technology and what we can do to ensure that the basic Fourth Amendment right to privacy, which is implied in that amendment, that it be upheld. Thank you.

Mr. NADLER. Thank you.

And that is the bells ringing for votes on the House floor.

Without objection, all Members will have 5 legislative days to submit to the Chair additional written questions for the witnesses, which we will forward and ask the witnesses to respond as quickly as they can so that their answers may be made part of the record. Without objection, all Members will have 5 legislative days to submit any additional materials for inclusion in the record.

With that, I want to thank our panel of expert witnesses for their service.

I want to thank the Members.

And this hearing is adjourned.

[Whereupon, at 11:48 a.m., the Subcommittee was adjourned.]

# APPENDIX

---

MATERIAL SUBMITTED FOR THE HEARING RECORD

## *Congressman Henry C. "Hank" Johnson, Jr.*

## Statement for the Hearing on Electronic Communications Privacy Act (ECPA) Reform and the Revolution in Location Based Technologies and Services

## June 24, 2010

Thank you, Mr. Chairman, for holding this important hearing and giving Members the opportunity to examine the Electronic Communications Privacy Act with respect to location-based technologies such as cell phones and smart phones.

The Electronic Communications Privacy Act ("ECPA") provides the standards for law enforcement access to the electronic and wireless technology we use.

Specifically, this hearing will give Members the opportunity to hear from witnesses about reform under the Act and issues relating to historical and real time location data.

This hearing is timely as mobile communication devices have evolved from being little more than a convenience for the wealthy, to a basic necessity for most Americans.

Cell phones have transformed the way we communicate and work with each other on a daily basis. In today's society, it is more common for one to have a cell phone rather than a traditional landline phone.

According to a 2009 Wireless Association report, there were approximately 277 million cell phone service subscribers in the United States last year -- that is about ninety percent of the overall population.

Whenever these subscribers have their cell phones on, the phones can automatically scan for cell towers and register location information with the network.

This has lead to substantial privacy concerns as cell phone data may be collected without a person's knowledge.

Further, some data provides the ability to track all of a person's movements on a relatively precise and continuous basis. When it comes to law enforcement and national security, the value of a person's location at a particular moment in time cannot be overstated.

Criminal investigators can use this information to find a child that has been kidnapped or to apprehend a dangerous criminal.

While the benefits of technology to aid law enforcement are great, it is important to remember that Americans have privacy rights. The founding fathers recognized that that citizens need privacy for their "persons, houses, papers, and effects."

While technology has been advancing at the speed of light that basic principle the framers had in mind, when they drafted the Constitution, has not changed. Therefore, it is important to have a balance between user privacy expectations and law enforcement needs.

The ability to monitor communications has grown enormously. As technology continues to expand, Congress should adjust laws accordingly to keep up with modern technology.

It has come to Congress' attention that the standards governing law enforcement access to historical and real time cell site data regarding location information may be the most confusing area of the Act's application to wireless technology.

With more than 500 federal magistrate judges serving in district courts around the country, there is no room for confusion when it comes to the Electronic
Communications Privacy Act.

If courts are issuing conflicting decisions with differing standards, regarding law enforcement access to this wireless location data under the Act, Congress should step in and act accordingly.

I am anxious to hear from the witnesses today as I have a number of questions. Should Congress step in and reform the Electronic Communications Privacy Act?

If so, how should the Act be reformed to strike the proper balance between consumer privacy and law enforcement?

What should law enforcement officers have to provide cell phone providers in order to obtain access to historical and real time data?

Would it be premature for Congress to legislate if there are unresolved Fourth Amendment issues?

I hope our witnesses can shed light on these questions.

I look forward to hearing from the witnesses today, and yield back the balance of my time.

Questions for the Record
House Constitution Subcommittee Hearing
"Electronic Communications Privacy Act Reform and the Revolution in Location-Based Technologies and Services"
June 24, 2010

**Answers to Additional Questions for United States Magistrate Stephen Wm. Smith from Congressman F. James Sensenbrenner, Jr.:**

1. Are there any specific examples of "Cell-Site" information being abused by law enforcement?

**ANSWER:** The press has occasionally reported anecdotal instances of law enforcement abuse of cell-site information, such as those mentioned by other Members at the June 24 hearing. In addition, a 2007 report from the Department of Justice inspector general found hundreds of violations by the FBI in their use of "national security letters" to collect telephone and other records of U.S. citizens under another provision of ECPA. I have no personal knowledge of such abuses, nor can I say with confidence that serious abuses have not occurred. The existing regime of secrecy covering electronic surveillance orders makes it impossible to know. The temptation to abuse secret governmental power is always present and, if history is any guide, often proves irresistible. That is why, in my opinion, any ECPA reform is useless without transparency.

2. In your 2005 opinion, you found that a cell phone functions as a tracking device under 18 U.S.C. 3117. If a cell phone is, in fact, a tracking device for purposes of ECPA, then wouldn't text messages and emails sent from a cell phone be fair game for interception by anyone under 18 U.S.C. 2510(12)(C), which excludes communications from a tracking device from the definition of "electronic communication"? ("electronic communications" are subject to "super-warrant" requirements under ECPA).

**ANSWER:** No, not at all. ECPA's graduated legal standards are keyed to the type of information sought, rather than to the device used. As explained in my 2005 opinion, a single multi-functional device (like a cell phone) may generate different kinds of information accessible under different standards. *See In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority,* 396 F.Supp.2d 747, 756 (S.D.Tex. 2005). A cell phone becomes a "tracking device" only when it is used for that purpose, just like a phone book can become a doorstop if used in that way. It would make no sense to authorize a cell phone wiretap under the pen register standard simply because the cell phone can also generate pen register information; nor would it make sense to authorize a pen register only

under the wiretap standard merely because the cell phone can also transmit the human voice. I read the definitional exclusion of 18 U.S.C. 2510(12) simply as the means Congress used to distinguish tracking device information from the other three categories of electronic surveillance regulated by ECPA. (See Ex. A to my written testimony). Nothing in that definition suggests that a device which might yield tracking information must be excluded from ECPA coverage when it generates text messages and e-mail regulated under the other ECPA surveillance categories.

3. At the conclusion of your opinion in 2005, you openly hope that higher courts will render authoritative guidance for the magistrate judges. Do you have more or less guidance from the appellate courts about ECPA then when you wrote your opinion?

**ANSWER:** To date magistrate judges have received no guidance whatever from appellate courts on cell phone tracking under ECPA. While the case pending in the Third Circuit will break the shutout, there are no other cases like it on the horizon, as far as I can see. This state of affairs will likely continue unless ECPA is amended to afford the general public– as well as those affected by electronic surveillance orders — meaningful access, notice, and opportunity to challenge such orders, as is the case with ordinary search warrants.

4. You state that not one reported decision has ever allowed access to unlimited location data on anything less than a probable cause showing and that the consensus for obtaining historical location information is that, as a form account record or customer information in the hands of the phone company, a 2703(d) order is appropriate.

   If clarification as to what standard applies to which technology is needed, does it follow that the standard has to be the same for all types of cell-site information (as is the proposal advanced by the Digital Due Process Coalition)?

**ANSWER:** I believe so, as a practical matter. If clarity is to be achieved, fewer distinctions, not more, are needed. The "consensus" for obtaining historical location information may be more apparent than real. No decision has yet come to grips with how to define "historical" location information — reasonable arguments could range from one millisecond after transmission to 180 days. And Judge Lenihan's decision requiring probable cause for all location information is proving to be persuasive. Last week a magistrate judge sitting in Austin, Texas issued an opinion adopting her position. *In the Matter of Application of the United States,* No. A-10-561 M (W.D. Tex. July 29, 2010) ( Austin, M. J.). Others may well have followed suit, without a published opinion.

5. Explain the distinction you raised in your testimony between historical cell-site location information that is captured at the instigation of law enforcement and that which the service provider generates on its own. Do you think the standard to create this information should be different from that to receive the information that is maintained in the ordinary course of business?

**ANSWER:** An example is precise location data derived from a cell phone's "Enhanced 911" services (commonly referred to as "E-911"). Law enforcement applications seeking such information typically admit that phone companies ordinarily do not create or maintain records reflecting the precise location data derived from such sources, and for that reason they seek an order compelling the service provider to create and maintain such records. I do not believe ECPA currently authorizes such an order. *See In re Application of the United States,* 2007 WL 2086663, at *1 (S.D. Tex. 2007). If the statute were amended to "deputize" the service provider in this fashion, I believe the standard should be at least as stringent as that for other location-based information, i.e. Rule 41 probable cause.

**Answers to Additional Questions for United States Magistrate Stephen Wm. Smith from Congressman Henry C. "Hank" Johnson, Jr.:**

1. Location tracking using cell phone location has been a common practice for more than a decade, yet the first appellate challenge to this practice has only been brought this year. Some judges, including you, have asked the Department of Justice to appeal these decisions. Why do you think that DOJ has not appealed to the circuit courts before now?

**ANSWER:** I can only speculate. Presumably, the DOJ has been content with the status quo, which permits law enforcement to channel electronic surveillance requests to judges with the most accommodating view of the law. An appeal would risk a binding, unfavorable decision which such judges could not ignore.

2. If ECPA reform is passed, would it interfere with service providers in their providing information to law enforcement?

**ANSWER:** No, not if the reforms recommended by the Digital Due Process coalition were enacted.

**Questions for the Record**
**Committee on the Judiciary**
**Subcommittee on the Constitution, Civil Rights and Civil Liberties Hearing**
**"Electronic Communications Privacy Reform and the Revolution in Location-Based Technologies and Services"**

**June 24, 2010**

*Response of*
Richard Littlehale
Assistant Special Agent in Charge
Technical Services Unit
Tennessee Bureau of Investigation

**Questions of Congressman F. James Sensenbrenner, Jr.**

**Questions for Mr. Littlehale**

1. **If the standard for cell-site information were to be probable cause, what would the probable cause be of? That a person associated with a crime is in the area of the tower? That the communications facility was used in furtherance of the crime?**

In the most general terms, the Fourth Amendment requires that two types of probable cause exist together in order for a search warrant to issue: (1) probable cause that a crime has been committed, and (2) probable cause that evidence of that crime (or contraband, or a fugitive) will be found in the location to be searched. There is no requirement that the person or company whose person or premises are searched be, themselves, somehow culpable in the offense. So, if Congress established a probable cause requirement akin to the search warrant requirement for cell-site location information in the possession of a service provider, then the legal analysis would go as follows: the location to be searched (the place where the cell site records are kept) would be the corporate data center of the service provider; a law enforcement officer would first have to establish probable cause that a crime had been committed, and then establish probable cause to believe that some of the cell site records in that data center constituted evidence of that crime.

This description highlights just one of the potential problems with elevating the evidentiary standard to probable cause in all cases. What about the case where an individual with a mobile device is suicidal, or a missing child, or a missing senior with severe dementia? In all of those situations, location information could be critical to a

safe recovery of the individual, but none of them are crimes in most jurisdictions, so a law enforcement officer could not meet the first prong of the test, and a search warrant would be unavailable. Exceptions could be carved out in those cases, but then the goal of simplicity begins to suffer.

Proponents of a uniform probable cause standard are quick to point out that there is a provision in the law allowing a service provider to release location information to law enforcement in the case of an emergency. What they usually don't point out is that in many cases, under current law, the decision of whether or not a particular set of circumstance constitutes an emergency lies in the hands of a civilian employee in the service provider's call center, rather than in the judgment of the law enforcement officer with all the facts of the case and all their experience and training to call upon. Couple that with the demands placed on the often overwhelmed, understaffed call centers at many service providers, and the result could be a refusal to declare an emergency in a case where it is warranted, leaving law enforcement without recourse.

**2. Why should/or why shouldn't the evidentiary standard be raised to one of probable cause? Is this an unnecessary burden on law enforcement?**

I believe that the balance between privacy and safety currently struck by the law in this area is a reasonable one, and that any change to that balance should be broadly discussed and carefully considered, as it will have substantial and far-reaching secondary consequences.

At present, law enforcement generally distinguishes between network *transactional* location records (ordinary records of communications captured, stored and recorded by the service provider in the ordinary course of its business as a necessary incident to providing the services they provide) and *demand*-based location information (manufactured information generated solely based on a law enforcement demand pursuant to lawful emergency or court authorization). Because the latter is not a record that already exists, it is commonly believed to require a higher standard of proof because it is more invasive. As to records that exist in the ordinary course of business and which a person has "voluntarily turned over to a third party" – such as cell site location information – the Supreme Court has repeatedly found no reasonable or constitutionally-valid expectation of privacy.

Cell site location records are routinely generated in the normal course of a cellular provider's business. They indicate nothing more that which piece of the telephone company's equipment (the particular cell tower and sector) that a particular customer's cellular handset was communicating with on a particular call event began or concluded. Those records would be created whether or not law enforcement would later attempt to obtain them or to receive them contemporaneous with their creation; and they would be kept for a certain period of time and then discarded or archived.

Contrast this with a demand-based location request. In that instance, at law enforcement's direction and based on lawful emergency or court authorization, the service provider causes a more precise location record to be generated – one that would not otherwise exist at all. That record would not have been created "but for" the law enforcement demand; as a result, it is reasonable and prudent to suggest that a higher level of proof be met for that information to be turned over.

This framework is reasonable because it is consistent with other ways location information can be obtained and used by law enforcement, and because it is consistent with the view that information voluntarily turned over to a third party enjoys less privacy than those things we keep from the outside world. It is worth considering that a person's location at a particular time can be derived from any number of sources other than mobile devices, sometimes in very precise ways. A bank will have records of a customer's use of a credit or ATM card in their possession that would show exactly when and where that particular card was used. A transportation authority might have records of when a commuter passed by particular tollbooths based on the information provided by their electronic commuter pass. Those records can currently be obtained with a subpoena in most cases – and when they relate to communications records, Congress has already acted to afford them greater protections under ECPA's existing framework. Should that standard change? If not, how can the inconsistency be explained, if the purpose of reform is to bring clarity and consistency to the law?

Simplicity for its own sake is not always a virtue, and complexity is hardly foreign to the Constitution: the same piece of property – a person's suitcase, say – may be governed by completely different legal standards when it is laying on a closet shelf, in the trunk of a car, or passing through a border checkpoint. The current ECPA framework has existed in broad form since 1986; there is always room for improvement, but that does not necessarily recommend altering the fabric of the existing framework in such a fundamental way.

As to the second part of the question, I believe that an across-the-board increase in the standard of proof would, for the reasons above, constitute an unnecessary burden on law enforcement. The desire of private citizens for privacy in their communications is sufficiently protected by the current legal framework. The present balance of judicial supervision and law enforcement efficiency has existed for some time, and should not be abandoned without a demonstrated need for an increase in privacy and a demonstrated pattern of abuse – presently nonexistent – by government officials. Yes, isolated instances of abuses have been cited by the ACLU, but to say that enforcement as a whole should be deprived of efficient use of this valuable tool because of those isolated instances is the functional equivalent of saying that police officers shouldn't be allowed to carry firearms because there have been some instances where officers discharged their weapons when they shouldn't have done so.

One thing is certain, whether or not the standard should be raised in some areas or any at all: law enforcement officials currently utilizing communications records to serve the public have, in their training and experience, an invaluable source of information about the real-world impact of changes to the law. I would respectfully urge the members of the subcommittee to seek testimony from a number currently serving law enforcement professionals about the effects of DigitalDueProcess.org's proposals before adjusting a framework that is of such critical importance to public safety.

**3. Can you give us some examples of how cell-site location information has had a life saving outcome in a law enforcement situation?**

My agency and agencies that we support use location information from mobile devices on a regular basis to catch dangerous fugitives, identify and apprehend online child predators, and identify homicide suspects. The examples that follow are just a few of the cases that would not have been as successful – indeed, that might have resulted in great harm to innocent victims or the public – if law enforcement was not able to efficiently gain access to location information:

*Last year, my unit utilized communications records analysis, including location information, to identify a woman who stabbed a new mother repeatedly and abducted her four-day-old son. These techniques, along with other methods, resulted in the safe recovery of the child within just a few days.*

*My unit utilized location information from cellular phones in concert with other intelligence to identify the location of two subjects who were on the run after murdering a Tennessee State Trooper. Tactical units were called in, and both subjects surrendered and were taken into custody without incident, removing the potential for a dangerous pursuit and bringing two cop killers to justice.*

*Several years ago, a Tennessee woman killed her husband with a shotgun and fled with her three daughters, the youngest of whom was an infant at the time. An AMBER Alert was issued, and my unit utilized location information to dispatch patrol officers to her area. She was apprehended to stand trial, and the children were safely recovered.*

*On at least two occasions within the last year, my unit has used location information to find individuals who are threatening suicide to their families over mobile devices. In both cases, the individuals were found safe and turned over to crisis intervention personnel to get the help that they needed.*

There is no doubt that similar stories can be found throughout the law enforcement community. Simply put, all across this country, there are Americans who would not be alive today without this technique.

**4. These hearings have focused on the gap between law and technology. Is there a gap between certain technologies that will result in what law enforcement refers to as "Going Dark"? What is this and what problems will create for law enforcement? What is being done to address this?**

"Going Dark" is a term used by a coalition of federal, state, and local law enforcement agencies to refer to the steadily increasing rate at which law enforcement is losing access to communications streams that contain evidence of criminal activity. The purpose of the initiative is to identify and gather the fiscal, technological, and organizational resources necessary to reverse this dangerous trend.

To be clear, the "Going Dark" initiative is not an effort to increase the amount of information law enforcement can obtain or to lower the legal standards that we must meet to obtain it. Instead, it is an effort to minimize the rate at which communications relevant to criminal and national security investigations migrate onto technologies that law enforcement agencies simply cannot access, whatever legal process they might possess.

ECPA reform and the "Going Dark" initiative are separate issues, but from the law enforcement perspective, they implicate many of the same basic concerns. Legal barriers such as an increase in ECPA proof standards are not the only ones that keep communications records out of law enforcement hands. In many instances, we are unable to utilize evidence that would be of enormous value in protecting the public because the technologies used to carry and store that information are not accessible to us, no matter what legal process we obtain.

As Congress moves forward with discussions of how it might simplify the legal requirements for obtaining communications records, and whether or not to change the standards law enforcement must meet to get the records it wants, the technology gap has a place in the discussion. I would urge that Congress ensure that whatever level of process it decides is appropriate, that steps are taken to guarantee that law enforcement will be able to access the required communications technologies once that process is obtained.

**Questions for the Record**
**Committee on the Judiciary**
**Subcommittee on the Constitution, Civil Rights and Civil Liberties Hearing**
**"Electronic Communications Privacy Reform and the Revolution in Location-Based Technologies and Services"**

**June 24, 2010**

*Response of*
Richard Littlehale
Assistant Special Agent in Charge
Technical Services Unit
Tennessee Bureau of Investigation

**Questions of Congressman Henry C. "Hank" Johnson, Jr.**

**Questions for Mr. Littlehale**

**1. If ECPA reform is passed, would it interfere with service providers in their providing information to law enforcement?**

In order to address this question in the most complete way possible, I think it is worth taking a moment to distinguish between ECPA reform as a whole, and the need to reform ECPA in the way that DigitalDueProcess.org is advocating in particular. As communications technology evolves, so too must the laws that govern it, and a discussion about update ECPA is entirely appropriate, but we should remember that ECPA can be reformed – that is, any areas in the law that are perceived to lack clarity can be refined – without changing the current balance struck between privacy and safety. There is always room to debate how that balance is struck, but that debate should involve a robust presence by all stakeholders. Those stakeholders must surely include the law enforcement community and the members of the general public who we are sworn to protect, because any substantial change to the current balance of interests may have substantial and far-reaching secondary implications for our effectiveness in their defense.

With that said, and assuming that the question refers to ECPA reform as it has been urged by DigitalDueProcess.org, then yes, it will interfere with law enforcement's use of communications records in support of both critical and routine investigations. It is impossible to overstate the value of location evidence and other communications records that can be obtained through the ECPA framework to law enforcement. These techniques allow us to find a kidnapped child, apprehend a dangerous fugitive, or

prevent a terrorist from following through on a violent plan. Time is always a factor in investigations, and the more important the investigation, the more important time becomes. Most of the DigitalDueProcess.org principals claim to be "clarifying" or "simplifying" the law, but in fact they are also raising the level of proof from some lower standard to probable cause. Any time you elevate the level of proof required for law enforcement to gain access to the records it needs, you run the risk of increasing the time it will take for law enforcement to reach time-critical stages of its investigations, or reduce the number of investigations in which the techniques can be used.

On that note, let me address a point that DigitalDueProcess.org has made in support of their efforts to raise the level of proof in these cases: they say that their proposals won't affect law enforcement's ability to get communications records in truly critical cases, because there are emergency provisions in many of the laws in this area. I would respectfully differ; those emergency provisions will not insulate law enforcement from the consequences of a significant change in the law. In many cases, under current law, the decision of whether or not a particular set of circumstance constitutes an emergency lies in the hands of a civilian employee in the service provider's call center, rather than in the judgment of a law enforcement officer with all the facts of the case and all their experience and training to call upon. Couple that with the demands placed on the often overwhelmed, understaffed call centers at many service providers, and the result could be a refusal to declare an emergency in a case where it is warranted, leaving law enforcement without recourse.

In closing, the present balance of judicial supervision and law enforcement efficiency has existed for some time, and should not be abandoned without a demonstrated need for an increase in privacy and a demonstrated pattern of abuse – presently nonexistent -- by government officials. Yes, isolated instances of abuses have been cited by the ACLU, but to say that enforcement as a whole should be deprived of efficient use of this valuable tool because of those isolated instances is the functional equivalent of saying that police officers shouldn't be allowed to carry firearms because there have been some instances where officers discharged their weapons when they shouldn't have done so.

The tools ECPA provides law enforcement are incredibly valuable, and the current legal framework balances liberty and safety appropriately. I would respectfully urge the members of the subcommittee to seek testimony from a number currently serving law enforcement professionals about the effects of DigitalDueProcess.org's proposals before adjusting a framework that is of such critical importance to public safety.

1000 Chesterbrook Blvd
Suite 200 Berwyn, PA 19312

+1 610.680.1000 tel
+1 610.680.2136 fax
info@trueposition.com
www.trueposition.com

August 3, 2010

The Honorable Jerrold Nadler
Chairman, Subcommittee on the
Constitution, Civil Rights and Civil Liberties
Committee on the Judiciary
House of Representatives
Washington, D.C.

Re: Response of TruePosition, Inc. to
follow up questions- Electronic Privacy and Communications
Act Hearing, June 24, 2010

Dear Chairman Nadler:

Please find attached TruePosition's response to follow up questions relating to the Subcommittee's hearing addressing the Electronic Privacy and Communications Act (EPCA) Hearing on June 24, 2010.

TruePosition would be pleased to assist the Subcommittee and provide further information with regard to issues associated with EPCA. Please do not hesitate to contact me at 212.301.2814 or via electronic mail at Michael.Amarosa@TruePosition.com.

Respectfully,

Michael Amarosa
Senior Vice President- Public Affairs

Copy to:
The Honorable F. James Sensenbrenner Jr.
Ranking Minority Member

**Congressman Henry C. "Hank" Johnson, Jr.**
**Questions for the Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services**

**June 24, 2010**

1. **If EPCA reform is passed, would it interfere with service providers in their providing information to law enforcement?**

   Amendments to the Electronic Communications Privacy Act (EPCA) are necessary to align the law with the technology advances that have evolved since its last examination by the Congress. Recognizing how location technology has emerged as a crucial element to effective emergency response by police, fire, emergency medical and other emergency service agencies is but one example of what should be explicitly recognized by the law. Advances in wireless technology has delivered more services to vastly more Americans and served to enhance a core government responsibility- responding to a citizen confronted with an emergency.

   ECPA was enacted to establish rules governing how law enforcement agencies can obtain third party information from telecommunications carriers and other service providers. The law seeks a careful balance between the legitimate needs of law enforcement, the burdens on carriers and service providers and the public's reasonable expectations of privacy. With the enormous technology changes in how information is transmitted, stored and disposed of, the Subcommittee's examination and record is vital to determining that balance for the current and future environment. Included in the review is the need to structure a fair and expeditious process that does not burden carriers or providers while serving crucial nation security and law enforcement responsibilities. The ability to respond to emergency circumstances where death or serious bodily injury is threatened should be an important facet of the structure that emerges.

   TruePosition believes that a fair balance can be struck. Yet it defers to the national security and law enforcement agencies, telecommunications and other service providers and public interests groups, and ultimately to the Congress as to how to best formulate the balance. TruePosition's purpose in participating in the hearings is to provide insight to the technical characteristics of wireless location technology to assist the Subcommittee. We present no stance with regard to what amendments should be enacted. In providing technology and services, TruePosition's foremost principle is fidelity to the laws Congress enacts.

**Congressman F. James Sensenbrenner, Jr.**

**Questions for the Record**
**House Constitution Subcommittee Hearing**
**"Electronic Communications Privacy Act Reform and the Revolution in Location-Based Technologies and Services"**

1. **How does GPS technique differ from Uplink-Time-Difference of arrival? How do these differ from the cell-site location information we have heard today about today? What are the differences in accuracy for locating the handset/cell-phone of each of these?**

Cell-site location information is an element of a carrier's network. Generally, the data presents the broad geographic area which can be used to identify the appropriate region, quadrant or a more refined area of the call. In most circumstances, the data is not precise enough to assist with identifying a location that can be used for emergency dispatch.

Two geolocation technologies have evolved to address the requirement for more specific and reliable information to dispatch emergency response, a handset based technique known as GPS/AGPS and a network based technique known as UTDOA.

Geolocation is the process of determining the location of a point in a coordinate system by measuring the distances from the point of unknown location to three or more points of known location. Graphically, in two dimensions, the location of the unknown point can be visualized as the common intersection of three circles whose centers are at the location of the known points and whose radii are the measured distances. Radiolocation uses the properties of radio waves to measure the distances from the unknown point to the known points. The specific property utilized is the velocity of radio wave propagation. Radio waves propagate, i.e. travel, at a constant velocity. Therefore, the distance between two points can be determined by measuring the time it takes a radio wave to travel between the two points and multiplying by the velocity of propagation of radio waves to derive the distance.

*Global Positioning System*

The Global Positioning System (GPS) uses this property of radio wave propagation to permit the determination of the location of a GPS receiver. The GPS is comprised of at least 24 satellites constantly orbiting the earth in six low earth orbits. Each satellite possesses a very accurate time clock that is synchronized with the time clocks in all of the other GPS satellites. Each satellite transmits at least one civilian signal with its own unique signature, i.e. code, with its time of transmission and location of the satellite embedded into it. GPS receivers on the surface of the earth with an unobstructed view to a number of GPS satellites receive the transmissions from them and note the time of reception with respect to their local clock. Typically, at least four GPS satellites uniformly distributed about the sky must be received to accurately solve for the latitude, longitude, elevation and time offset between the GPS receiver's local clock and the GPS satellites' clocks. Reception of more than four satellites will improve the

accuracy of these four quantities. Reception of only three satellites permits determination of the latitude, longitude and time offset but not the elevation of the GPS receiver. The GPS was primarily designed for outdoor radiolocation because it requires an unobstructed view of satellites uniformly distributed about the sky by the GPS receiver, i.e. a clear view of the sky.

There is another property of radio wave propagation that is important to consider in radiolocation. Radio waves emanate spherically from their source to their destination as opposed to a single point-to-point path from their source to their destination. This property permits multiple listeners to hear radio broadcasts even though they are at many different locations. The consequence of this spherical spreading for radiolocation is that the power of the radio wave diminishes as it gets further from its source. Noise is always present in receivers and a receiver can get so far away from a transmitter that the transmitter's signal cannot be received reliably because its power is too low with respect to the ever present noise level. The distance between GPS satellites and GPS receivers on the surface of the earth is approximately 26,560 kilometers. Thus, the powers' of GPS signals are fairly low, with respect to noise, when they reach the surface of the earth even with an unobstructed view of the satellites by the GPS receiver. The power transmitted by GPS satellites is fixed.

GPS receivers used indoors will suffer additional attenuation, i.e. reduction in power, of the GPS satellite signals by the materials that buildings are constructed of. When a radio wave impinges upon building material a portion of its power will be reflected and the remaining portion will be refracted into the building material. Reflection and refraction of radio waves results in attenuation of the radio wave and, ultimately, an even lower power signal arriving at the GPS receiver. Assisted GPS (AGPS) is a technique devised to enhance the integrity of received GPS satellite signals by providing the GPS receiver additional information about the GPS satellite signals so low powered ones can be recovered better in the presence of noise. AGPS provides significant enhancement of the GPS satellite signals permitting them to be received reliably in some indoor environments, like residential structures constructed primarily of wood.

However, the attenuation of GPS satellite signals by buildings constructed of metal, concrete and metal tinted glass is too great to permit indoor reception in these types of buildings even with the signal enhancement provided by AGPS. Wireless handsets with AGPS receivers are unable to receive a sufficient number of satellites to determine an accurate location indoors of these common buildings.

*Uplink-Time-Difference-of-Arrival*

Uplink-Time-Difference-of-Arrival (UTDOA) is a network based geolocation technique used for determining the location of E911 calls made from GSM handsets on their networks. Like GPS it is also a time based geolocation technique in that it measures the time of travel of radio waves. Specifically, the difference in time it takes the radio wave to travel from the handset to a pairs of LMUs is the information utilized for UTDOA geolocation. However, the radio wave it measures is the same signal the GSM handset uses for signaling and communications on the GSM network. It measures the time of travel to multiple auxiliary receivers collocated with the base stations. These auxiliary receivers are known as Location

Measurement Units (LMU) and are very accurately time synchronized to each other. A minimum of three LMUs must receive the handset's GSM signal to uniquely determine the location of it. Reception of the handset by more than 3 LMUs also enhances the accuracy of the location estimated. In this regard, UTDOA suffers in extreme rural conditions where cell sites are arranged in a "string of pearls" configuration.

Although the radio waves UTDOA measures are reduced in power by attenuation from building materials just like GPS, UTDOA provides accurate and reliable geolocation of handsets even when they are indoors. This occurs for two reasons. First, the distances between the transmitter, i.e. the handset, and receiver, i.e. the LMU, is much less than with GPS so there is much less loss due to spherical spreading of the propagating radio wave. Second, and more significant, the power output of handsets can be varied and are controlled by the wireless network and dynamically adjusted many times per second to assure reliable communications. Thus, when the loss between the transmitter and receiver increases because of attenuation by building materials, the wireless network commands the handset to increase its output power to compensate for this additional attenuation in order to achieve reliable communications. If a handset can communicate with its wireless network from indoors then UTDOA can reliably and accurately geolocate it.

**2. Can you give us some examples of how cell-site location information has had a life saving outcome in a medical or a non-law enforcement environment?**

A/GPS and UTDOA, in contrast to basic cell site information, are technologies providing significant enhancement to dispatching emergency response. The greatest challenge 911 Centers face is determining where an emergency is. The standard of emergency dispatch is providing the most effective resources in the most expeditious way possible. Time is unforgiving. Those calling for emergency services are unsettled and distressed even in familiar surroundings. That the trauma of an event delays response is affirmed emphatically by the daily experience of police, fire, ambulance and other emergency service agencies.

Mobile device customers expect that 911 Centers have location ability paralleling the wireline environment. There are now more than 265 million mobile devices in the US. The estimates that nearly 50 percent of emergency calls originate from mobile devices are confirmed in the US, Canada, the European Union and Australia. Over half of these calls are placed indoors. The US is the global leader is location technology. In this regard, since the FCC's rules addressing location accuracy became effective, the improvements in emergency response-dispatching emergency response to the correct location- are measureable and now the accepted standard. The circumstances detailed below are but two incidents where location technology was crucial:

- In February 2008, the United States Coast Guard (USCG) station in Corpus Christi, Texas received an emergency call from a boater after his boat capsized in the Gulf of Mexico. The caller was swept overboard and carried out to sea by strong currents; he was confused and unaware of his position. Although wireless coverage was marginal, the boater was able to use his mobile phone to make

contact with the USCG that he was in urgent need of assistance. But due to his location on the extreme fringe of the wireless network coverage, the call disconnected before the boater was able to convey more information about his position, direction of travel, or time of departure from port. With only with the boater's mobile phone number, the USCG faced a search and rescue mission covering an estimated 100 square miles.

USCG contacted the wireless carrier that serviced the call to obtain any information that would narrow the search area. The wireless carrier used TruePosition's Uplink Time Difference of Arrival (U-TDOA) Location Platform to comply with the FCC's E9-1-1 Phase II mandate. The USCG officers provided the wireless carrier with details establishing reasonable belief of an imminent threat to life. The carrier's security personnel determined the last known registration event and the serving cell site/sector information.

The information coincided with the time of the mayday call to USCG. While this historical information provided the USCG a geographic direction in which to focus its search, it was unable to narrow the size of the search area from the initial scope of 100+ square miles. Prevailing currents carried the boater to a sandbar in the gulf. There, he reestablished a network signal and made a second call to the USCG. The wireless carrier activated the U-TDOA Location Platform. U-TDOA was able to quickly calculate the boater's precise location and the wireless carrier provided the latitude and longitude coordinates to the USCG for rescue.

Two factors made the difference in this search and rescue mission. First, the boater's wireless carrier deployed U-TDOA, enabling the location of any mobile phone, in any environment. Second, because it is based on U-TDOA technology and not GPS satellites, the system had the ability to locate all active handsets — whether making calls or idle — allowing the wireless carrier to query this information in a critical situation.

- On July 8, 2010 CBS 11 and TXA 21 News in Dallas, Texas reported that a North Richland Hills Texas man nearly died after accidentally swallowing a plastic fork. The incident happened after the man had stopped at a local restaurant and bought a salad to bring home for lunch. He commenced eating it while watching the news and started to choke. After failing to dislodge the blockage, he called 911 on his cell phone, but was worried that dispatchers would not be able to find his address without a landline. The 911 tape reveals a man clearly in distress, gagging and choking on the phone. At times, the man's voice was barely a whisper. But a fast-acting North Richland Hills 911 dispatcher was able to locate the caller's address and dispatched a detective who was in the vicinity. The dispatcher's and detective's fast actions likely saved the man's life.

  For further details, see
  http://cbs11tv.com/local/Plastic.Salad.Fork.2.1793639.html

**3. Does a phone or other device that has GPS capability always transmit location information or does the user of the device have to activate the function such as placing a 911 call?**

In a GPS device, the user has the ability to activate the location function of the device; when 911 is dialed, the carrier is obligated to provide the 911 center the location of the device consistent with FCC rules. Network based location technology can locate all devices.

**Marc J. Zwillinger**

**Responses to Questions for the Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services**

**August 4, 2010**

**Questions from Congressman F. James Sensenbrenner, Jr.**

1. *Should a search warrant be required for all types of location information, some of which may not be very precise?*

   **Not necessarily. In keeping with the public's expectation of location privacy, the standard should reflect both the relative precision of the location information and the nature of the tracking. A lesser standard than a warrant may be appropriate where the data sought is relatively nonspecific and isolated in time. For example, such a standard may be aptly applied where the government is seeking data that only discloses a target's location within a twelve mile radius of a cell tower at the time a call is placed. However, as there is a greater expectation of privacy in one's precise location, a showing of probable cause should be required before the government is given access to GPS data that can pinpoint a target's location inside a building or provide multiple location points from which a targets movement can be tracked.**

2. *Wireless carriers retain or have access to a wide range of location information; some of it is very general. Would the Digital Due Process proposal sweep in routine business records showing that customer was roaming on another network somewhere in Europe a month ago? If so, how do you define the outer boundaries of "location information?" Is an area code location information?*

   **No. Area codes are imprecise and therefore do not raise the same sort of privacy concerns as granular location data. For example, area codes do not indicate where the person is at the time he or she placed the call. Currently, area codes would likely be included as connection records under ECPA and can be obtained through use of a subpoena. This**

**standard seems appropriate as this data does not reflect the location of a target at any given time.**

3. *Is there a diminished expectation of privacy when a cell phone user is using a service like "Loopt," that shows friends and family where users are?*

**A Loopt user's expectation of privacy is largely dependent on the privacy controls that the individual has implemented on Loopt. If the user only divulges his location to specific family and friends, then as with social networks, he likely retains a certain expectation that his location is "private" and the content (in this case the location information) should be protected from government access. However, if the user has made his account information available to the public, it would be very difficult to then argue that the location should be protected.**

**Marc J. Zwillinger**

**Responses to Questions for the Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services**

**August 4, 2010**

**Questions from Congressman Henry C. "Hank" Johnson, Jr.**

1. *As an attorney, could you describe the negative effects of the uncertainty that currently exists under the law?*

   **The lack of certainty under ECPA has resulted in confusion and inefficiencies for the courts, law enforcement agencies, service providers and users.**

   **The resources of the legal system, including the courts and law enforcement are wasted on litigation of the applicable standards. Judges across the country are spending hours hearing these cases and issuing lengthy and conflicting decisions with differing standards as to how the government may access location information. The variation can cause friction between service providers and law enforcement on a daily basis, especially when the provider and the law enforcement agency are located in different judicial districts.**

   **Further, the unsettled nature of the law can place prosecutions by law enforcement in jeopardy. Although ECPA has no suppression remedy, any data collection that is authorized under the Act but which does not meet constitutional standards may result in a conviction that is subject to reversal should an appellate Court find that the information was obtained unlawfully.**

   **As the holder of the data, service providers are negatively impacted by the unpredictability of the law, as they are often caught in the middle of litigation. (*See question 3 for additional discussion*).**

   **Also, electronic service subscribers suffer under the current state of the law because they can never be certain whether the data collected through their interaction with a particular service will be secure if it is requested by**

**law enforcement. This may discourage certain subscribers from using the services.**

2. *Conversely, what would be the benefits of a reform that would introduce a great degree of certainty and consistency in the application of the ECPA statute?*

   **A law that could be consistently applied would better protect privacy rights, and at the same time facilitate the exchange of information between law enforcement agencies and service providers. The enactment of new legislation with properly robust standards could potentially prevent law enforcement agencies from overstepping their bounds, provide clear guidelines so that service providers are certain what they can and cannot disclose and protect the integrity of prosecutions by ensuring that evidence properly obtained under the statute will be admissible.**

   **Another potential benefit of ECPA reform is the conservation of judicial resources. As technology has become increasingly sophisticated, magistrate judges have devoted a significant amount of time to analyzing the correct application of a 1986 law to 2010 electronic communications. In fact, over the past five years, at least 30 federal opinions containing varying standards for government access to cell phone location information were published. Enacting a standard that is more easily applied and consistently applied would reduce the time spent litigating these issues.**

   **Additionally, new legislation could provide subscribers with a clear understanding of the security of their data and help inform their expectation of privacy connected to the electronic services they use.**

   **Finally, new legislation would also benefit service providers. (*See answer to Question 3*).**

3. *If ECPA reform is passed, would it interfere with service providers in their providing information to law enforcement?*

   **No. In fact, it would likely help service providers better comply with government demands. Because ECPA has not been applied consistently, service providers are uncertain of their responsibilities to law enforcement. As a result, service providers are often forced to litigate issues surrounding the disclosure of information. For example, service providers**

that prudently withhold information that falls into the "grey areas" of ECPA often find themselves answering government motions to compel. On the other hand, service providers that are deemed to have improperly disclosed information - like the service provider in *Quon v. Arch Wireless Operating Company, Inc.* -- may later find themselves held civilly liable for those disclosures.

School of Engineering and Applied Science
Department of Computer and Information Science
3330 Walnut Street, Levine Hall
Philadelphia, PA 19104-6309
Tel 215.898.8560 Fax 215.898.0587
www.cis.upenn.edu

August 20, 2010

Subcommittee on the Constitution, Civil Rights and Civil Liberties
Committee on the Judiciary
House Of Representatives
111th Congress of the United States
2138 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Nadler, Rep. Sensenbrenner, and Rep. Johnson:

Thank you very much for the opportunity to testify before the Subcommittee on the Constitution, Civil Rights and Civil Liberties at the hearing on ECPA Reform that was held June 24th. It was a great honor to testify on such an important, and yet technologically complex, matter as location-based technologies. I am certain that your work on this issue will, in the years to come, prove extraordinarily important in ensuring both law enforcement access to critical information and in protecting the privacy of law-abiding Americans as they use an increasingly pervasive array of technologies that incorporate more and more precise geo-location capabilities.

This letter is in response to your letter of August 9th in which you forwarded additional questions from Reps. Johnson and Sensenbrenner. My responses for the record are attached. As with my hearing testimony, these responses are my own, and do not represent any other party.

Thank you again for the opportunity to testify, and I will, of course, be glad to respond to any further questions the committee may have and to assist you and your staff in any way that I can.

Respectfully,

Prof. Matt Blaze

**Responses of Matt Blaze on ECPA Reform, August 20, 2010**

**Rep. Johnson** asks:

**Question: If ECPA reform is passed, would it interfere with service providers in their providing information to law enforcement?**

**Response**: My understanding is that the various proposals for ECPA reform deal with clarifying the legal standards under which subscriber location information can be provided to the government under different circumstances. I am not aware of any provision proposed or under consideration that would interfere with a service provider's ability to respond to a lawful request from the government.

On the contrary, I would expect that, with the benefit of clear legal standards for what information information can be provided under what legal standards, service providers would be better able to quickly and confidently respond to law enforcement requests under ECPA reform than they are today. The current law is, at best, ambiguous, and as the location technology incorporated into cellular and other wireless services advances to reveal more precise and real-time location information as part of ordinary business record records, the current (ambiguous) legal standard for what can be provided and when will become more and more difficult to apply. ECPA reform will remove this increasing degree of uncertainty, and this should facilitate, rather than hamper, information sharing between service providers and law enforcement.

**Responses of Matt Blaze on ECPA Reform, August 20, 2010**

**Rep Sensenbrenner** asks:

**Question 1 [Rep. Sensenbrenner]: Location information has been described to use in three general categories: 1) How close is a subject to a tower? ; 2) How close is a subject to "these towers (triangulation)"? ; and 3) GPS data. How broadly is the term "location information" used? In your opinion, is that part of the confusion from what you heard at the hearing?**

**Response**: In today's wireless networks, location information might be collected about a subscriber by any (or a combination) of the three techniques you describe. The term "location information" can be sensibly applied regardless of which of these techniques are used to collect it.

Going forward, I believe it is very important *not* to tie the concept of "location information" to any particular geo-location technique, because the effective differences in precision yielded by these techniques are, to a large extent, disappearing as wireless technology advances. Historically, the best location precision required that the subscriber's handset be equipped with a GPS satellite receiver, but emerging cellular location technologies are able to locate a handset with a precision that approaches that of GPS, even for subscribers that do not have GPS or that are not in "view" of the GPS satellites.

**Responses of Matt Blaze on ECPA Reform, August 20, 2010**

**Question 2 [Rep. Sensenbrenner]: How specific is the historical cell-site location information that is maintained by a service provider? What information can be learned from obtaining single tower information that a cell phone has communicated with? Does the information that is maintained vary from provider to provider?**

**Response:** Every cellular provider has its own policy for the call detail records that it maintains, what is contained in these records, and how long the records are maintained. Some providers divide their records into two classes: "billing records", which comprise the records of incoming and outgoing calls and the tower location that served them, and "maintenance records", which may include far more detailed information, such as records of when subscribers' handsets move through the network even when no calls are being made.

The degree of information that can be obtained from these records depends on the precise collection practices of the particular provider. Some providers may collect only information about the nearest tower; as I discussed in my testimony, how revealing this is depends on the density of the area in which the subscriber is located. Other providers, however, may collect more precise information and may collect location records at more frequent intervals, which might reveal, for example, not only a subscriber's individual locations but also his or her direction and rate of travel, travel habits, and other patterns of behavior.

**Responses of Matt Blaze on ECPA Reform, August 20, 2010**

**Question 3 [Rep. Sensenbrenner]: Explain the difference in the specificity of cell-site location as between a rural vs. an urban environment.**

**Response:** Current cellular systems work by dividing their coverage area into small local "sectors", each served by a base station or tower located within the sector. The most basic technique for locating a cellular subscriber's handset in these systems is to identify the particular base station that handled a call, which gives the sector in which the handset was located during the call. That is, someone who knows the base station that handled a call could infer that the handset was located somewhere within that base station's coverage sector.

The size of a sector is limited by two factors. The first is the maximum range that the (relatively low power) cellular radio signals will cover from the base station location. This depends very much on the terrain; in a flat, open environment (such as rural farmland), a well-located base station could theoretically cover a radius of five miles or more. In an urban environment, littered with objects (such as tall buildings) that tend to absorb and obstruct radio signals, this radius will be much smaller, sometimes as little as a few city blocks. A relatively new generation of cellular base stations (called "microcells") are deliberately engineered to cover only very small areas, such individual office complexes or residences, to fill in coverage gaps in sector areas.

**Responses of Matt Blaze on ECPA Reform, August 20, 2010**

Another factor that limits the maximum size of a sector is the number of subscribers in the sector's coverage area. A cellular base station can handle only a limited number of simultaneous voice calls and data traffic. As cellular service has become more popular and as higher-bandwidth services (such as 3G internet) have become available, base station sectors have had to become correspondingly smaller, to accommodate the increasing density of cellular users in any given area.

The effect is that in very sparsely populated areas that are relatively flat, the information revealed by a sector may even today locate a handset only to within several miles. But in an urban environment or in an area served by microcells, a sector can today be a very precise locator. In some environments, the sector by itself effectively locates a handset to within a particular building, floor of a building, or even to within a particular room or suite of rooms.

**Responses of Matt Blaze on ECPA Reform, August 20, 2010**

**Question 4 [Rep. Sensenbrenner]: Please explain the concept of triangulation. Is the data that is needed for triangulation constantly transmitted whereby it can be directly intercepted by law enforcement, or is this information maintained and obtained from a service provider as something they monitor for billing and quality of service purposes?**

**Response:** "Triangulation" in this context refers to a range of techniques for more precisely locating a cellular subscriber handset by comparing the radio signal received from the handset at multiple vantage points. A variety of triangulation technologies can be used to accomplish this; some use the angle at which the radio signal arrives at different places, while others compare the precise time the signal arrives at different points. Early cellular networks did not incorporate triangulation capabilities into the network infrastructure.

Current and emerging cellular infrastructure, however, increasingly incorporates some form of triangulation-based location capability into the network that can be used to locate individual subscriber handsets at any time they are turned on and registered with the network. There are two reasons for this. The first is to enable compliance with the FCC's "E911" mandate for more precisely locating cellular callers to emergency services. When a subscriber places a call to 911, many cellular networks automatically employ some form of triangulation and automatically transmit the calculated location of the caller to the 911 call center. But

many cellular networks also increasingly collect triangulated location information about subscribers who are not placing calls to 911. This data is collected for maintenance and network optimization purposes. It tells the provider where its customers are located, how well its infrastructure is performing in different places in is coverage area, and indentifies where new bases stations might be required or where existing base stations might be redundant. As cellular base station technology has advanced, this data is increasingly easy and inexpensive to collect, and is extraordinarily valuable for the cellular provider's business purposes. Although each provider will have its own policy for when such data is collected, how it is stored, and how long it is retained, we can expect the collection of such data to become more and more routine as the technology becomes more pervasive.

Law enforcement agencies can and do rely on location information provided by cellular providers to locate the telephones of suspects and other surveillance targets. They can also, under some circumstances, collect cellular location data themselves, without the direct cooperation of the service provider. A variety of devices are marketed to and use by law enforcement (going by trade names such as "Triggerfish", "Stingray", and others), that can identify the cellular phone numbers in use in an area and that can calculate a directional bearing along which a given handset is located. These devices are typically used as an adjunct to physical surveillance. They allow a surveillance team to effectively "follow" a subject (and his or her phone) even without visual contact, and can identify the phone numbers of the cellular phones used by or in proximity to a surveillance target.

Written Statement of the
American Civil Liberties Union

Laura W. Murphy
Director
ACLU Washington Legislative Office

Christopher Calabrese
Legislative Counsel
ACLU Washington Legislative Office

Catherine Crump
Staff Attorney
ACLU Speech, Privacy and Technology Project

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

June 24, 2010

*Hearing on*

*ECPA Reform and the Revolution in Location Based Technologies and Services*

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

Chairman Nadler, Ranking Member Sensenbrenner, and Members of the Committee:

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

The danger posed by unregulated location tracking to American's privacy is real, immediate and universal. Because of the prevalence of mobile phones in modern society, almost every American is carrying a portable tracking device, one that can be used to reveal their current and past locations. These devices store their every move. Whether it is a visit to a therapist or liquor store, church or gun range, many individuals' locations will be available either in real time or months later. Because of the sensitivity and invasiveness of these records, law enforcement agents should always be required to obtain a warrant and show probable cause, no matter the technology employed or the age of the records.

Unfortunately, the government frequently obtains location tracking information without first obtaining a warrant and establishing probable cause. Law enforcement has obtained location information since at least the late 1990s[1] but more than a decade later we still have no uniform standard for when law enforcement can gain access to this information. While the Department of Justice has issued recommendations setting out when prosecutors should show probable cause, Freedom of Information Act requests (FOIAs) by the ACLU demonstrate that United States Attorney Offices are ignoring these recommendations at least in some cases. Worse, the government has effectively prevented the creation of a uniform standard by refusing to seek appellate court decisions on the issue. This legal maneuvering has prevented public debate and allowed a practice that is inconsistent with our constitutional principles to become entrenched.

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

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

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

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

**Background**

As of June 2009, there were an estimated total of 277 million cell phone service subscribers in the United States – about 90% of the overall population.[2] Whenever these subscribers have their cell phones on, the phones automatically scan for cell towers and, approximately every seven seconds, the phones register their location information with the network.[3] The carriers keep track of the registration information in order to identify the cell tower through which calls can be made and received. The towers also monitor the strength of the telephone's signal during the progress of the call, in order to manage the hand-off of calls from one adjacent tower to another if the caller is moving during the call.[4]

The cell phone technology yields several types of location information of interest to law enforcement officers. The most basic type of data is "cell site" data, or "cell site location information," which refers to the identity of the cell tower from which the phone is receiving the strongest signal at the time and the sector of the tower facing the phone.[5] This data is less accurate because it relies on simple proximity to a cell phone tower so it can be anywhere from a 200 meter to 30 kilometer (656 feet to 18 miles) radius from the tower.[6] This range is shrinking,

---

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

[3] *See In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 534 F. Supp. 2d 585, 589-90 (W.D. Pa. 2008) (Lenihan, M.J.), *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *appeal docketed*, No. 08-4227.

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

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

[6] But sometimes, depending on topography or other impediments to transmission, a phone receives the strongest signal from a cellular tower other than the one that is closest to it. Hodor Decl., *supra*, at 7-8.

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

Beyond cell site location information, cellular service providers have the capacity and the obligation under the Wireless Communications and Public Safety Act of 1999 to create and disclose even more precise location information in certain emergencies.[9] Cell phone providers generate this data in two ways. First, under the "network-based approach," the providers triangulate information regarding the strength of the signals from the cellular towers nearest to the phone.[10] Under the Federal Communications Commission (FCC) guidelines this information must be accurate within 100 meters for 67% of the calls and within 300 meters for 95% of the calls by 2012.[11]

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

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

**Current Legal Practices for Accessing Location Information**

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

*Department of Justice Standards*

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

---

[7] *See* CTIA, *supra*, at 9.
[8] *See* Thomas Farley and Ken Schmidt, *Cellular Telephone Basics: Basic Theory and Operation*, http://www.privateline.com/mt_cellbasics/iv_basic_theory_and_operation/ (last accessed Dec. 21, 2009).
[9] Pub. L. No. 106-81, 113 Stat. 1286 (1999)
[10] *See* Note, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 Harv. J. L. & Tech. 307, 308-10 (2004); *See, e.g.*, *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 749-51 (S.D. Tex. 2005) (Smith, M.J.).
[11] 47 C.F.R. § 20.18(h)(1)(i).
[12] *See Who Knows Where You've Been?*, *supra*, at 308.
[13] 47 C.F.R. § 20.18(h)(1)(ii).
[14] Mario Aguilar, *GPS Power-Up: Get Ready for New Sense of Place*, Wired, April 19, 2010
[15] *See* CTIA, *supra*, at 9.
[16] *People v. Weaver*, 12 N.Y.3d 433, 441 (N.Y. 2009).

that the government can obtain most cell phone location information by demonstrating to a judge or magistrate that the information is relevant and material to an ongoing criminal investigation. According to a document obtained by the ACLU and the Electronic Frontier Foundation (EFF) through a FOIA request, it is DOJ's policy to obtain mobile location information under the following standards[17]:

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

The DOJ maintains that the government need not obtain a warrant and show probable cause to track people's location with only one exception: real-time GPS and triangulation data. Since at least 2007, DOJ has recommended that U.S. Attorneys around the country obtain a warrant based on probable cause prior to engaging in precise cell phone tracking.[18]

This policy position turns out to be more disturbing because some U.S. Attorney offices don't comply even with this very lax set of guidelines.[19] The ACLU's and EFF's FOIA litigation revealed that U.S. Attorney Offices in the District of New Jersey and the Southern District of Florida both obtain even the most precise cell tracking information without obtaining a warrant and showing probable cause.[20] Because the FOIA focused on only a small number of U.S. Attorneys offices around the country, it may well be that many other offices also ignore DOJ's recommendation.

In fact, this practice may be widespread. There are no published legal opinions on the lawfulness of warrantless cell phone tracking in either the District of New Jersey or the Southern District of Florida, and yet the FOIA litigation proved conclusively that cell phone tracking occurs in those districts and indeed that federal prosecutors do not feel obligated to show probable cause for even the most invasive forms of this surveillance. In the vast majority of judicial districts in this country, there are no decisions addressing cell phone tracking, yet there was cell phone tracking occurring in every district subject to the FOIA, even where there is no published opinion.[21] Given that cell phone tracking is now a decades-old law enforcement technique that has proven useful, we must assume authorities use it in all or essentially all of the country, most frequently under an unknown standard.

---

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

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

[19] Letter from William G. Stewart II, to Catherine Crump, *Mobile Phone Tracking (Items 3-5)/DNJ*, Dec. 31, 2008, available at http://www.aclu.org/pdfs/freespeech/cellfoia_released_074132_12312008.pdf; Letter from William G. Stewart II to Catherine Crump, *Mobile Phone Tracking(Items 3-5)FLS*, Dec. 31, 2008, available at http://www.aclu.org/pdfs/freespeech/cellfoia_released_074135_12312008.pdf

[20] *Id.*

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

*Procedures for Gathering Location Information*

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

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

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

Ex parte adjudication of cell phone tracking applications also contributes to the dearth of published legal opinions on the subject. Ex parte proceedings - when the government presents its arguments in favor of surveillance without presentation of any opposing argument – will favor unpublished decisions because there is no motivation for the only party present – the government – to ask the court to render a public decision. The ACLU and others have tried to remedy the situation by offering to submit amicus briefs to present the pro-privacy viewpoint. Unfortunately, because many applications for surveillance are so time-sensitive they must be acted on immediately, some judges have taken the position that there is unlikely to be a practical way to permit amicus participation.[25] As long as the judicial system continues to proceed in a manner that favors one side over the other, it emphasizes the need for a full, open and fair debate about the propriety of warrantless cell phone tracking in Congress.

*Reaction from the Judiciary*

---

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

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

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

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

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

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

This highlights the lengths the government will go to maintain a relevance standard. A valuable law enforcement technique is being disallowed repeatedly and the government is taking no appellate action. Decisions by magistrate judges and district court judges are not binding precedent, even on other judges of the same district court.[30] So long as there are at least some judges in a district who believe that warrantless cell phone tracking is permissible, the government will be able to get its application approved at least some of the time.

This is exactly the situation in the Southern District of New York, where one district court judge has approved warrantless real-time cell phone tracking in the absence of probable cause and another has held that probable cause is required.[31] Although the government initially filed a notice of appeal on the adverse ruling adverse, after the ACLU received permission to submit an amicus brief in the Second Circuit, the government sought and obtained multiple

---

[26] *In re Applications of the United States of America for Orders Pursuant to Title 18, United States Code, Section 2703(d)*, 509 F. Supp. 2d 76, 78 (D. Mass. 2007) (Stearns, D.J.); see W.D. Penn 2008 (Lenihan), 534 F. Supp. 2d at 600-01 (listing majority opinions holding that real-time cell site information cannot be obtained without a Rule 41 warrant)

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

[28] *In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008).

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

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

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

extension requests and then voluntarily dismissed its appeal.[32] Judges in the Eastern District of New York also split on the question and only prosecutors and the courts know how this issue is handled in the majority of the country where there are no published opinions.[33]

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

**Resulting Harms**

These practices have trampled on the rights of Americans and led to misuse. A recent *Newsweek* article highlighted the problem:

> "Some abuse has already occurred at the local level, according to telecom lawyer Gidari. One of his clients, he says, was aghast a few years ago when an agitated Alabama sheriff called the company's employees. After shouting that his daughter had been kidnapped, the sheriff demanded they ping her cell phone every few minutes to identify her location. In fact, there was no kidnapping: the daughter had been out on the town all night. A potentially more sinister request came from some Michigan cops who, purportedly concerned about a possible "riot," pressed another telecom for information on all the cell phones that were congregating in an area where a labor-union protest was expected."[34]

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

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

> "Sprint Nextel has even set up a dedicated Web site so that law-enforcement agents can access the records from their desks—a fact divulged by the company's "manager of electronic surveillance" at a private Washington security conference last October. "The tool has just really caught on fire with law enforcement," said the Sprint executive, according to a tape made by a privacy activist who sneaked into the event."[35]

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

---

[32] In re application for a cell site order, Case No. 09-0807 (2d Cir. docketed Feb. 27, 2009).
[33] *Compare* 396 F. Supp. 2d 294 (E.D.N.Y. 2005) (Orenstein, M.J.) (probable cause for prospective tracking) and 2009 WL 1530195 (E.D.N.Y. 2009) (Pollak, M.J.), (probable cause for prospective tracking, reversed by Judge Garaufis) *with* 2009 WL 1594003 (E.D.N.Y. 2009) (Garaufis, D.J.) (no probable cause necessary for prospective tracking);
[34] Michael Isikoff, *The Snitch in Your Pocket*, Newsweek, Feb. 19, 2010.
[35] *Id.*

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

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

> "Mr. NADLER. You keep for 20 years information about innocent people, private information that you have collected in the course of an investigation in which it turns out they had nothing to do with.
> Mr. MUELLER. We may well undertake an—an allegation may come in as to the involvement of a person in a mortgage fraud scheme. We go and investigate, find that that person is innocent, the allegation is false, we keep those records, yes."[37]

So the collection of the movements and habits of innocent people will remain part of an FBI profile for 20 years.

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

> "The following issues are faced by service providers every day in response to government demands for acquisition and use of location Information …
>
> d. Target v. Associates (hub and spokes). Regardless of the legal standard applicable to the target phone, what standard applies to obtain the location information for all those with whom the target communicates? **It is common in hybrid orders for the government to seek the location of the community of interest – that is, the location of persons with whom the target communicates.**" (emphasis added) [38]

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

---

[36] Brief of Amici Curiae in Support of Motion To Suppress, *United States v. Soto*, Case No. 09-cr-200 (D. Conn. June 18, 2010), available at http://www.aclu.org/files/assets/2010-6-18-USvSoto-AmiciBrief.pdf.

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

[38] *Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights and Civil Liberties*, 111th Cong. (2010) (statement of Albert Gidari, Partner, Perkins Coie LLP).

[39] It may be that the problem is actually *worse* than described here. In a report on the misuse of exigent letters the Department of Justice Inspector General describes widespread requests for community of interest information. Apparently it was part of "boilerplate" request language for at least some National Security Letters. *A Review of the*

**Conclusion**

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

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

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

---

*Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records*, Inspector General, Department of Justice, January 2010 at 56. Further according to an Office of Legal Counsel opinion there may be some telephone records that the FBI can access without any process under ECPA. *Id.* at 264.

epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

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

Marc Rotenberg, Executive Director
Jared Kaprove, Domestic Surveillance Counsel
Ginger McCall, Staff Counsel

Hearing on

"ECPA Reform and the Revolution in Location Based Technologies and Services"

Before the

Committee on the Judiciary
Subcommittee on the Constitution, Civil Rights, and Civil Liberties
United States House of Representatives

June 24, 2010
2237 Rayburn House Office Building
Washington, DC

Mr. Chairman, Members of the Committee, this statement was prepared for the hearing "ECPA Reform and the Revolution in Location Based Technologies and Services" to be held on June 24, 2010 before the House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights, and Civil Liberties. We ask that it be included in the hearing record.

The Electronic Privacy Information Center (EPIC) is a non-partisan public interest research organization established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC fully supports the Committee's examination of the Electronic Communications Privacy Act of 1986 (ECPA)[1] and locational information. Mobile devices have become ubiquitous in modern society, and they have become increasingly capable of recording and transmitting users' locations. In light of this, it is important that clear standards are formulated in order to protect the privacy of users by giving the users control over their own data and requiring an opt-in model for the use of this data. This statement outlines several steps that the Subcommittee on the Constitution, Civil Rights, and Civil Liberties can take to strengthen the privacy protection of US customers whose data is collected and used by companies around the world.

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

In 1999, Congress amended the Communications Act of 1934 with the Wireless Communication and Public Safety Act of 1999. The Act required wireless carriers to implement 911 emergency calling and added location privacy provisions to the Telecommunications Act.[2] Section 222 protects location information along with other customer proprietary network information (CPNI), requiring user "approval" for uses or disclosures.[3] CPNI includes "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier."[4]

Express prior authorization of the customer is required for uses and disclosures of "call location" information, with certain exceptions. These exceptions are to providers of emergency services, to family and guardians in emergency situations, and to information or database services solely for assisting in delivering emergency services.[5] Location technologies not based on CPNI, or not run by an entity subject to the § 222 protections, are not covered by these regulations. After the Act was passed, the Federal Communications Commission (FCC) considered a rulemaking to develop guidelines governing the collection and use of location data generated by wireless communications systems.

During this time, in April of 2001, EPIC filed comments encouraging the FCC to follow through on the rulemaking process because "location privacy is one of the most significant issues facing American consumers and the expeditious establishment of comprehensive,

[1] Pub. L. No. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. § 2510 et seq.).
[2] Pub. L. No. 106-81, 113 Stat. 1286 (1999).
[3] 47 U.S.C. § 222(c)(1).
[4] 47 U.S.C. § 222(h)(1)(A).
[5] 47 U.S.C. § 222(d)(4).

technologically neutral privacy protections would serve the public interest. "[6] EPIC recognized that locational tracking technologies "enable the creation of detailed daily itineraries for millions of consumers, [and] have the potential to fundamentally alter the nature and use of wireless communications systems. "[7] EPIC encouraged the FCC to enact rules that would give consumers "meaningful control over the collection and use of location data."

In later reply comments, EPIC stated that "rulemaking is needed . . . because some commenters recognize limits on implied consent, while others do not."[8] Because of this, EPIC encouraged the FCC to "carefully constrict the circumstances under which implied consent could be utilized, if at all"[9] and to clarify the meaning of several key terms—including "location information"—that are used in the Act. EPIC recommended a number of other rules, including a rule that would require consent to be specific as to the third party that can receive the information and the purpose for which that information will be used by that party, and a rule that would require carriers to keep a record of consent for as long as the permission is valid. With all of these steps, EPIC sought to give users greater control over their locational information by requiring opt-in consent for locational tracking.

The FCC ultimately declined to embark on rulemaking regarding the Wireless Communications and Public Safety Act. The Commission said that a federal statute enacted in 1999 "imposes clear legal obligations and protections for consumers,"[10] and that "the better course is to vigorously enforce the law as written, without further clarification of the statutory provisions by rule."[11] Commissioner Michael Copps dissented, citing EPIC's comments and arguing, "Commission action is needed because the statute's meaning apparently is subject to varying interpretations within the industry."[12]

### II. Locational Privacy Concerns are Substantial and Growing More Severe

The FCC's failure to address locational privacy issues should be remedied as soon as possible. The problem grows more severe as the number of mobile device users increases and location-based advertising technology becomes more advanced. The number of American cell phone users increases every year. The Pew Research Center found that 77% of all adults had a cell phone or other mobile device in 2008.[13] By April 2009, this number had risen to 85%.[14]

Cell phone usage is also increasingly commonplace among younger demographic groups. A Pew Research Center study on Social Media and Mobile Internet Use Among Teens and

---

[6] EPIC, Comments to the F.C.C. on Commission Public Notice, DA 01-696 (Apr. 6, 2001), *available at* http://www.epic.org/privacy/wireless/epic_comments.pdf.
[7] *Id.*
[8] EPIC, Reply Comments to the F.C.C. on Commission Public Notice, DA 01-696 (Apr. 24, 2001), *available at* http://www.epic.org/privacy/wireless/epic_reply.pdf.
[9] *Id.*
[10] F.C.C., Order Declining to Commence Rulemaking to Establish Fair Location Information Practices (July 24, 2002), *available at* http://epic.org/privacy/wireless/FCC_order.pdf.
[11] *Id.*
[12] *Id.*
[13] Pew Research Center, Teens and Internet Over the Past Five Years: Pew Internet Looks Back (Aug. 19, 2009), *available at* http://www.pewinternet.org/Reports/2009/14--Teens-and-Mobile-Phones-Data-Memo.aspx.
[14] *Id.*

Young Adults reported that three-quarters (75%) of teens and 93% of young adults ages 18-29 now have a cell phone. The level of usage in this age group has jumped rapidly from 2004 (45% of teens had a cell phone), to 2006 (63% of teens had a cell phone), and then to 2008 (71% of teens had a cell phone).[15] The Pew Research Center found that "in the past five years, cell phone ownership has become mainstream among even the youngest teens. Fully 58% of 12-year-olds now own a cell phone, up from just 18% of such teens as recently as 2004."[16]

Mobile devices have also become an increasingly popular way to access the internet. A 2009 Pew Research Center study reported that 55% of American adults connect to the internet wirelessly, either through a WiFi or WiMax connection via their laptops or through their handheld device like a smart phone.[17] Roughly half of 18-29 year-olds have accessed the internet wirelessly on a cell phone (55%).

Advertisers and technology companies are taking advantage of these trends and the lack of federal regulation by developing technology that uses mobile device GPS tracking capabilities in order to gather users' information and serve targeted advertisements. On February 19, 2010, it was reported that Point Inside, a company that makes shopping center mapping and navigation apps for smartphones, had announced the launch of its new indoor mobile advertising platform that provides the indoor location and location-specific advertising for mall-based retailers and brands.[18] Advertisements are served on smartphones based on user location and interest in a particular store or brand.[19]

In late 2009, Google announced the launch of a Google smartphone, called the Nexus One. There was wide speculation that Google, the internet's largest advertising company, would use these mobile devices as another opportunity to place advertisements.[20] Some speculated that the company would offer users the choice to subsidize the phone cost by accepting advertisements—a strategy that has been employed by a company in Germany.[21]

Apple, the creator of a number of mobile devices, including the iPhone and iPad, recently made an announcement that applications which utilize location-based advertising would be spurned from its applications store. This announcement, paired with the company's recent

---

[15] *Id.*
[16] Pew Research Center, Social Media and Mobile Internet Use Among Teens and Young Adults (Feb. 3, 2010), *available at* http://pewresearch.org/pubs/1484/social-media-mobile-internet-use-teens-millennials-fewer-blog.
[17] Pew Research Center, Internet, Broadband, and Cell Phone Statistics (Jan. 5, 2010), *available at* http://www.pewinternet.org/Reports/2010/Internet-broadband-and-cell-phone-statistics.aspx.
[18] Mobile Marketing Watch Blog, *Point Inside Launches Indoor Mobile Advertising Solution Via SmartMap Android/iPhone Apps*, Feb. 19, 2010, http://www.mobilemarketingwatch.com/point-inside-launches-indoor-mobile-advertising-solution-via-smartmap-androidiphone-apps-5414/.
[19] *Id.*
[20] Matt Hamblen, *Google's Nexus One Smartphone: Will Mobile Ads Offset Cost?*, Computer World, Dec. 14, 2009, http://www.compnterworld.com/s/article/print/9142245.
[21] Matt Hamblen, *Alcatel Lucent to Serve Mobile Ads to Wireless Customers in Germany Who Opt-in*, Computer World, June 29, 2009, http://www.computerworld.com/s/article/9134904.

acquisition of advertising firm, Quattro Wireless, has caused increasing speculation that Apple, itself, plans to have exclusive control over location-based advertisements on its products.[22]

Indeed, with the release of its newest operating system for the iPhone and iPad devices, iPhone OS 4.0, alongside a new advertising platform called iAd, Apple has altered[23] its Terms of Service for users of those devices to include a provision that "Apple and [its] partners and licensees may collect, use, and share precise location data, including the real-time geographic location of your Apple computer or device."[24]

Another recent grab for locational data has come from Google's Street View product. When Google began the Street View project in 2007, many privacy concerns were raised, but the debates focused almost exclusively on the collection and display of images obtained by the Google Street View digital cameras. It has been revealed Google was also obtaining a vast amount of Wi-Fi data from Wi-Fi receivers that were concealed in the Street View vehicles. Following independent investigations, Google now concedes that it gathered MAC addresses (the unique device ID for Wi-Fi hotposts) and network SSIDs (the user-assigned network ID name) tied to location information for private wireless networks.[25] Google also admits that it has intercepted and stored Wi-Fi transmission data, which includes email passwords and email content.[26]

As of June 18, 2010, investigations of Google's Street View Wi-Fi data collection have been initiated in eighteen countries and several U.S. states, as well as by the FTC and the FCC.[27] EPIC has written to the FCC suggesting that the actions may have violated, among other things, the Wiretap Act as amended by ECPA.[28] Congressmen Edward Markey and Joe Barton wrote a letter to the FTC asking for such an investigation, also asking whether that agency believed Google had violated federal law.[29]

These examples show the ubiquitous nature of access to location-based data and the necessity of clarity in the laws regulating this form of technology.

---

[22] Chris Foresman, *Apple Tells Devs that Location-Based Advertising is a No-no*, Ars Technica, Feb. 5, 2010, http://arstechnica.com/apple/news/2010/02/apple-tells-devs-that-location-based-advertising-is-a-no-no.ars ; Kevin Anderson, *Apple Hints at Location-based Advertising and Services Strategy*, The Guardian Technology Blog, Feb. 5, 2010, http://www.guardian.co.uk/technology/blog/2010/feb/05/apple-iphone-advertising-location.
[23] David Sarno, *Apple Collecting, Sharing iPhone Users' Precise Locations*, L.A. Times, June 21, 2010, http://latimesblogs.latimes.com/technology/2010/06/apple-location-privacy-iphone-ipad.html.
[24] Apple, *Privacy Policy*, http://www.apple.com/legal/privacy/ (last visited June 22, 2010).
[25] Google, *Data Collected by Google Cars*, European Public Policy Blog, Apr. 27, 2010, http://googlepolicyeurope.blogspot.com/2010/04/data-collected-by-google-cars.html.
[26] Google, WiFi Data Collection: An Update, May 14, 2010, http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html.
[27] For a full discussion of the status of these ongoing investigations, see EPIC, *Investigations of Google Street View*, http://epic.org/privacy/streetview/.
[28] Letter from EPIC to FCC Chairman Julius Genachowski, May 18, 2010, *available at* http://epic.org/privacy/cloudcomputing/google/EPIC_StreetView_FCC_Letter_05_21_10.pdf.
[29] Letter from Edward Markey & Joe Barton to FTC Chairman Jon Leibowitz, May 19, 2010, *available at* http://epic.org/privacy/ftc/google/5_19_10_Markey_Barton_FTC_re_Google_WiFi.pdf.

### III. The European Commission has Provided an Effective Model for Regulating Locational Data

Concerns regarding locational privacy are arising in other countries, as well. The responses in Europe, in particular, provide the United States with a possible model to protect the privacy of locational data. With Directive 2002/58 on Privacy and Electronic Communications, also known as E-Privacy Directive, the European Commission has created effective regulation of locational data. The Directive addresses cellular location information.[30]

The Directive differentiates between location information needed to enable transmission and location information used for value-added services.[31] Location data other than traffic data is treated under Article 9, which requires that location data be processed anonymously or with consent of the individual.

Obtaining this consent requires informing the user of the type of data, the purpose of the collection, the duration of the collection and whether a third party will be doing the processing. Consent may be withdrawn at any time, and there must be a simple and free means for a user to refuse the processing of location data for a specific connection or transmission. The processing of data is restricted to what is necessary for providing the value-added service.[32] Further, Article 26 of the Universal Service Directive requires that Member states ensure that providers of public telephone networks make call location information available to emergency authorities.[33]

The Article 29 working party, an E.U. advisory group of experts on privacy and data protection, has issued an opinion further clarifying the rule regarding location information.[34] Consent means specific consent, not obtained as part of an agreement to more general terms.[35] Location data may not be stored beyond the delivery of the location-based service, unless kept for billing purposes, or anonymized.[36] In locating employees, the working group considers the collection excessive in situations where employees would be free to make their own travel arrangements or where the location monitoring is done for the sole purpose of monitoring employees and other means are available.[37] Location information should not be collected outside of working hours, and the working group recommends that location equipment which is also used for private purposes permit employees to turn off the location tracking.

---

[30] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.
[31] *Id.* at 35.
[32] *Id.* at Art. 9.
[33] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and user's rights to electronic communications networks and services (Universal Service Directive), *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_108/l_10820020424en00510077.pdf.
[34] Working Party 29 Opinion on the use of location data with a view to providing value-added services, 2130/05/EN, November 2005, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf.
[35] *Id.* at 5.
[36] *Id.* at 7.
[37] *Id.* at 11.

The Transatlantic Consumer Dialogue (TACD) has also passed a resolution on mobile commerce that addresses privacy concerns of consumers.[38] The resolution states that the E.U. and U.S. governments should: "Protect consumer privacy in mobile commerce and prohibit use of any personal data (including purchase and location information) for purposes that consumers have not explicitly agreed to or that unfairly disadvantage them." Industry group CTIA has released a "Best Practices and Guidelines for Location-based Services."[39] The guidelines "rely on two fundamental principles: user notice and consent."[40] Notice can be achieved by a disclosure in a privacy policy and consent may be implicit.[41] However, in situations such as child safety or business settings, the decision on the use of location-based services will be made by the account holder, rather than data subject.[42]

**IV. EPIC's Recommendations**

We specifically recommend that the Subcommittee consider the following objectives in the development of new safeguards to protect location data:

- Require that location not be collected or shared without affirmative user consent;
- Require that consent be fully informed consent: that users be informed of the type of data and the purpose of the collection;
- Require that consent be specific intent: consent which is not obtained as part of an agreement to more general terms;
- Require that companies provide users with a simple and free means to refuse the processing of location data for a specific connection or transmission;
- Require that location data not be stored beyond the delivery of the location-based service, unless kept for billing purposes, or anonymized.

**V. Conclusion**

EPIC respectfully requests that the Subcommittee takes the steps outlined in this statement, including investigating the ways in which companies gather locational data from their users; clarifying the Electronic Communications Privacy Act's treatment of how companies may gather and store users' data; adopting guidelines similar to those in the European Commission's Directive 2002/58, which would give users control over their locational data; adopting guidelines that mirror those in the TACD resolution, which require companies to obtain explicit consent from users in order to use location data; and ensuring the locational data privacy of U.S. consumers.

Thank you for your consideration of these views.

---

[38] Transatlantic Consumer Dialogue, Resolution on Mobile Commerce, August 2005, http://www.tacd.org/cgi-bin/db.cgi?page=view&config=admin/docs.cfg&id=283.
[39] CTIA - The Wireless Association, Best Practices and Guidelens for Location-based Services, April 2, 2008, http://www.ctia.org/business_resources/wic/index.cfm/AID/11300.
[40] *Id.*
[41] *Id.*
[42] *Id.*



○