ELECTRONIC COMMUNICATIONS PRIVACY ACT REFORM

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

MAY 5, 2010

Serial No. 111–98

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
56–271 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. SÁNCHEZ, 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

MAY 5, 2010

ELECTRONIC COMMUNICATIONS PRIVACY ACT REFORM

WEDNESDAY, MAY 5, 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 2:53 p.m., in room 2141, Rayburn House Office Building, the Honorable Jerrold Nadler (Chairman of the Subcommittee) presiding.

Present: Representatives Nadler, Watt, Scott, Johnson, Cohen, Chu, and Sensenbrenner.

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

Mr. NADLER. This hearing of the Subcommittee on the Constitution, Civil Rights, and Civil Liberties will come to order. We apologize for coming to order late, but the votes on the floor necessitated that. We will begin by recognizing myself for a 5-minute opening statement.

Today's hearing is the beginning of a process through which the Subcommittee will revisit the statutory framework Congress established in the 1986 Electronic Communication Privacy Act, ECPA, in spite of the enormous technological advances which have taken place in electronic communications over the last 24 years.

Because of the complexity of the subject, both legal and technological, this hearing will probably be the first of several we will hold as we consider what, if any, reforms should be made to the Act so that it might function more effectively in the future.

ECPA was passed in 1986, well before we commonly used the Internet for e-mail, much less for cloud computing and remote storage, at a time when cell phones were rare, often the size of small kitchen appliances, and included no tracking technologies capable of mapping our every movement. Communications technology now evolves at an exponential pace.

So in 1986 ECPA fixed the statutory standards law enforcement would have to meet to access private communications data in a technological environment as far removed from our own as that of 1986 was from the day Alexander Graham Bell said, "Mr. Watson, come here. I need you." in the first telephone call 110 years earlier.

The lightning pace of innovation in communications technology brings with it enormous improvements in the quality of life for our

citizens that in many ways marked the age we live in as a new epoch, which might be called the Internet Age. But it must be said, particularly by the Committee on the Judiciary, that these events also provide criminals with new platforms for unlawful activity.

Moreover, it must also be said here on the Subcommittee on the Constitution that these robust new communications technologies bring with them new opportunities for law enforcement agencies, charged to protect us from such criminals, to intervene in our private lives. Thus, we must consider whether ECPA still strikes the right balance between the interests and needs of law enforcement and privacy interests of the American people.

This is only the beginning of a dialogue that must go on to include the input of, among others, law enforcement at the Federal, state and local level, private industry stakeholders across the complex network of networks that is modern communications, and academic experts on technology, privacy and Fourth Amendment issues.

But today all of the Members of the Subcommittee can begin this inquiry through a dialogue that raises these issues with this distinguished panel of witnesses. Today we can begin the work of making ECPA work for our time and for all concerned. This is an enormous responsibility, and this Subcommittee needs everyone's help to get it right. As such, all of us sit on this panel at least in part as students today.

I thank you in advance for what you will teach us.

As for myself, some of the questions I propose to the class are how have changes in the Internet made it difficult for private industry to determine its obligations under Title II of ECPA, the Stored Communications Act? How do current advances in location technology test traditional standards of the ECPA of 1986?

More generally, in what ways have these and other technologies potentially subverted one of the original and central goals of ECPA, which was to preserve "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement?" If we are out of balance, what concepts should guide reform? I know my distinguished colleagues will have other questions.

Finally, I would like to observe that we are aware that privacy advocates and members of industry have worked together in an impressive common effort to derive and propose some common principles that should guide our inquiry on ECPA reform. I look forward to hearing them articulated by our witnesses here in person.

It is my hope that we on this Subcommittee can emulate your example and come together in a bipartisan spirit as we forge ECPA reform legislation that will put needed reforms in place, hopefully this year. I welcome our witnesses, and I look forward to your testimony.

With that, I yield back. And I will now recognize for an opening statement the distinguished Ranking Member of the Subcommittee.

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

The purpose of today's hearing is to examine the need to update the Electronic Communications Privacy Act of 1986. Today's hearing is a result of calls by a coalition called the Digital Due Process to examine how far apart technology and the law may have become

and to see if reforms are necessary to keep the law current with constantly evolving technology.

The genesis of ECPA in 1986 was a needed response to the emergence and rapid development of wireless communications services and electronic communications of the digital era. At that time e-mail, cordless phones and pagers were by today's standards in their infancy, and as these devices have become smaller, cheaper and more sophisticated, we have embraced them more and more in our everyday lives.

The evolution of the digital age has given us devices and capabilities that have created conveniences for society and efficiencies for commerce. But they have also created conveniences and efficiency for criminals, as well as innovative new ways to commit crimes. Fortunately, new ways to detect and investigate crimes and criminals have also evolved.

At the intersection of all these developments and capabilities are the privacy rights of the public, the economic interest in expanding commerce, the public policy of encouraging development of even better technologies, and the legitimate investigative needs of law enforcement professionals.

While some of the issues we will hear about today have been heard before, this new initiative by the Digital Due Process coalition was officially launched on March 30th this year. There has been neither sufficient time to examine the concepts that are being advanced in any meaningful way, nor has there been time to hear from other stakeholders, including relevant members of the law enforcement community.

While the Digital Due Process coalition makes note that some of the principles have been previously embraced by the House Judiciary Committee in 2000, it should be noted that just last year the full Committee voted down advancing the requirements for obtaining authority to utilize the pen register and for obtaining authority to utilize the trap and trace device.

In fact, enhancing the standard for a pen register and trap and trace device drew strong opposition from the National District Attorneys Association, the National Sheriffs Association, the Fraternal Order of Police, and the International Association of Chiefs of Police, all of whom agree that the proposed changes to criminal pen register and trap and trace devices would unduly burden state and local law enforcement agencies, who regularly use these tools in state criminal investigations.

There will no doubt be considerable debate on what may or may not need to be changed, but there will also be debate on how any needed change should be effected. I look forward to the witnesses today, and I look forward to having you start the debate. Let me say it won't be the end of the debate.

Mr. NADLER. In the interests of getting to our witnesses and mindful of our busy schedules, I ask that other Members submit their statements for the record. Without objection, all Members will have 5 legislative days to submit opening statements for inclusion in the record. Without objection, the Chair will be authorized to declare a recess of the hearing.

We will now turn to our first panel of witnesses—in fact, our only panel of witnesses.

Jim Dempsey is vice president for public policy at the Center for Democracy and Technology, where he concentrates on privacy and government surveillance issues. Mr. Dempsey coordinates the Digital Privacy and Security Working Group, a forum for companies, trade associations, think tanks and public interest advocates interested in cyber security, government surveillance and related issues. He received his J.D. from Harvard Law School. Additionally, Mr. Dempsey was counsel to this Subcommittee under Chairman Don Edwards. He continues to carry on that work at CDT, and I am pleased to welcome him back.

Albert Gidari is a partner at Perkins Coie—or Perkins Coie, I think, LLP, where he represents a broad range of companies on privacy, security, Internet, electronic surveillance and communications law. His practice also includes both civil and criminal litigation, investigations and regulatory compliance counseling. He is a graduate of the George Mason University School of Law.

Orin Kerr is a law professor at George Washington University, who has written extensively on the Electronic Communications Privacy Act. From 1998 to 2001, Mr. Kerr was a trial attorney at the computer crime and intellectual property section of the U.S. Department of Justice. He earned his JD magna cum laude from Harvard Law School.

Annmarie Levins is an associate general counsel at Microsoft Corporation. She manages the legal support for Microsoft's U.S. and Canadian subsidiaries, directing the legal teams responsible for licensing and service transactions, anti-piracy investigations and enforcement, Internet safety work and other areas. Ms. Levins formerly served in the U.S. Attorney's Office in Seattle and in the Southern District of New York. She graduated summa cum laude from the University of Maine School of Law.

I am pleased to welcome all of you. Your written statements in their entirety will be made part of the record. I would ask each of you to summarize your testimony in 5 minutes or less. There is a light in front of you. When it turns yellow, that means you have a minute left. And I would advise you that the Chair is somewhat lax in—or latitude in that area maybe in interpreting the time limit.

Before we begin, it is customary for the Committee to swear in its witnesses.

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

You may be seated.

And we will first—I now recognize Mr. Dempsey for 5 minutes.

TESTIMONY OF JAMES X. DEMPSEY, CENTER FOR DEMOCRACY AND TECHNOLOGY, VICE PRESIDENT FOR PUBLIC POLICY

Mr. DEMPSEY. Chairman Nadler, Members of the Subcommittee, good afternoon. Thank you for holding this hearing.

In setting rules for electronic surveillance, the courts and Congress have long sought to balance three critical interests—the individual's right to privacy, the government's need to obtain evidence to prevent and investigate crimes and respond to emergencies, and the corporate interest in clear rules that provide confidence to con-

sumers and that afford the companies the certainty they need to invest in the development of innovative new services.

Today it is clear that the balance among those three interests has been lost. Powerful new technologies create and store more and more information about our daily lives. The protections provided by judicial precedent and statute have failed to keep pace.

The major Federal statute setting standards for governmental access to communications, the Electronic Communications Privacy Act, or ECPA, was written in 1986, light years ago in Internet time. Among other key points, private information directly analogous to a telephone call or letter now falls outside of the traditional warrant standard when stored online. As a result, a major section of ECPA is probably unconstitutional in many applications.

Every witness at this table today agrees that ECPA is outdated and needs to be reformed to provide strong privacy protections while also preserving the tools that law enforcement agencies need to act quickly to investigate crimes and respond to emergencies.

For the past several years the Center for Democracy and Technology, my organization, has been chairing a dialogue among leading Internet companies, communications companies, privacy advocates, law professors and attorneys in private practice to discuss how ECPA was working and how it needed to be updated. We had as part of our group several former prosecutors and several alumni of the Computer Crime and Intellectual Property Section of the Department of Justice.

In our discussions we were acutely aware of the needs of law enforcement. We started with a list of over a dozen issues. Some of the privacy advocates and scholars wanted to go farther in strengthening the rules, but the former prosecutors emphasized the importance of preserving a sliding scale of authorities. We met monthly and then even weekly.

Ultimately, we reached consensus on four principles—consistent application of the warrant standard to private communications and documents, consistent application of the warrant standard for location tracking of cell phones and other mobile devices, true judicial review of pen registers and trap and trace devices—and we can go into more detail about what pen register/trap and trace devices are and how they work—and no blanket use of subpoenas.

Now, in some ways—many ways, actually—these proposals are modest. The proposals would preserve all current exceptions, including the emergency exception that permits disclosure of e-mail and other content without a warrant, even without a subpoena, in times of emergency. We do not propose any changes to FISA or to the national security letter provision in ECPA.

Our proposals on e-mail and stored documents focus solely on compelled production from a service provider providing service to third parties. We do not propose any change to the rules governing how you get information directly from the subject of an investigation. A company could not hide behind ECPA if the government is investigating that company. The rules permitting subpoenas served directly on targets of an investigation will remain unchanged.

As Chairman Nadler indicated, the companies and organizations endorsing this principle call themselves the Digital Due Process coalition. The coalition now includes major Internet and communica-

tions companies, major think tanks, and advocacy organizations ranging from the ACLU to Americans for Tax Reform and FreedomWorks. We are continuing to add new members each week.

We see our principles as the first step—and I emphasize this—just an opening framework in a process that will require public discussion, the engagement of other stakeholders, and most importantly, dialogue with law enforcement agencies. We have already begun the process of discussing these principles with the Department of Justice, the FBI, and the National Association of Attorneys General.

We intend to get very specific in follow-up discussions, addressing concrete hypotheticals about how updates to the law would affect ongoing practices.

Mr. Chairman, the coalition is not urging the introduction of legislation. Many details remain to be discussed before we get to the legislative phase. Other issues might be brought forward in addition to the four that we have put on the table. We urge this Committee and we are urging the Senate Judiciary Committee to move cautiously, to hold further hearings, as you already indicated you would, to listen to the views of law enforcement, of the telephone companies and other carriers.

Professor Kerr in his testimony has proposed some excellent questions that need to be and can be addressed and resolved. Some of them, speaking for CDT, I have answers to. Others of them I don't have answers to yet. But we agree they need to be addressed. Our coalition foresees a long-term process of hearings, dialogue and consensus building. Together, though, we can re-establish the balance among those interests that were critical in 1986—law enforcement, privacy and business.

I look forward to your questions, Mr. Chairman and Members of the Subcommittee. Thank you.

[The prepared statement of Mr. Dempsey follows:]

PREPARED STATEMENT OF JAMES X. DEMPSEY

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE
www.cdt.org

CENTER FOR DEMOCRACY & TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Statement of James X. Dempsey
Vice President for Public Policy
Center for Democracy & Technology

before the House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights, and Civil Liberties

ELECTRONIC COMMUNICATIONS PRIVACY ACT REFORM

May 5, 2010

Chairman Nadler, Ranking Member Sensenbrenner, Members of the Subcommittee, thank you for the opportunity to testify today.

Introduction and Overview

Justice Brandeis famously called privacy "the most comprehensive of rights, and the right most valued by a free people." The Fourth Amendment embodies this right, requiring a judicial warrant for most searches or seizures,[1] and Congress has enacted numerous laws affording privacy protections going beyond those mandated by the Constitution.

In setting rules for electronic surveillance, the courts and Congress have sought to balance two critical interests: the individual's right to privacy and the government's need to obtain evidence to prevent and investigate crimes, respond to emergency circumstances and protect the public. More recently, as technological developments have opened vast new opportunities for communication and commerce, Congress has added a third goal: providing a sound trust framework for communications technology and affording companies the clarity and certainty they need to invest in the development of innovative new services.

Today, it is clear that the balance among these three interests – the individual's right to privacy, the government's need for tools to conduct investigations, and the interest of service providers in clarity and customer trust – has been lost as powerful new technologies create and store more and more information about our daily lives. The protections provided by judicial precedent and statute have failed to keep pace, and important information is falling outside the traditional warrant standard.

---

[1] "Warrantless searches are presumptively unreasonable, though the Court has recognized a few limited exceptions to this general rule." United States v. Karo, 468 U.S. 705, 717 (1984).

Two major developments in technology in the past ten years stand out:

- "cloud computing," the use of Internet-based resources for the storage and processing of all kinds of information - more and more private information is moving off the desktop or laptop computer and out of our homes and offices onto the remote computers of service providers; and
- the wireless revolution, in which nearly 300 million Americans rely in their business and personal lives on cell phones and other mobile devices, which generate information locating the individual every few seconds.

Under the Electronic Communications Privacy Act of 1986, neither of these technologies is accorded the traditional protection of the judicial warrant. According to ECPA, private documents stored in the cloud, including all our email more than 180 days old, are available to government investigators without a warrant. Likewise, ECPA does not specify that a warrant is required for the government to track our location through our cell phones. The courts, as they often have been in the past, are being slow in responding to these technological changes.

The personal and economic benefits of technological development should not come at the price of privacy. In the absence of judicial protections, it is time for Congress to respond, as it has in the past, to afford adequate privacy protections, while preserving law enforcement tools and providing clarity to service providers.

A Brief History of Electronic Surveillance Law

The history of privacy in America is characterized by the recurring efforts of courts and Congress to catch up with technology.

In 1928, in *Olmstead v. United States*, 277 U.S. 438, the Supreme Court held that a telephone wiretap was not a search or seizure requiring a warrant under the Fourth Amendment. In 1877, the Court had held in *Ex parte Jackson*, 96 U.S. 727, that the Fourth Amendment applied to sealed letters: even though the letter was turned over to the Post Office for delivery, it could not be opened without a warrant. The *Olmstead* Court, however, focused on the fact that wiretapping was done at a remote point from the home, without a physical invasion, and therefore it failed to see how a telephone conversation was similar to a letter. The Court concluded, in essence, that users of the telephone voluntarily surrendered the privacy of their communications: "The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment." 277 U.S. at 466.

Justice Brandeis, in his famous dissent, said that the majority opinion was inconsistent both with the development of technology and with the Court's earlier ruling on the privacy of letters. Quoting the lower court, Brandeis said, "There is, in essence, no difference between the sealed letter and the private telephone message. ... 'True, the one is visible, the other invisible; the one is tangible, the other intangible; the one is sealed, and the other unsealed; but these are distinctions without a difference.'" *Id.* at 475. Brandeis warned that technology would continue to change in ways that would erode privacy if the law remained static: "The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from

secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." Id. at 474.

It took 40 years for a Court majority to acknowledge Justice Brandeis' call for technology neutrality in the application of the Fourth Amendment. Finally, in *Katz v. United States*, 389 U.S. 347 (1967), Justice Stewart wrote that the "Fourth Amendment protects people, not places. ... [What a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." The Court based its decision in part on the fact that the telephone had come to play a central role in everyday life. *Id.* at 352 ("To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.").

To implement the Constitutional ruling of *Katz* and the related case on bugging, *Berger v. New York*, 388 U.S. 41 (1967), Congress in 1968 adopted the federal Wiretap Act, 18 U.S.C. 2510 *et seq.*, establishing detailed procedural rules for obtaining judicial warrants to carry out wiretaps. Congress, however, forgetting Justice Brandeis' prediction about the steady progress of technology, only covered voice communications carried over a wire and face-to-face oral conversations.

After *Katz*, the pace of technological change accelerated dramatically. By the 1980s, two forms of communications were emerging that did not fit well within the definitions of the Wiretap Act; wireless telecommunications were emerging in the form of early cellular phones, and the modem was making it possible to transmit non-voice data over the telephone system. The rationale of *Katz* would seem to suggest that wireless and data communications were just as much protected by the Fourth Amendment as wireline, voice calls. However, there were arguments, harking back to *Olmstead*, that cell phone users surrendered their privacy when they voluntarily used a service that went over the air. Similarly, decisions of the Supreme Court holding that there was no privacy right in some kinds of records stored with a third party cast a shadow of doubt over the status of Internet communications, which were stored on network computers as they hopped from node to node and before they were accessed by their intended recipients.

Congress concluded that it would be unwise to wait for cases resolving the status of these emerging technologies to percolate up through the courts. After all, it took decades for the Supreme Court to extend the Fourth Amendment to the telephone. The fledgling wireless and Internet industries wanted to be able to assure potential customers that their communications were private. Key policymakers foresaw the potential of these technologies, in terms of both economic development and human interaction. Another *Olmstead* would have been devastating to privacy and innovation. To remove the cloud of doubt about privacy, and in order to provide a sound footing for investment and innovation, Congress adopted the Electronic Communications Privacy Act of 1986.

The stated goal of ECPA was twofold: to preserve "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement," House Committee on the Judiciary, Electronic Communications Privacy Act of 1986, H. Rep. No. 99-647, 99th Cong. 2d Sess. 2, at 19 (1986), and to support the development and use of these new technologies and services, *see* S. Rep. No. 99-541, at 5 (noting that legal uncertainty over the privacy status of new forms of communications "may unnecessarily discourage potential customers from using innovative communications systems"). It was the intent of Congress to encourage the proliferation of new communications technologies, but it recognized that consumers would not

trust new technologies if the privacy of those using them was not protected. *Id.*; H.R. Rep. No. 99-647, at 19 (1986).

ECPA updated the Wiretap Act by specifying that a judicial warrant was required for the "interception" of wireless communications and data communications – that is, the monitoring of cellular calls and email in real-time, as they were being transmitted. ECPA also specified that the government needed a warrant to compel a service provider to disclose the content of email it was holding in electronic storage – but only up to a point. In 1986, Congress assumed that users would access their email accounts periodically and download their email onto their local computers. The service providers would then delete the email from their servers. Congress thought that the longest conceivable time that any service provider would keep email would be 6 months. So Congress provided that a warrant was required only for access to email 180 days old or less. After 180 days, the account was assumed to be abandoned and the service provider could be compelled with a mere subpoena to turn over anything it still had.

ECPA also set standards for use of pen registers and trap trace devices to intercept dialed number information. The Supreme Court had ruled that telephone users had no privacy interest in the dialing information associated with their phone calls. Congress reacted by requiring a court order for live interception of dialing information, but it set a very low standard, specifying that the courts "shall" approve all government requests certifying that the information likely to be obtained is relevant to an ongoing investigation. ECPA also authorized use of subpoenas to compel disclosure of subscriber identifying information and stored transactional records.

Changes in Technology Have Outpaced ECPA

While ECPA was a forward-looking statute when enacted in 1986, technology has advanced dramatically since 1986, and the statute has been outpaced. ECPA has not undergone a significant revision since it was enacted in 1986 – light years ago in Internet time. ECPA today is a patchwork of confusing standards that have been interpreted inconsistently by the courts, creating uncertainty for many service providers and law enforcement agencies alike. Moreover, it provides inadequate protection for huge amounts of personal information.

Since enactment of ECPA, there have been fundamental changes in communications technology and the way people use it, including –

- **Email**: Most Americans have embraced email in their professional and personal lives and use it daily for confidential communications of a personal or business nature. Because of the importance of email and unlimited storage capabilities available today, most people save their email indefinitely, just as they previously saved letters and other correspondence. The difference, of course, is that it is easier to save, search and retrieve digital communications. Many of us now have many years worth of stored email. Moreover, for many people, much of that email is stored on the computers of service providers.[2] **However, ECPA provides only weak protection for stored email that is more than 180 days old, allowing governmental access without a warrant.**

[2] For example, Google's Gmail service offers more than seven gigabytes of free storage space. Google, *Google Storage*, *available at* http://mail.google.com/support/bin/answer.py?hl=en&answer=39567 (visited Mar. 30, 2010). Google also encourages its users not to throw messages away. Google, *Getting Started with Gmail*, *available at* http://mail.google.com/mail/help/intl/en/start.html (visited Mar. 30, 2010) ("Don't waste time deleting . . . . [T]he typical user can go years without deleting a single message.").

Moreover, the Justice Department argues that email loses the protection of the warrant the instant the user sends it or opens it.

- **Mobile location:** Cell phones and mobile Internet devices constantly generate location data that supports both the underlying service and a growing range of location-based services of great convenience and value. This location data can be intercepted in realtime, and is often stored in easily accessible logs files. Location data can reveal a person's movements, from which inferences can be drawn about activities and associations. Location data is augmented by very precise GPS data being included in a growing number of devices. **ECPA does not clearly specify a standard for government access to location information, and agents have been obtaining it without a warrant.** See Michael Isikoff, The Snitch in Your Pocket, Newsweek (Feb. 19, 2010) http://www.newsweek.com/id/182403.

- **Cloud computing**: Increasingly, businesses and individuals are storing data "in the cloud," with potentially huge benefits in terms of cost, security, flexibility and the ability to share and collaborate. **ECPA needs to clarify that data stored and processed in the cloud has the same protections and standards for law enforcement access as data stored locally.**

- **Social networking**: One of the most striking developments of the past few years has been the remarkable growth of social networking. Hundreds of millions of people now use these social media services to share information with friends and as an alternative platform for private communications. **Even when private records, photos and other materials are shared only with a couple of friends, ECPA may provide only weak protection, allowing governmental access without a warrant.**

- **Tracking and logging of online activity:** For a variety of reasons, Internet service providers, websites and other online service providers collect and log detailed information about online activity. While many Internet users have a perception of anonymity, in fact much of what they do online can be personally tied to them through their computer addresses and other information disclosed and logged in the ordinary course of using the Internet. ECPA authorizes a subpoena to acquire certain types of subscriber identifying information. **However, government agencies have been filing blanket subpoenas seeking to identify all individuals who visited a particular site containing lawful content or all users of a legitimate online service.**

In the face of these developments, ECPA does not provide protection suited to the way technology is used today:

- **Conflicting standards and illogical distinctions:** ECPA sets rules for governmental access to email and stored documents that are not consistent. A single email is subject to multiple different legal standards in its lifecycle. See Appendix A. To take another example, a private document stored on a desktop computer is protected by the warrant requirement of the Fourth Amendment, but DOJ argues under ECPA that the same document stored with a service provider is not be subject to the warrant requirement.

- **Unclear standards:** ECPA does not clearly state the standard for governmental access to location information. In the past 5 years, no fewer than 30 federal opinions have been published on government access to cell phone location information, reaching a variety of conclusions.

- **Judicial criticism:** The courts have repeatedly criticized ECPA for being confusing and difficult to apply. The Ninth Circuit in 2002 said that Internet surveillance was "a confusing and uncertain area of the law."
- **Constitutional uncertainty:** The courts are equally conflicted about the application of the Fourth Amendment to new services and information. A district court in Oregon recently opined that email is not covered by the constitutional protections, while the Ninth Circuit has held precisely the opposite. Last year, a panel of the Sixth Circuit first ruled that email was protected by the Constitution and then a larger panel of the court vacated the opinion on procedural grounds, leaving the issue up in the air.

This murky legal landscape does not serve the government, customers or service providers well. Customers are, at best, confused about whether their data is subject to adequate protections when the government seeks access. Companies are uncertain of their responsibilities and unable to assure their customers that subscriber data will be uniformly protected. The current state of the law does not well serve law enforcement interests either, as resources are wasted on litigation over applicable standards and prosecutions are in jeopardy should the courts ultimately rule on the Constitutional questions. The solution is a clear set of rules for law enforcement access that will safeguard end-user privacy, provide clarity for service providers, and enable law enforcement officials to conduct effective and efficient investigations.

The Digital Due Process Coalition

For nearly three years, privacy advocates, legal scholars, and major Internet and communications service providers have been engaged in a dialogue to explore how ECPA applies to new services and technologies. The Center for Democracy & Technology chaired those discussions. Earlier this year, those discussions reached a milestone when a diverse coalition developed consensus around a core set of principles for updating ECPA. The principles are open for signature and new entities are continuing to endorse it. The coalition so far includes AOL, AT&T, CCIA, eBay, Google, Intel, Microsoft, NetCoalition, and Salesforce.com, as well as the ACLU, the Electronic Frontier Foundation, FreedomWorks, Americans for Tax Reform, and the Competitive Enterprise Institute. See Appendix B for a full list of Coalition members.

The coalition did not seek to answer all questions or concerns about ECPA. Though members of the coalition may differ on the specifics, and some individual members would support additional changes, all agreed on four principles that provide a framework for opening a public dialogue on the issue. This is what the coalition reached consensus on:

> ***Updating The Electronic Communications Privacy Act of 1986***
>
> ***Overarching goal and guiding principle:*** *To simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public.*
>
> *These principles would not change, and are subject to, the current definitions, exceptions, immunities and permissions in ECPA:*

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

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

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

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

In this written testimony and in my oral remarks, I speak only on behalf of CDT. I do not speak for the coalition or any of its other members. However, I draw extensively on a background memo prepared by the coalition. The full consensus text of the DDP memo is online at http:/www.digitaldueprocess.org. In addition, the site includes a lengthy analysis by J. Beckwith Burr of WilmerHale.

The overarching goal of ECPA reform should be to balance the law enforcement interests of the government, the privacy interests of users, and the interests of communications service providers in certainty, efficiency and public confidence. In addition, the following concepts should guide any reform:

- **Technology and Platform Neutrality**: A particular kind of information (for example, the content of private communications) should receive the same level of protection regardless of the technology, platform or business model used to create, communicate or store it.

- **Assurance of Law Enforcement Access**: The reform principles would preserve all of the building blocks of criminal investigations – subpoenas, court orders, pen register orders, trap and trace orders, and warrants – as well as the sliding scale that allows the government to escalate its investigative efforts.

- **Equality Between Transit and Storage**: Generally, a particular category of information should be afforded the same level of protection whether it is in transit or in storage.

- **Consistency**: The content of communications should be protected by a court order based on probable cause, regardless of how old the communication is and whether it has been "opened" or not.
- **Simplicity and Clarity**: All stakeholders – service providers, users and government investigators – deserve clear and simple rules.
- **Recognition of All Existing Exceptions**: Over the years, a variety of exceptions have been written into the ECPA, such as provisions allowing disclosures to the government without court orders in emergency cases. These principles should leave all those exceptions in place.

Rather than attempt a full rewrite of ECPA, which might have unintended consequences, it is best to focus just on the most important issues – those that are arising daily under the current law: access to email and other private communications stored in the cloud, access to location information, and the use of subpoenas to obtain transactional data.

What Would ECPA Reform Mean in Practice

Stored Communications and Private Documents: The first principle endorsed by the DDP coalition is that the government should obtain a search warrant based on probable cause before it can compel a service provider to disclose a user's private communications or documents stored online.

- This principle applies to private communications, documents and other private user content stored in or transmitted through the Internet "cloud" the same warrant standard that the Constitution and the Wiretap Act have traditionally provided for the privacy of our phone calls or the physical files we store in our homes. It is intended to apply to private emails, instant messages, text messages, word processing documents and spreadsheets, photos, Internet search queries and private posts made over social networks. It is not intended to apply to materials revealed to the public on the Internet.
- This change was first proposed in bi-partisan legislation introduced in 1998 by Senators John Ashcroft and Patrick Leahy. It is consistent with recent Appeals Court decisions holding that emails and SMS text messages stored by communications providers are protected by the Fourth Amendment, and is also consistent with the latest legal scholarship on the issue.

Location Tracking: The second DDP reform principle states that the government should obtain a search warrant based on probable cause before it can track, prospectively or retrospectively, the location of a cell phone or other mobile communications device.

- This principle addresses the treatment of the growing quantity and quality of data based on the location of cell phones, laptops and other mobile devices, which is currently the subject of conflicting court decisions; it proposes the conclusion reached by a majority of the courts that a search warrant is required for real-time cell phone tracking, and would apply the same standard to access to stored location data.
- Many details of this principle would have to be worked through, including the definition of location information, the exceptions that would be recognized (which would certainly have to include emergency circumstances), and the relationship between requests for

location information and requests for other call detail records and subscriber identifying information.

- A warrant for mobile location information was first proposed in 1998 as part of the bipartisan Ashcroft-Leahy bill. The House Judiciary Committee in 2000 reported by a 20-1 vote legislation that would have required a warrant for real-time tracking of mobile phones. See Appendix C for a comparison between the DDP principles and the 2000 House Judiciary Committee vote.

Access to Transactional Data: Under the DDP's third principle, before obtaining transactional data in real time about when and with whom an individual communicates using email, instant messaging, text messaging, the telephone or any other communications technology, the government should demonstrate to a court that such data is relevant to an authorized criminal investigation.

- In 2001, the law governing "pen registers and trap & trace devices"—technologies used to obtain transactional data in real time about when and with whom individuals communicate over the phone—was expanded to also allow monitoring of communications made over the Internet. In particular, the data at issue includes information on who individuals email with, who individuals IM with, who individuals send text messages to, and the Internet Protocol addresses of the Internet sites individuals visit.

- This principle would update the law to reflect modern technology by establishing judicial review of surveillance requests for this data based on a factual showing of reasonable grounds to believe that the information sought is relevant and material to a crime being investigated.

Overbroad Subpoenas: Finally, before obtaining transactional data about multiple unidentified users of communications or other online services when trying to track down a suspect, the government should first demonstrate to a court that the data is needed for its criminal investigation.

- This principle addresses the circumstance when the government uses subpoenas to get information in bulk about broad categories of telephone or Internet users, rather than seeking the records of specific individuals that are relevant to an investigation. For example, there have been reported cases of bulk requests for information about everyone that visited a particular web site on a particular day, or everyone that used the Internet to sell products in a particular jurisdiction.

- Because such bulk requests for information on classes of unidentified individuals implicate unique privacy interests, this principle applies a standard requiring a showing to the court that the bulk data is relevant to an investigation.

What the Digital Due Process Principles Would Not Do

In the view of CDT, the recommendations endorsed by the Digital Due Process coalition are quite modest and would have minimal adverse impact on law enforcement investigations while providing important privacy protections.

- They would not affect FISA or the National Security Letter authority of ECPA (18 U.S.C. 2709).
- They would not affect emergency disclosures. The Wiretap Act, the Stored Communications Act, and the pen register/trap and trace provisions all contain emergency exceptions that permit interceptions and service provider disclosure without a warrant (and even without a subpoena). The principles offered by the DDP would not affect any of these emergency disclosures. The warrant requirement for access to location information recommended by DDP would have to be subject to similar emergency exceptions. Calls to 911 would also be exempted from the warrant requirement, under both the consent principle and the emergency exception.
- The principles would not affect cybersecurity. Service providers currently have broad authority to monitor their own networks for cybersecurity purposes and to disclose to the government information about suspected attacks or intrusions. The DDP recommendations would not alter these authorities.
- They would have zero impact on child pornography, child abuse and child safety investigations. The principles were carefully crafted to preserve fully the tools critical to these investigations. They do not alter in any way the child pornography reporting provisions in federal and state law. They do not alter the exceptions or other permissions granted in the statute for providing information to the government in child abduction cases. They do not alter any authority that service providers have to monitor their systems for child abuse images and to disclose such images to NCMEC or law enforcement.
- The recommendations would not cover anything publicly disclosed on the Internet. Moreover, they would not stop a police officer from "friending" someone on Facebook and obtaining access to otherwise private communications. The rules permitting undercover operations and other deceptive techniques would remain unaffected.
- The recommendations, like ECPA itself, focus on compulsory access from service providers. The recommendations would not change the rules for voluntary disclosure by the customers of those service providers. Nor do the recommendations change the rules for use of subpoenas served on the sender or recipient of an email or the creator of a document. The rule applicable to postal mail would also apply to email: the recipient of an email, like the recipient of a letter, could voluntarily disclose that email to the government and could be compelled to disclose it with a subpoena. The sender of an email could be compelled to disclose it with a mere subpoena to the same extent that the sender of a letter can be compelled to disclose a retained copy. If the creator of a document could be compelled with a subpoena to disclose it, under the DDP principles the creator could be compelled to disclose whether the document was stored locally or in the cloud.
- The recommendations preserve the "building blocks" of criminal investigations. Under current law, government investigators often work their way up the ladder to probable cause, starting with subpoenas for subscriber identifying information and stored transactional data, then moving to court orders under 2703(d) for more detailed transactional data and court orders, based on less than probable cause, for real-time interception of signaling and routing information. Based on analysis of this and other

data, they may then have probable cause to obtain a search warrant. The DDP recommendations preserve all these building blocks of the investigative process.

Disclosure to a Third Party Does Not Destroy a Privacy Interest

The ECPA reform proposals here are consistent with the long line of cases holding that individuals have privacy rights in materials that they entrust to third parties and in spaces rented from third parties. As noted above, the Supreme Court has recognized a Constitutional expectation of privacy in the contents of sealed packages and letters, even when those letters and packages are voluntarily given to the government-run Post Office. *Ex Parte Jackson*, 96 U.S. 727, 733 (1877). Bank customers have a privacy interest in the contents of their safe deposit boxes, requiring a warrant for government access. *United States v. Thomas*, No. 88-6341, 1989 WL 72926, at *2 (6th Cir. July 5, 1989). Moreover, this privacy right survives even if the service provider has rights to enter the protected space or inspect the material. Tenants in rented residences and hotel rooms maintain Fourth Amendment privacy rights in their units. *Stoner v. California*, 376 U.S. 483, 489 (1964). The fact that landlords and hotel managers may be entitled to enter the premises for maintenance and other purposes does nothing to diminish the tenants' expectations against the government. *Id.*

The Wiretap Act recognizes the same principle. It permits service providers to conduct service quality monitoring and to examine and disclose customer communications for the purpose of protecting the rights and property of the service provider. None of these actions diminish the privacy right of the telephone customer as against governmental intrusion, nor should the activities of providers of free Internet email and free cloud computing services diminish the privacy rights of users as against others.

Other ECPA Issues May Deserve Attention

There are other issues that may merit attention in addition to those covered by the consensus principles of the Digital Due Process coalition.

- Civil litigant access. Several court decisions have made it clear that ECPA does not allow civil litigants to compel the disclosure of communications by electronic communications service providers or providers of remote computing service to the public; under these rulings, such requests should be served on the sender or recipient of the communications who can be compelled under normal discovery rules to either retrieve them and disclose them to the litigant or to give consent to the service provider to disclose them. While these cases are a correct reading of ECPA, and while they offer a clear path to discovery in most cases, service providers continue to spend considerable resources defending against civil litigant requests, briefing the issue one court at a time. Some have argued that ECPA could be clarified, while perhaps including a safety valve process for cases in which the user whose communications are sought cannot be found.
- Reporting and transparency. The Wiretap Act requires annual publication of statistics on wiretapping, but there is no comparable requirement for pen register and trap and trace devices or for compulsory disclosure of stored content.
- The Wiretap Act only covers interception of communications. It does not cover the use of video cameras in private places. The recent case in Marion County, PA, in which a

school turned on the cameras in computers issued to students and took pictures of the students engaging in a variety of activities inside their homes, highlighted this gap in the law. See Testimony of Kevin Bankston before the Senate Judiciary Committee, Subcommittee on Crime and Drugs (March 29, 2010) http://www.eff.org/files/bankston_video_surveillance_testimony.pdf.

Conclusion

In just the past 5 to 10 years, entrepreneurs have developed and the American public has embraced truly revolutionary changes in communications and information technology. These changes have yielded remarkable benefits in terms of economic activity, education, democratic participation and support for friendships and family relationships. Further amazing developments are surely on the way. Our economic recovery depends in large part on innovation in information and communications technologies.

These benefits should not come at the price of privacy. Nor should privacy concerns be allowed to discourage further innovation. As it has in the past, Congress should update the privacy laws to preserve the balance between government power and personal privacy, preserving law enforcement tools and giving companies the clarity they deserve. Congress should extend the traditional warrant standard to our personal communications, private documents and highly sensitive information like mobile tracking data. Other less sensitive data should be available with a subpoena, so long as the government cannot make blanket requests without judicial approval. These changes would provide the framework for further innovation and growth.

Appendix A

One Email - Multiple Different Standards

ECPA, as interpreted by the Justice Department and the courts, provides a patchwork quilt of standards for governmental access to email. Under ECPA today, the status of a single email changes dramatically depending on where it is stored, how old it is, and even the district within which the government issues or serves its process.

Standards for access to the content of an email:

- Draft email stored on desktop computer – As an email is being drafted on a person's computer, that email is fully protected by the Fourth Amendment: the government must obtain a search warrant from a judge in order to seize the computer and the email.
- Draft email stored on gMail – However, if the person drafting the email uses a "cloud" service such as Google's gMail, and stores a copy of the draft email with Google, intending to finish it and send it later, ECPA says that Google can be compelled to disclose the email with a mere subpoena. 18 U.S.C. 2703(b).
- Content of email in transit – After the person writing the email hits "send," the email is again protected by the full warrant standard as it passes over the Internet. Most scholars and practitioners assume that the Fourth Amendment applies, but in any case the Wiretap Act requires a warrant to intercept an email in transit.
- Content of email in storage with service provider 180 days or less – Once the email reaches the inbox of the intended recipient, it falls out of the Wiretap Act and into the portion of ECPA known as the Stored Communications Act, 18 U.S.C. 2703(a). At least so long as the email is unopened, the service provider can be forced to disclose it to the government only with a warrant.
- Content of opened email in storage with service provider 180 days or less – The Justice Department argues that an email, once opened by the intended recipient, immediately loses the warrant protection and can be obtained from the service provider with a mere subpoena. (Under the same theory, the sender of an email immediately loses the warrant protection for all sent email.) The Ninth Circuit has rejected this argument. The question remains unsettled in the rest of the country. The Justice Department recently sought opened email in Colorado without a warrant; when the service provider resisted, the government withdrew its request, which means in effect that outside of the Ninth Circuit there is one standard for service providers who comply with subpoenas and one for service providers who insist on a warrant.
- Content of email in storage with service provider more than 180 days – ECPA specifies that all email after 180 days loses the warrant protection and is available with a mere subpoena, issued without judicial approval.

Appendix B

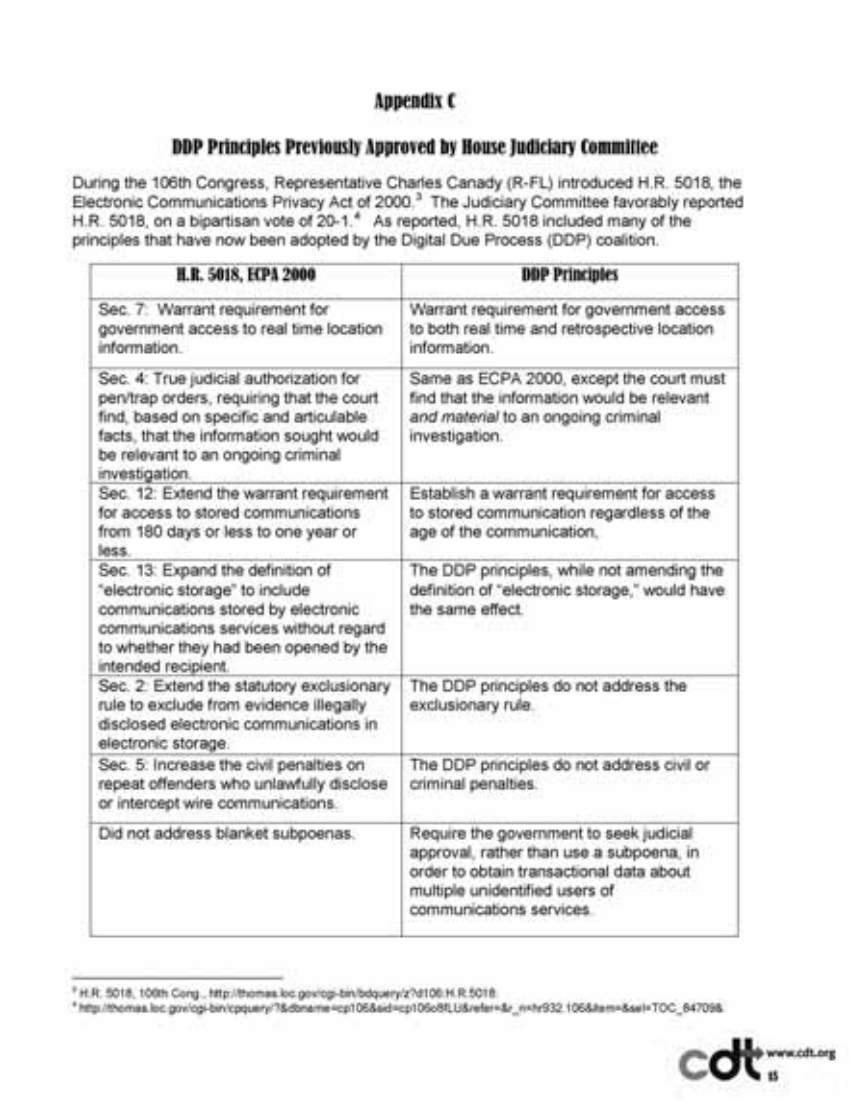
Members of Digital Due Process
(as of May 3, 2010)

Companies

AOL
AT&T
Data Foundry
eBay
Google
Integra Telecom
Intel
Loopt
Microsoft
Salesforce.com
TRUSTe

Trade Associations, Thinks Tanks and other Organizations

American Booksellers Foundation for Free Expression (ABFFE)
American Civil Liberties Union (ACLU)
American Library Association (ALA)
Americans for Tax Reform (ATR)
Association of Research Libraries (ARL)
Bill of Rights Defense Committee (BORDC)
Center for Democracy & Technology (CDT)
Center for Financial Privacy & Human Rights
Competitive Enterprise Institute (CEI)
The Constitution Project
Citizens Against Government Waste (CAGW)
Computer & Communications Industry Association (CCIA)
Consumer Action
Distributed Computing Industry Association (DCIA)
Electronic Frontier Foundation (EFF)
The Future of Privacy Forum
FreedomWorks
Information Technology & Innovation Foundation (ITIF)
NetCoalition
The Progress & Freedom Foundation (PFF)



Appendix C

DDP Principles Previously Approved by House Judiciary Committee

During the 106th Congress, Representative Charles Canady (R-FL) introduced H.R. 5018, the Electronic Communications Privacy Act of 2000.[3] The Judiciary Committee favorably reported H.R. 5018, on a bipartisan vote of 20-1.[4] As reported, H.R. 5018 included many of the principles that have now been adopted by the Digital Due Process (DDP) coalition.

H.R. 5018, ECPA 2000	DDP Principles
Sec. 7: Warrant requirement for government access to real time location information.	Warrant requirement for government access to both real time and retrospective location information.
Sec. 4: True judicial authorization for pen/trap orders, requiring that the court find, based on specific and articulable facts, that the information sought would be relevant to an ongoing criminal investigation.	Same as ECPA 2000, except the court must find that the information would be relevant *and material* to an ongoing criminal investigation.
Sec. 12: Extend the warrant requirement for access to stored communications from 180 days or less to one year or less.	Establish a warrant requirement for access to stored communication regardless of the age of the communication.
Sec. 13: Expand the definition of "electronic storage" to include communications stored by electronic communications services without regard to whether they had been opened by the intended recipient.	The DDP principles, while not amending the definition of "electronic storage," would have the same effect.
Sec. 2: Extend the statutory exclusionary rule to exclude from evidence illegally disclosed electronic communications in electronic storage.	The DDP principles do not address the exclusionary rule.
Sec. 5: Increase the civil penalties on repeat offenders who unlawfully disclose or intercept wire communications.	The DDP principles do not address civil or criminal penalties.
Did not address blanket subpoenas.	Require the government to seek judicial approval, rather than use a subpoena, in order to obtain transactional data about multiple unidentified users of communications services.

[3] H.R. 5018, 106th Cong., http://thomas.loc.gov/cgi-bin/bdquery/z?d106:H.R.5018:
[4] http://thomas.loc.gov/cgi-bin/cpquery/?&dbname=cp106&sid=cp106o8fLU&refer=&r_n=hr932.106&item=&sel=TOC_84709&

www.cdt.org

15

Mr. NADLER. Thank you.

Mr. Gidari is recognized for 5 minutes.

TESTIMONY OF ALBERT GIDARI, PERKINS COIE LLP

Mr. GIDARI. Thank you, Mr. Chairman, Committee Members. It is a pleasure to be here.

Today I appear as an individual not representing any particular service providers or clients, but over 15 years I have had the pleasure of working with many in industry in their implementation and

compliance with ECPA and with the Communications Assistance for Law Enforcement Act.

These service providers are caught in the middle every day. The best way to determine whether ECPA is out of balance is to take a look at what service providers do every day, and that is essentially guess.

They try to understand what the law requires and implement it on a daily basis, but because the law relies so much on definitions, like an electronic communication service provider to the public or a remote computing service provider to the public, service providers have to understand how the law applies to them and the legal process they need to disclose user communications and information. If they don't understand the bright line rule, then mistakes can be made, and those mistakes carry real consequences.

We have cases, one heard just recently in the U.S. Supreme Court, where the service provider guessed wrong, thinking it was one thing when it was another, in disclosing communications on a lower standard than it should have and therefore being liable for that privacy breach.

That is an untenable position for the men and women of service provider security offices, who every day deal with these requests from law enforcement and understand that those requests are valid, important, and sometimes life-threatening, but yet they also have user privacy concerns, and they must meet that imperative to protect user information.

So it is an untenable position for them. They have a real identity crisis about what they are today when in a social networking environment, you could be just as easy an electric communications service provider as a remote computing service provider, and who knows under the definition what you are? It is a very difficult position.

So we know it is out of balance, and we know clarity is important. As much as the academic debate about what the right standard is interesting, it isn't as interesting to service providers as having a clear rule. So if there is anything that can come out of this hearing and future hearings, clarity first and foremost.

I would like to observe also with location-based services, for 15 years I have worked with wireless carriers and their response to law enforcement requests to use what is a remarkably robust and important tool for law enforcement, tracking capabilities, the ability to find a bad person or a kidnap victim in real time as quickly and as efficiently as possible. It is a great, great capability, but right now it is a muddle.

Service providers haven't got a clue what the right legal standard is, and within the same judicial district, you might have two magistrates who disagree and issue contrary orders for the standard upon which to disclose that information. And what information should be disclosed? How often? How frequently? It is not uncommon for law enforcement to ask for a phone to be pinged every 15 minutes.

In a lot of ways service providers' security offices and their personnel feel like they are the customer service of some computer organization, having to respond to incessant and continuous requests. Now, they are important requests, but the fact is the law does not

state how often, how frequently, how rich, how detailed and to whom that information should be provided. The service providers simply need the clarity to understand what to do.

Lastly, I would like to just observe that in ECPA there are some areas for improvement on transparency. It is difficult to make policy if one doesn't know how much information is collected. And from a personal perspective dealing with the volume of requests every day, this Committee and the public would do well to have clear numbers before them.

The number of user records requested on a daily basis is astronomical. We can commend Google, who recently published through their transparency project, a list of statistics that show the number of requests that they receive on a regular basis. Those numbers are dwarfed by the number of requests that service providers like wireless carriers receive every day.

Just yesterday the administrator of the courts received the wiretap report, and that annual report tells you the number of wiretaps conducted each year. For the past year, 2009, the numbers went up 26 percent. There is some good in those numbers. The U.S. stacks up pretty well compared to the rest of the world. If all we had was 2,600 total Federal and state wiretaps last year, somebody is doing something right and reviewing them carefully and not over using them.

Unfortunately, we don't know how many pen registers have been implemented. We don't know how many location orders are implemented. And we certainly don't know how many user records have been asked for, used, and how long those are retained. If we could do anything to improve ECPA and its transparency, the collection and publication of that data would go a long way to helping the Committee make decisions on good, solid policy.

Thank you, and I hope to answer any questions you have.

[The prepared statement of Mr. Gidari follows:]

PREPARED STATEMENT OF ALBERT GIDARI

Before the

Committee on the Judiciary

Subcommittee on the Constitution, Civil Rights, and Civil Liberties

B353 Rayburn House Office Building

Washington, D.C. 20515

HEARING ON ELECTRONIC COMMUNICATIONS PRIVACY ACT REFORM

May 5, 2010

Written Testimony
of
Albert Gidari, Partner
Perkins Coie LLP

agidari@perkinscoie.com

Mr. Chairman and Members of the Subcommittee on the Constitution, Civil Rights, and Civil Liberties, my name is Albert Gidari and I am a partner at Perkins Coie LLP where, among other things, I represent service providers in responding to government requests for user information under the Electronic Communications Privacy Act of 1986 ("ECPA"). Thank you for the opportunity to submit this testimony concerning the need for reform of ECPA to address new innovations such as social networking, cloud computing and location-based services.

Let me say at the outset that these comments reflect my personal views and I am not speaking for or on behalf of any client or group of clients. Instead, I offer my personal observations on the state of ECPA, drawn from over 15 years of working with a wide variety of service providers, including wireless carriers, ISPs, and other online companies. Frankly, from a service provider's perspective, ECPA is broken. How the law applies to all of the new services, applications and technology available to users today is at best an educated guess. As a result, service providers are caught in the middle between law enforcement demands for ever more information and the legal imperative to protect the user's privacy.[1]

ECPA reform should get service providers out of the middle. The privacy community and law enforcement may not agree on the legal standard that should apply in every case, but everyone agrees that service providers must have clear rules for disclosing user communications and information. The rules are not clear today and will be less clear tomorrow as innovation and new services arise that Congress did not contemplate in 1986 when ECPA was first passed.

The Center for Democracy and Technology's Digital Due Process Principles[2] (the "Principles") provide a sound basis for ECPA reform and would go a long way toward addressing what service providers want – bright line rules for disclosing user communications and information regardless of the characterization of the service, the type of technology employed, or whether the information is in transit, at rest on some computer server before reaching its intended destination or stored in the cloud. To demonstrate the need for clarity, these comments review how ECPA might or might not apply to a typical cloud computing application – the online editing and sharing of documents – and the uncertainty about the legal standards that apply to disclosure of the document and user annotations. Similarly, location based services are proliferating, but the legal standards for disclosing historical and prospective location information are a muddle at best and inconsistently applied at the state level. Finally, there are a number of steps Congress can take to improve transparency and process in ECPA to the benefit of user privacy and service provider operations. Enhanced reporting of the number of user records obtained each year, for

---

[1] For a detailed discussion of the serious conflicts that arise between service providers, law enforcement and users, *see* A. Gidari, *Keynote Address: Companies Caught in the Middle*, 41 Univ. of San Francisco L. Rev. 555 (Spring 2007).

[2] The Principles can be found at: http://www.digitalidueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163.

example, would provide the grist for better policy determinations. Likewise, service providers should be able to recover their costs of compliance, and users should be notified of legal process unless doing so would have an adverse effect on an investigation. These improvements would go far to improve ECPA.

What Rules Apply to Services in the Cloud?

Consider how ECPA might apply to a cloud computing service that permits users to create, store, edit and share documents over the Internet with others. The service is free to users, but it is advertising supported; that is, ads are served to users based on a mechanical scan of the content of the document for key words that advertisers use to display text ads. The service permits users to post documents and then invite others to view or edit them. Indeed, invited "collaborators" can annotate and edit the document in real time, seeing each others' changes as they are made.

Here's how such a service might be used today. A college student can post her paper via a cloud computing service and invite her professor to view it online. The invitation is in the form of an email generated from within the application when the student opts to share it with others. The professor can then access the document simply by clicking on the link provided in the email and then proceed to annotate the student paper, asking questions like "what is the cite for this quote?" The student may respond in real time by adding, for example, a footnote citation and inserting a comment that the citation was inadvertently omitted. The professor can see her typing as the words appear on the screen in the document itself. If the paper was a joint student project, other students could follow the real time annotations and changes. If they were offline when the changes were made, they would receive an email notice that the paper has been revised with a link to go view it.

There is substantial doubt as to whether or how ECPA applies to the service. Yet, the answer determines whether law enforcement will need probable cause and a search warrant to compel disclosure of the document and annotations or whether a mere subpoena issued without judicial review or even notice to the user will suffice. The privacy implications are palpable. If the service provider is a remote computing service to the public under ECPA, then law enforcement may compel the disclosure of the document and annotations with a grand jury or administrative subpoena with notice to the user unless such notice is delayed because it will have an adverse effect on the investigation.[3] If the service provider is an electronic communication service provider to the public under ECPA, then the government must obtain a search warrant based on probable cause to compel disclosure of content in electronic storage for less than 180 days. Thus, under ECPA today, it is the characterization of the service provider and its service

[3] As a practical matter, the service provider has no way of knowing whether a user has been given notice of the subpoena. Law enforcement agents are not required to certify that notice was given nor are service providers required to obtain proof of notice before disclosing the information.

offering rather than the content of the document or communication that determines the degree of protection afforded to users.

On the one hand, the student stores the document on the host's servers and uses the service's features to process her edits. The service seems to fit the ECPA definition of a remote computing service - "the provision to the public of computer storage or processing services by means of an electronic communications system."[4] But the sharing and collaboration features of the service have more in common with an electronic communication. Indeed, the purpose of posting the document is to provide others access to it and the service provides capabilities for users to communicate within the document itself through annotations or embedded comments. ECPA defines electronic communication to mean "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[5] If the service provider is wrong about how to characterize itself or the service, user information may be disclosed on a lesser standard, and the service provider may be subject to civil suit.

The risk is not theoretical. In *Quon v. Arch Wireless Operating Co., Inc.*,[6] a case just argued before the Supreme Court on a different point of law, the service provider incorrectly decided that it was a remote computing service for purposes of disclosing stored text messages to its customer, the City of Ontario, California. The Court of Appeals for the Ninth Circuit decided that the service provider was in fact delivering an electronic communication service and therefore it needed the consent of the individual users, not the City-subscriber, to disclose the stored communications. As a consequence of guessing wrong, the service provider incurred liability.

To further confuse matters, the Department of Justice ("DoJ") takes the position that, notwithstanding the *Quon* opinion, a service provider may offer both a remote computing service and an electronic communications service simultaneously, or it may not be covered by ECPA at all. For our college student's document in the cloud, if she didn't share it with anyone and simply stored it with the service provider for her own use, presumably DoJ likely would view the service as a remote computing service. But because the service provider is permitted to access the content of the document for advertising purposes, DoJ would say that ECPA does not apply at all to the service. The document simply falls outside ECPA and a simple subpoena without any notice to the user would suffice to compel its disclosure.

---

[4] 18 U.S.C. § 2711(2).

[5] *Id.* § 2510(12).

[6] 529 F.3d 892 (9th Cir. 2008).

It is unclear whether DoJ would agree that the collaboration and sharing features of the service that permit users to communicate with each other within the document itself constitute an electronic communication service. But even if it did, once the annotations were read by any other person authorized to view them, DoJ's position would be that ECPA no longer applies, just as it contends ECPA does not apply to opened email.[7]

So what is a service provider to do? CDT's Principles would treat user generated and stored content the same regardless of the service, functionality or technology involved. The Principles would require the government to obtain a search warrant based on probable cause to compel disclosure of any content stored in the cloud. This approach has the virtue of assuring users that their information will be protected the same in the cloud as it would be on their own computer in their home. Service providers would have a clear rule that would be easy to follow, and litigation would be avoided. In practice, some service providers already take this position and any applications that permit users to share content are treated as electronic communication services.

What ECPA Issues Arise with Location Based Services?

Location information long has been a mainstay in criminal investigations, yet after almost two decades of acquisition and use of the data, the legal standard for obtaining historical location information records, current real time location, and prospective tracking remain unsettled. Whether probable cause is the appropriate standard for obtaining historical location information is before the Court of Appeals for the Third Circuit,[8] but plainly, the government routinely acquires historical data using the lower standard in Section 2703(d) of Title 18.

The legal standard for obtaining prospective location information and tracking data has been the subject of a "magistrates' revolt" for several years. Many federal magistrates have refused to permit prospective location information acquisition on less than a probable cause showing. Those magistrates who reject the lesser standard find that when the government uses a cell phone to track a user, it converts the phone

---

[7] The DoJ steadfastly maintains that once an email has been opened, it is no longer in electronic storage and can be obtained with a subpoena. The Court of Appeals for the Ninth Circuit has rejected this interpretation, but DoJ disagrees and routinely moves to compel service providers who reside in the Ninth Circuit and store user data within that jurisdiction to disclose such information in districts outside the Ninth Circuit states. Just last month, DoJ moved to compel Yahoo to make such a disclosure in the United States District Court for the District of Colorado, but subsequently withdrew its demand. An amicus brief filed in the case can be found at: http://www.eff.org/files/filenode/inreusaorder18/AmiciBriefYahooEmails.pdf.

[8] *In re U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government,* 534 F. Supp. 2d 585 (W.D. Pa. 2008)(entire district rejects government request and requires probable cause for stored and prospective location), *order aff'd by In re U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 2008 WL 4191511 (W.D. Pa. Sep. 10, 2008).

into a mobile tracking device, which is governed by Section 3117 of Title 18 and which, pursuant to Federal Rule of Criminal Procedure 41, requires a search warrant based on probable cause.

But sometimes even in the same judicial district, some magistrates have ruled that the government is entitled to the information on a lesser showing. Because a single district judge's ruling does not establish binding precedent within a district,[9] service providers must follow whichever form of order they receive. And because ECPA provides the floor for state legal process as well, the proper legal standard is more confusing when federal magistrates sitting in the same federal district in a state disagree – which standard should a state court judge follow when issuing a tracking order? The result is that two identically situated users under investigation in the same state may have their location information acquired by federal agents on two different standards, and for state investigators, it essentially is a dealer's choice as to which standard is applied to get the tracking information.

As interesting as the debate is over the proper legal standard for tracking, there are other legal issues not answered in ECPA today as well. The following issues are faced by service providers every day in response to government demands for acquisition and use of location Information:

a. Duration and Periodicity of Order. Orders for location information seldom state the duration. If Rule 41 applied, the duration would be 10 days; but common practice is to require location information reporting for the duration of a pen register order, up to 60 days. Further, how frequently location information is to be acquired during the course of a day remains unclear and whether it is to be limited to the beginning and end of a call, or autonomous registration. In other words, can law enforcement require reporting of location information every 15 minutes for a period of 60 days?

b. Compensation to Service Provider. Under the government's hybrid theory, service providers should be entitled to cost recovery under both Sections 3124 and 2706 of Title 18, but there is no clear reimbursement rule for Rule 41.

c. Notice to Users. Notice is not prohibited for historical records obtained by a court order alone under Section 2703(d); it is prohibited for hybrid order; and it is unclear for Rule 41.

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

---

[9] *See, e.g., ATSI Communs., Inc. v. Shaar Fund, Ltd.,* 547 F.3d 109, 112 & n. 4 (2d Cir. 2008) (citing cases).

to seek the location of the community of interest – that is, the location of persons with whom the target communicates.

e. Customer or User Consent to Track/disclose (implied or express). Can a user consent to tracking or disclosure of location information, and if so, whose consent is necessary – the user's or subscriber's?

f. Preemption of less strict state law. To the extent a state law or rule permits location information to be disclosed on a lower than federal standard, ECPA preempts the state rule, but state law enforcement authorities disagree or seldom have heard of ECPA.

g. GPS standard. The accepted rules of *Knotts*[10] and *Karo*[11] -- tracking in a public place is permissible without a warrant; tracking in the home is not -- are under attack in state courts as those rules have been applied to GPS.[12] Courts are now deciding that modern GPS is much more intrusive than the "bugs" used in *Knotts* and *Karo*, and such sensory enhancements may require reevaluation in light of the Supreme Court's decision in *Kyllo.*[13] GPS is now part and parcel of many third party applications as well -- what standard applies to GPS data in a third party's possession?

h. Location information as content. In the case of many location-based services ("LBS"), some logging of a user's location may occur and be retained. In many such applications, the user is conveying his or her location to another user essentially as a communication – "here I am." LBS providers treat such electronic communications as content that cannot be disclosed under ECPA without complying with the requirements of Section 2703, which means that the characterization of the service provider as a remote computing service or an electronic communication service will determine the standard under which the location information is disclosed.

---

[10] *United States v. Knotts*, 460 U.S. 276 (1983) (Fourth Amendment does not prohibit tracking in a public place).

[11] *United States v. Karo*, 468 U.S. 705 (1984) (monitoring a beeper in a private home violates the rights of those justifiably expecting privacy there).

[12] *See People v. Weaver*, http://www.nycourts.gov/ctapps/decisions/2009/may09/53opn09.pdf (N.Y. Court of Appeals, May 12, 2009).

[13] *Kyllo v United States*, 533 U.S. 27 (2001) (use of thermal-imaging device to detect relative amounts of heat in the home is an unlawful search).

How Can Greater Transparency be Achieved in ECPA?

Service providers are overwhelmed by the volume of governmental requests for user communications and information. There are over 10,000 federal, state and local governmental agencies with subpoena power. The volume of user information collected by government is astonishing, but largely unreported. Only Google publicly reports the number of governmental requests it receives.[14] The number of requests Google receives is dwarfed by the number of requests wireless carriers receive each year.

It is difficult to understand how sound policy can be made without knowing how much user information is collected. Take pen register information for example. DoJ is required to report the number of pen registers conducted each year to Congress.[15] It has not done so with any regularity, but even if it had, the number of pen register orders implemented is not all that revealing. More important is the number of subscriber records obtained under the order.

Pen register orders routinely authorize the investigating agent to compel disclosure of subscriber records for every person called or calling the target phone. A target can make hundreds of calls during a typical 60-day pen register period. The pen register yields a list of numbers, and law enforcement agents routinely send that list to every carrier that might possibly provide service, demanding production of any records for any number that belongs to that carrier. Thus, a single pen register order can result in the disclosure of hundreds of individual customer phone records. Likewise, a single grand jury subpoena may list dozens of accounts for which subscriber information is sought.

Account-based reporting would provide Congress and the public with the necessary information to judge whether the right balance has been struck as to the standards and ease with which information is

---

[14] *See* the Google Reporting Tool at http://www.google.com/governmentrequests/.

[15] *See* 18 U.S.C. § 3126. Reports concerning pen registers and trap and trace devices.

The Attorney General shall annually report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice, which report shall include information concerning—

(1) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;
(2) the offense specified in the order or application, or extension of an order;
(3) the number of investigations involved;
(4) the number and nature of the facilities affected; and
(5) the identity, including district, of the applying investigative or law enforcement agency making the application and the person authorizing the order.

gathered. Congress has required as much for emergency disclosures, but again, no public reports are available as to whether DoJ has complied with this requirement either.[16]

Service providers are prohibited by ECPA from recovering the cost of producing phone records,[17] but service providers otherwise may recover costs reasonably necessary for the production of other subscriber information. When records are "free," such as with phone records, law enforcement over-consumes with abandon.[18] Pen register print outs, for example, are served daily on carriers without regard to whether the prior day's output sought the same records. Phone record subpoenas often cover years rather than shorter, more relevant time periods. But when service providers charge for extracting data, such as log file searches, law enforcement requests are more tailored. Further, mandatory reimbursement would permit Congress to "follow the money," creating an audit trail of how much is spent in collecting user communications and information.

Users, of course, generally are unaware of requests for their information. The law precludes notice of interception and pen register orders, but there is no prohibition on notice of grand jury or administrative subpoenas or other court orders. Yet, because ECPA does not require notice to the user prior to service provider disclosure to the government, most service providers do not give notice.

The government has the ability to obtain an order to prevent notice in limited cases where such notice may yield an adverse result such as (a) endangering the life or physical safety of an individual; (b) flight from prosecution; (c) destruction of or tampering with evidence; (d) intimidation of potential witnesses; or (e) otherwise seriously jeopardizing an investigation or unduly delaying a trial.[19] But more commonly, it simply requests nondisclosure (although some have argued that disclosure would be an obstruction of justice), and service providers generally comply.

But the government has a means to ensure against an adverse effect on an investigation. Mandatory notice should be required in all other cases so that users (rather than service providers) can assert their

---

[16] *See* 18 U.S.C. § 2702(d) Reporting of emergency disclosures.--On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing--

> (1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8); and
> (2) a summary of the basis for disclosure in those instances where--
>
> > (A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and
> > (B) the investigation pertaining to those disclosures was closed without the filing of criminal charges.

[17] *See* 18 U.S.C. § 2706(c).

[18] No one knows how long the collected information is retained or which agencies have access to it.

[19] 18 U.S.C. § 2705.

rights. How would a service provider know that an otherwise routine-looking subpoena was directed at protected First Amendment rights for example? Service providers should not be in the middle of such disputes.

Finally, service provider response to the enormous volume of government requests is an exercise in daily triage. Every agency believes its request should be handled first, its investigation is most important, and any other agency's needs can be given lower priority. It is not uncommon in pen register orders today to see a requirement to produce subscriber records "immediately" upon agency request or in an expedited fashion such as "no later than 3 days after demand." Rules of procedure typically allow only a short period of time in which to respond, and put the burden on the third party to move to quash or amend an unduly burdensome request.

This "press for production" establishes all the wrong incentives. There should be no incentive to rush or not review legal process. Moreover, the squeaky wheel should not get the oil of advanced or quicker production by calling security office personnel and threatening contempt or cajoling early compliance. The service provider ought to have, and ECPA should provide, a priority rule of "first in, first out" for any request, and a uniform time frame for compliance of 30 days should be set for both federal and state governmental entities, absent an emergency.

Conclusion

Thank you for the opportunity to present these comments today in favor of ECPA reform. ECPA always has been a complicated statute and difficult for service providers to implement in the simplest of times. But as new services and innovations come along, the task of legal compliance has become more luck than art. Service providers want clarity and bright line rules. I believe that users, privacy advocates and law enforcement want the same thing.

In closing, the Committee should understand one thing – service providers employ hundreds of security office professionals who each day confront ECPA problems of interpretation and implementation. These men and women know that their hesitation or delay may have life or death consequences. At the same time, they know that user privacy is important and an imperative. It is really these men and women who are caught in the middle and deserve our appreciation for the professional job they do every day.

Similarly, law enforcement agents who seek user communications and information generally do so in a professional and courteous way. By far, the majority of requests are handled in this way and do not give rise to disputes. While the relationships between law enforcement and service providers may vary from provider to provider, in my experience, mutual respect and professionalism has been the rule.

Mr. NADLER. Thank you.
And I now recognize Mr. Kerr for 5 minutes.

TESTIMONY OF ORIN S. KERR, PROFESSOR, THE GEORGE WASHINGTON UNIVERSITY LAW SCHOOL

Mr. KERR. Chairman Nadler and Members of the Subcommittee, thank you very much for the invitation to be here today.

I think it might help to start with understanding why we are here. In traditional criminal investigations, the police do the work on their own. They walk the beat. They conduct their own searches. If they see evidence of a crime that they think they need, they take it. They don't work with providers. They don't work with anybody else. They make all the decisions on their own, sometimes pursuant to judicial review by a judge, but not with the work of any private party.

The opposite is true with new online crimes, crimes committed using networks, whether it is the Internet, crimes committed using telephones, or simply a case where there happens to be evidence that is stored or available over some sort of a network, whether the Internet or the cell network.

In all those cases, the government is working through the intermediary of the provider. There is a company, a company that runs a network that has data, and the real question, and the question that the Electronic Communications Privacy Act is designed to address, is what should the rules be when the government wants data that the network has, or when the network company, the third-party provider, wants to disclose information to the government?

Now, that means that in order to understand the issues raised by ECPA, we need to think about what the data is and when does the government obtain it. So it may be helpful to think about two different kinds of data that the communications providers may have.

One category is content of communication. That is the actual message that somebody may be sending or receiving over the network. It might be an e-mail. It might be a text message. In the case of a phone call, it would be the actual conversation that two people are having.

And then there is lots of non-content information. The non-content information is information that the network is generating and using in order to deliver the communication. Now, we can understand what kind of content the network might have, because we as users of the network are aware of that. If somebody sends you an e-mail, for example, you know that the e-mail is there.

Non-content information is quite different. The amount of information that may exist depends on the technology, depends on the network. It may depend on the company, depends on business decisions that each company is making as to whether to keep records, whether to generate certain records. And that means there are lots of records available, and those records may vary dramatically, based on the company and based on the technology. So that is the issue of what the records are that are out there.

The next thing you need to think about is when is the government collecting the information. So again, we can think of two basic categories. The one category would be when the government comes to the provider and says, "We are going to compel you to dis-

close certain information. We want you to act on our behalf as our agent, essentially, and provide certain information."

Maybe it will be stored content that the government wants. Maybe it will be stored non-content information that the government wants, these records. And other times the government will want a real-time surveillance to occur, sometimes of content in the case of wiretapping, sometimes in the case of non-content information, for example, where somebody's cell phone is located or who somebody is e-mailing. So that is the case when the government is compelling information.

And then the flipside of that is what if the provider comes across evidence and wants to disclose it to the government? Maybe the provider has uncovered child pornography. Maybe the provider has discovered some evidence of some other crime and wants to provide that information either to the government or even to a non-government group. What should those rules be? That is the question that the Electronic Communications Privacy Act was designed to address in 1986.

Now, of course, in 2010, technology has changed dramatically. And I am very glad to hear that the Committee has planned more hearings, because I think what really we need to hear from is we need to hear from these providers. We need to find out what information do they have.

What are their practices? What is the technology? How does it work? What kind of cell phone location information do different providers have? How close can they get to finding out the location of the user of the phone? How long do they keep their records?

So we need to find out from the providers what are their practices. And then we also need to find out from the government how do their investigations work? Those of us that watch a lot of television know we have seen a lot of Law and Order, and we know how those investigations work, or at least how they work on TV.

But mostly we don't know how these new online investigations work. We haven't seen those investigations. Very few people have. So we need hearings to talk about not only the technology, but what are the kinds of cases that the government is working? How do these cases actually unfold?

And I think it is only after getting that informed sense of what the technology is and how the investigations actually work that the Committee can think about what do these rules need to be like. How do these rules need to change? It has been a quarter century since ECPA was passed, and it is time to think about how the technology has changed and how to balance the security interests and privacy interests, given the technology of today, not the technology of 1986.

So I am very glad that the Committee is interested in these issues. Obviously, today's hearing is just the tip of the iceberg. There is a lot that we can talk about. But I think starting off by recognizing that this problem exists, both in terms of the new technologies and these new types of investigations, is a very important first start, and I am happy to be here. Thank you.

[The prepared statement of Mr. Kerr follows:]

PREPARED STATEMENT OF ORIN S. KERR

Testimony of Orin S. Kerr
Professor, George Washington University Law School
United States House of Representatives
Committee on the Judiciary
Subcommittee on the Constitution, Civil Rights, and Civil Liberties
Hearing on Electronic Communications Privacy Act Reform

May 5, 2010

Chairman Nadler, Ranking Member Sensenbrenner, and Members of the Subcommittee:

My name is Orin Kerr, and I am a Professor at George Washington University Law School. I wish to thank the Members of the Committee for their willingness to delve into the complicated and yet extremely important privacy laws that Congress has created to protect Internet and telephone communications. I teach these statutes to my students as part of my law school course on Computer Crime Law, and my students are routinely surprised that the law here is so out-of-date.

Reforms here are surely needed. The question is, what reforms are best? I have set out many of my own views in a law review article, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, published by the George Washington Law Review in 2004. But today's hearing has been prompted by a specific set of proposals offered by the Digital Due Process coalition. Given that, I thought it would be most help to list the proposals offered by the Digital Due Process coalition and then respond to them.

Before I begin, I want to stress two points. First, I think it's helpful to approach reforming these statutes with a simple goal in mind: In my view, the goal of the Electronic Communications Privacy Act should be to try to match privacy rights in online and telephone- based investigations to the kinds of privacy rights we are familiar with in traditional physical investigations. Most of us have watched the TV show *Law & Order*, and we're familiar with both the powers that the government has to solve crimes as well as the limitations placed on those powers needed to protect and preserve our individual rights. Those powers and their limitations reflect a constitutional balance: It is the balance that the Supreme Court tries to make in interpreting the Fourth Amendment's prohibition on unreasonable searches and seizures. The Electronic Communications

Privacy Act is a statutory version of the Fourth Amendment for a new technological age: It tries to impose the same sort of balanced approach to the new investigations involving new network technologies that the Fourth Amendment strikes in the physical world. As a result, the goal of reforming the statute should be to maintain that balance as technology continues to change.

Second, it would be extremely helpful for Congress to precede any amendments to these statutes with extensive hearings on the latest technologies and the latest government practices. The best way for Congress to update these statutes is to hold open hearings in which government officials can explain how they are using these new technologies and representatives from Internet service providers and phone companies can explain how their technologies work and how they cooperate with law enforcement. Without such hearings, we can only guess at the specifics of how different rules will actually impact real-world investigations. Informed rulemaking requires a thorough understanding of investigative practices and new technologies, and the best way to determine that would be through open Congressional hearings.

With those general points made, let me now turn to the four specific proposals made by the Digital Due Process coalition:

Proposal 1

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

My reaction: Generally favorable, but with two reservations.

Explanation: I agree that the distinctions found in the current statute make no sense. Further, it is my view that the Fourth Amendment requires a warrant to be obtained in this setting, as I explained in a recent article. *See* Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005 (2010).

As a result, any statutory rule that allows the government to obtain contents with less process than a warrant will be unconstitutional in many settings.

I have two reservations. First, such a rule may not work when the government obtains records from corporations that are suspected of engaging in criminal activity. In the corporate crime setting, the government generally obtains records using subpoenas rather than warrants. The government compels the corporation to disclose its records under the power of the subpoena without first obtaining probable cause. Because the Electronic Communications Privacy Act applies to all providers of electronic communication service, however, a warrant requirement for all contents stored by entities covered by the statute might inadvertently block investigations into such corporate crimes.

Consider how a warrant requirement might work in that setting. If a warrant is required for every compelled access to every e-mail account, the corporation under investigation will plausibly insist that each e-mail account of each corporate employee must be justified by its own search warrant and its own finding of probable cause. Corporations engaged in criminal activity could use this rule by keeping all their records stored in the form of e-mails: They could store the evidence of fraud in documents stored as attachments, using the protections of the Electronic Communications Privacy to hide evidence of fraud from investigators. The result would block many if not most investigations into corporate criminal activity. For example, my understanding is that the Securities and Exchange Commission (SEC) does not have criminal enforcement power and could not obtain a warrant to investigate securities violations under an all-warrant rule. The SEC relies on subpoenas, which would not be usable so long as the corporation under investigation provided e-mail to its employees.

To avoid this, Congress should consider a rule that permits the government to use its subpoena authority in the case of investigations into corporate crimes when obtaining records from a designated representative of the corporation. A similar rule may also be useful in the case of investigations into misconduct by government employees. The government employees may have no Fourth Amendment rights in their government-provided accounts, but investigators will nonetheless wish to compel the contents of a government employee's accounts from the agency that provides the service. If there are

no Fourth Amendment protections in that setting, a warrant should not be necessary and a subpoena should suffice.

Proposal 2

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

My reaction: I disagree in part.

Explanation: I have two concerns about this proposal. First, it is vague. Second, it does not distinguish among different types of location information.

My first difficulty with this proposal is that it is vague. The proposal would require probable cause, but probable cause *of what*? Is that probable cause to believe the person tracked is guilty of a crime? Or is it probable cause to believe the evidence of location information obtained would *itself* be evidence of crime?

The difference is important. In the case of a search warrant, "probable cause" generally refers to probable cause to believe that the information to be obtained is itself evidence of a crime. But cell phone location information will itself be evidence of crime only in specific kinds of cases. For example, such information normally will not be evidence of a crime if investigators want to obtain the present location of someone who committed a past crime.

To see this, imagine the police have probable cause to arrest a criminal for a crime committed last week. The police want to locate the suspect in order to arrest him. In that case, the police will not have probable cause to believe that the location of the criminal's cell phone is itself evidence of a crime. The suspect's location a week after the crime occurred does not give the police any information indicating that the suspect did or did not commit the crime. But if the police have probable cause to arrest someone, and they know his cell-phone number, I would think the law should allow the government some way of locating the suspect pursuant to an appropriate court order. A requirement that

location information be obtainable only based on probable cause to believe that the location information is itself evidence of a crime would not seem to allow that.

My second concern with the proposal is that not all location information is created equal. The level of cause that should be required may depend on the resolution of that identity information. Location information that tells investigators only that a suspect is somewhere in Manhattan is quite different from location information that tells investigators that a suspect is in the far left corner of his bedroom. Before legislating in this area, I think the committee should hold a hearing focused on the technology. Just how much resolution does location information from cell phones actually reveal? How is technology likely to change?

Such distinctions are important because mobile phone location can be determined in different ways. When investigators seek historical location data – that is, location data indicating where a phone was located at some point in the past when a crime occurred – the available information is likely to give only a very rough indication of location. In that case, the available information normally will consist only of indicating what cell towers were used to transmit calls to and from a phone in the past. So-called "cell site" information is generated because cell phones must communicate with local cell towers to transmit and receive calls: The information as to what cell towers a particular phone is communicating with gives the cellular phone provider a rough idea of the location of the phone.

Other techniques can be used to obtain more exact location information in "real time," that is, as a crime is actually occurring in the present. For example, GPS-enabled cell phones calculate location information by receiving signals transmitted from satellites in orbit. Cellular provide providers can then obtain the information received from those signals, and that information generally is much more precise than historical cell-site data. Similarly, cell phone providers normally can obtain precise information on the physical location of a cell phone in real time using methods that measure the strength and timing of communications between a particular cell phone and multiple towers. My understanding is that different telephone providers have different abilities to perform this sort of precise location determination in real time.

Given the range of different techniques that could be used to determine the location of a mobile phone, and the different resolution of the different techniques, it would be very helpful to have a hearing on the latest types of technologies and government practices. Representatives of cell phone providers can give you the most accurate sense of how their networks work and what information they can provide. Government officials can testify as to exactly how they use cellular phone location information. What are the cases? Is such information used to monitor ongoing crimes, such as monitoring a known criminal as he commits an offense? Is it used to find individuals known to have committed past crimes? Is it used to try to prove that a suspect was in a location in which a crime occurred, to rule out a potential alibi? It is hard to know the right level of protection without knowing the kinds of cases to which the new rule will be applied.

Proposal 3

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

My reaction: I agree.

Explanation: I agree that the standard for obtaining information under the pen register statute should require judicial review and should be raised to the specific and articulable facts standard used in 18 U.S.C. § 2703(d). However, I think the standard should not be higher than that. In particular, Congress should not require a warrant given that the kind of information here is non-content data rather than content data.

Proposal 4

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

My reaction: I'm certainly open to it, but it's very vague.

Explanation: I have no objections to the idea of requiring judicial review for bulk requests, but I'm not entirely sure what line the Digital Due Process coalition intends to draw with this proposal. What is the line between a "particularized" request and a "bulk" request?

For example, imagine the government seeks records of the Internet accounts assigned to a specific Internet Protocol address during a one-week period. Is that a "particularized" request or a "bulk" request? On one hand, it doesn't seem to specify the account or individual, but on the other hand it will often be the case that only one account was associated with that IP address during a one-week period. Similarly, imagine the government submits 1,000 account names and obtains a single subpoena to gather the basic subscriber information for all 1,000 accounts. On one hand, that seems to be a bulk request. On the other hand, it specifies which individual accounts will be obtained.

Greater clarity would be helpful to understand what the Digital Due Process coalition has in mind with this proposal. Further, additional hearings into the details of the investigations that prompted this proposal would be helpful. As I explained in the beginning of my testimony, Congress needs to be informed about what is actually happening "on the ground" before it can make sensible rules to govern those practices. Open hearings on the use of bulk requests to obtain identify information would give Congress a better sense of what is actually happening. This could then be used to craft the appropriate response to best balance government needs and individual privacy interests.

Mr. NADLER. Well, thank you.

And we will now recognize Ms. Levins for an opening statement.

TESTIMONY OF ANNMARIE LEVINS, ASSOCIATE GENERAL COUNSEL, MICROSOFT CORPORATION

Ms. LEVINS. Thank you, Mr. Chairman.

Mr. Chairman, Members of the Subcommittee, my name is Annmarie Levins. I am an associate general counsel at Microsoft. I manage the legal support for Microsoft U.S. and Canadian subsidiaries. My team is responsible for contracts with our customers and partners for anti-piracy and digital crimes investigations, for Internet safety work and other areas.

Before joining Microsoft in 1998, I had the privilege of serving as an Assistant United States Attorney in Seattle for 3 years and before that in the Southern District of New York for seven. During my 10 years as an A-USA, I worked with many smart, dedicated law enforcement officers investigating organized crime, racketeering, narcotics and financial fraud cases.

Thank you for this opportunity to share Microsoft's views on the reform of ECPA. Microsoft is in a unique position to comment on the need for ECPA reform. We have offered Internet-based services for almost 15 years, dating back to MSN dial-up Internet service. We have offered Hotmail, our free Web-based mail service, since 1997.

Today we offer a full array of cloud computing services, including our hosted suite of Enterprise class e-mail, relationship management and collaboration tools, and our cloud-based storage and computing resources called Microsoft Azure. Our customers range from individuals to small and medium-sized businesses to some of the largest multi-national corporations in the world.

From our vantage point, we have seen how the technologies governed by ECPA have evolved over the years since its enactment and the tremendous potential these technologies represent for all of our customers. Today users can store documents, data and communications to central locations and access them anywhere in the world on a wide variety of devices, including laptops, phones and other forms of personal devices.

Increasingly, Web-based accounts are used interchangeably with local storage devices. As these Internet-based resources become part of our everyday computing experiences, users may not even realize that the legal protection afforded their data and documents are not necessarily the same when they use third-party storage and processing capabilities in place of their own computers or networks.

While there has been a fundamental shift in the amount of sensitive information that we now trust to third parties, the law has not shifted in parallel to preserve reasonable privacy interests. Quite simply, the basic technological assumptions upon which ECPA was based are outdated. The nature of the protection afforded to stored electronic communications has not kept pace with the many innovations in online computing over the last 24 years.

For example, ECPA extends greater privacy protections to e-mail storage for less than 180 days than e-mail stored for more than 180 days. This distinction might have made sense in 1986 when e-mail services did not automatically retain messages for long periods of

time, but the distinctions no longer bear any relationship to reality. Hosted e-mail and other online services regularly store e-mails and other content for years, and users today reasonably expect these communications to remain just as private on day 181 as they were on day 179.

Microsoft believes that now is the time to address these issues. We are on the verge of a transformative age in Internet cloud-based computing. Cloud computing services can increase efficiencies for business and government, lower IT costs, create energy savings, and spur innovative job-creating enterprises. They will enable small and medium-size businesses, individual entrepreneurs and other innovators to tap into computing resources that previously had only been available to the largest companies, and at a fraction of the cost.

These capabilities can drive innovation, make America's businesses more competitive, and ultimately contribute to economic growth. But unless we are able to preserve and protect users' privacy interests to meet their reasonable expectations, adoption of cloud computing services may be limited, and the full potential of cloud computing may not be realized.

Indeed, in a recent poll conducted for Microsoft, more than 90 percent of the general population and senior business leaders said they were concerned about security and privacy when they contemplated storing their own data in the cloud. This is among the reasons why Microsoft joined the Digital Due Process coalition in the launch of a new initiative to update ECPA.

We understand the importance of supporting lawful investigations and spend significant resources every year to help make the online environment safer for all users. The Microsoft Digital Crimes Unit that I oversee was created specifically to assist law enforcement in pursuing digital crimes and to provide training to prosecutors and investigators around the world.

In conclusion, Microsoft believes that the decisions about the right balance between users' reasonable expectations of privacy and law enforcement's legitimate interests should be made by Congress, with input from all key stakeholders, rather than as a result of unanticipated shifts in technology.

We view the Digital Due Process coalition proposal as a good starting point for Congress' inquiry. Ultimately, smart, targeted reforms of ECPA are essential to restore proper balance between privacy and law enforcement in the digital age and will help cloud computing fully deliver on its promise.

Thank you for the opportunity to testify today. On behalf of Microsoft, we appreciate this Committee's leadership in addressing these important issues, and we look forward to working with you.

[The prepared statement of Ms. Levins follows:]

PREPARED STATEMENT OF ANNMARIE LEVINS

Statement of Annmarie Levins
Associate General Counsel
Microsoft Corporation

Before the
Subcommittee on the Constitution, Civil Rights, and Civil Liberties
United States House of Representatives

Hearing on Electronic Communications Privacy Act Reform

"Protecting Privacy in the Cloud:

Updating ECPA for the Internet Age"

May 5, 2010

Chairman Nadler, Ranking Member Sensenbrenner, and honorable Members of the Committee, my name is Annmarie Levins, and I am an Associate General Counsel at Microsoft Corporation. In that capacity, I manage the legal support for Microsoft's U.S. and Canadian subsidiaries, directing the legal teams responsible for licensing and services transactions, anti-piracy investigations and enforcement, Internet safety work, and other areas. One of the teams that I oversee is the Microsoft Digital Crimes Unit—which is devoted to working with law enforcement to fight digital crime. Before joining Microsoft in 1998, I served in the U.S. Attorney's Office in Seattle for three years as Co-Supervisor of the Financial Fraud Investigations Unit. Prior to that, I served for seven years as an Assistant U.S. Attorney in Southern District of New York with a focus on organized crime and racketeering investigations.

Thank you for this opportunity to share Microsoft's views on reform of the Electronic Communications Privacy Act of 1986 (ECPA). We appreciate the initiative that this Committee has taken in holding this hearing, and we are committed to working collaboratively with you, consumer organizations, law enforcement agencies, and all Americans to ensure that users' privacy interests are adequately protected in the digital age. As Microsoft's General Counsel, Brad Smith, announced in a speech at the Brookings Institution in January, we support efforts to modernize ECPA and bring the statute into alignment with today's technological realities.

ECPA was passed by Congress almost 25 years ago to establish rules that govern whether and how law enforcement can compel third party telecommunications and Internet service providers to disclose customer account information and stored

communications which they hold incident to their services. The law was originally designed to strike a balance between the legitimate needs of law enforcement, the burdens on service providers, and the public's reasonable expectations of privacy.

Microsoft is in a unique position to comment on the need for ECPA reform. We have offered Internet-based services for almost 15 years, dating back to MSN's dialup Internet service. We have been offering Hotmail, our free, web-based email service, since 1997. Today, we offer a full array of cloud computing services to individuals as well as to enterprises, including our hosted messaging and online collaboration solutions, Microsoft Business Productivity Online Suite, and our cloud-based storage and computing resources, Microsoft Azure. From our vantage point, we have seen the full arc of how online services have evolved over the time since EPCA was passed in 1986.

It is our experience that the state of the law has not kept pace with developments in technology. Today, users can store documents, data, and communications to networked computers and connect to them from anywhere in the world using a wide variety of devices, including laptops, phones, and other personal electronic devices. Increasingly, Web-based accounts are used interchangeably with local storage devices. As these Internet-based resources become part of our everyday computing experiences, users may not even realize when they are using third party storage and processing capabilities. Accordingly, we believe users would be surprised to learn that the legal protections afforded their information will vary depending upon whether it is in the hands of a third party service provider at the moment the government seeks to obtain it.

Over the last 20 years, there has been a fundamental shift in the amount of sensitive information that we entrust to third parties, but the law has not shifted in kind to maintain the proper balance between the needs of the law enforcement and the public's reasonable expectations of privacy. The reason is that ECPA, the law that regulates whether and how the government can require third party Internet and telecommunications providers to disclose customer information and stored communications, relies on outdated notions of how individuals and businesses interact with information technology.

Microsoft believes that now is a critical time to address these issues. We are on the cusp of a potentially transformative age of Internet-based "cloud" computing. Cloud computing services can increase efficiencies for businesses, lower IT costs, create energy savings, and spur innovative job-creating businesses. However, unless users' privacy interests are preserved and protected to meet their reasonable expectations, adoption of these services—particularly by enterprises—may, unfortunately, be rather limited and the full potential of cloud computing may not be realized.

This is among the many reasons why Microsoft has joined a broad coalition of advocacy groups, technology companies, and academics in the launch of a new initiative—the Digital Due Process Coalition. This Coalition is focused on updating ECPA to account for the profound changes in technology over the last two decades and to ensure that users' legitimate expectations of privacy are fully respected while also taking account of the needs of law enforcement. In advocating changes to ECPA, Microsoft in no way seeks to undermine the legitimate interests of law enforcement in obtaining access to electronic data in third party hands. Rather, this coalition's efforts are intended to open a dialogue with all interested stakeholders, including the government, so that we can restore the

original balance struck by Congress when ECPA was passed in 1986 between the needs of law enforcement to conduct lawful criminal and civil investigations and the rights of our citizens to have their sensitive stored communications protected against unreasonable governmental searches and seizures.

I. THE EMERGENCE OF CLOUD COMPUTING AND THE CHALLENGE OF PRIVACY INTERESTS IN THE CLOUD

We have entered a new era in computing, one in which software programs running on users' own PCs and IT systems increasingly are complemented by Internet-based cloud computing services. Microsoft has invested heavily in building a cloud infrastructure and providing cloud services because we believe they offer enormous benefits to our customers. These include greater efficiencies for organizations, including governments, to customize and rapidly scale their IT systems for their particular needs, expanded access to computational capabilities previously available only to the very largest companies, better collaboration through "anytime, anywhere" access to IT for users located around the world, and new opportunities for innovation as developers move to this new computing paradigm.

As a provider of cloud computing services, we are well situated to observe both these technological advances and user's choices and preferences for cloud services. Users care that their computing services and applications function as they expect and seamlessly interoperate with other computing services and applications. Increasingly, we are moving towards a world where users will focus less on whether their data and communications are stored and processed in a hard drive within the confines of their own networks or, instead, are accessed remotely via the Internet. We believe they do—and will continue to—care deeply about how their information is protected. In a recent poll conducted by Microsoft

and Penn, Schoen, and Berland, more than 90 percent of the general population and senior business leaders said that they were concerned about the security and privacy of personal data when they contemplated storing their own data in the cloud.[1]

While we believe there are compelling reasons for customers to take advantage of cloud-based services that will enhance the productivity of their software, we also believe that the concerns reflected in this survey should not be ignored by policymakers. The use of cloud services invariably involves the processing and storage of data on equipment that is owned or controlled by third parties. In other contexts, such as stored bank records and telephone calling information, courts have held that the disclosure of such information to third parties (e.g., banks and telephone companies, respectively) as part of using their services may diminish a user's reasonable expectation of privacy vis-à-vis the government. While the Fourth Amendment law in this area is unsettled—particularly with regard to the contents of communications held by third party services providers—such uncertainty has the potential to undermine public confidence in the adoption of cloud computing services.

In enacting ECPA almost 25 years ago, Congress moved to affirmatively address the uncertainty of the Fourth Amendment in connection with electronic communications services and computing. While the law has served us well for many years, continued advances in technology—and in particular the advent of widely available and low cost Internet-based cloud computing and storage services—call into question whether ECPA is adequate to meet our reasonable expectations of privacy today, much less in the future. This uncertainty not only may deter users from adopting cloud services and reaping their

[1] See Microsoft Poll Fact Sheet, *available at* https://www.microsoft.com/presspass/presskits/cloudpolicy/docs/PollFS.doc

benefits, but also may make businesses and other entities hesitate for fear that both their own information and that of their customers will enjoy less protection against government access than if they store the data locally. Put simply, the full benefits of cloud computing, which we believe will foster the development of innovative, job creating business models, will not be realized if users fear that data they create or store in the cloud is less private and secure than data they create or store locally.

The absence of a clear legal framework also can impact the competitiveness of online services offered by U.S. companies. It has become clear to us that foreign users—and particularly foreign enterprises—may be reluctant to use online services offered by U.S. companies for fear that data processed or stored with such services will be subject to less or uncertain protection under American law. Although a multilateral framework for law enforcement access to data in the cloud is beyond the scope of this hearing, clarifying our own laws by amending ECPA would be an important step in the right direction.

II. SUPPORT FOR ECPA REFORM

To address the uncertainty in the current scope of Fourth Amendment protection in the online world and to give potential users of cloud computing confidence that they will not suffer a loss of privacy by moving data to the cloud, we urge Congress to reform ECPA. At its inception, ECPA was intended to create a balance among the rights of individuals, the burdens on service providers, and the legitimate needs of law enforcement with respect to data shared or stored in various types of electronic and telecommunications services. ECPA grants certain protections to user data when it is transferred across or stored in such systems and establishes rules that law enforcement must follow before they can access that

data. Depending on the type of customer information involved and the type of service being provided, the process law enforcement must obtain in order to require disclosure by a third party will range from a simple subpoena to a search warrant based upon probable cause.

This framework made sense when it was adopted in 1986. However, in the intervening decades, the balance has shifted between the equities of users and law enforcement. This shift did not result from any policy decision by the Congress; rather, it resulted from technological advancements the effect of which has been to put more sensitive personal information of individuals within the reach of law enforcement tools that require a lower burden of proof.

Quite simply, the basic technological assumptions upon which the Act was based and the nature of the protection afforded to stored electronic communications have not kept pace with the many innovations in online computing over the last 25 years. For example, ECPA extends greater privacy protections to emails stored for less than 180 days than emails stored for more than 180 days. These distinctions might have made some sense in 1986, when email services did not automatically retain messages for long periods of time. But that distinction no longer bears any relationship to reality. Hosted email and other online services regularly store emails and gigabytes of other user-generated content for years, and users today reasonably expect these communications to remain just as private on day 181 as on day 179.

Because ECPA has been overtaken by technological change, Microsoft supports the Digital Due Process Coalition's ("DDP Coalition") efforts to modernize ECPA. In particular,

Microsoft supports changes that will ensure that individuals and businesses do not suffer a decrease in their level of privacy protection when they move data from on-premises computers to the cloud.

In recommending these changes, Microsoft also recognizes the legitimate needs of government investigators in obtaining access to data in the cloud. We spend significant resources every year working with and training law enforcement officers, agents, and prosecutors at the federal, state, and local government level. The Digital Crimes Unit that I oversee was created to assist law enforcement with its work and provides training to prosecutors and investigators around the world. We understand the importance of supporting lawful investigations. And, we remain committed to responding to emergency requests for assistance in matters where death or serious bodily injury are threatened even without being compelled to do so; the DDP Coalition's proposal would in no way threaten this cooperation.

Microsoft is not seeking special privacy protection for data in the cloud. Rather, we support focused, targeted changes to ensure that users enjoy the same level of privacy protection over data they store in the cloud as they currently enjoy when they store data locally. It is true that some actions that government agencies can take today under ECPA to gain access to information in third party hands might no longer be possible under the changes proposed by the DDP Coalition. Nothing in the DDP's proposals would, however, limit the government's power to compel the production of information directly from its owner. Moreover, the changes would rectify important inconsistencies in how the law is applied to user data and communications and would seek to create a modern set of clear and balanced rules to regulate government access to private data and communications in

third party hands. Moreover, we think that decisions about where the right balance lies should be made consciously by lawmakers after an open dialogue about the issues rather than as a result of unanticipated shifts in technology. Microsoft hopes the DDP Coalition proposal will serve as a helpful starting point for that dialogue with all stakeholders, including law enforcement.

III. CONCLUSION

Updating America's privacy laws as they apply to the online environment is a worthy and crucial objective. Microsoft believes that ECPA can be reformed in such a way that consumers will feel confident in the privacy of their data stored in the cloud without compromising the legitimate interests of government agencies in obtaining access to information necessary to carry out their law enforcement responsibilities. By responsibly reforming ECPA, we can restore the balance between the rights of individuals, the obligations of service providers, and the needs of law enforcement that motivated Congress to pass ECPA in 1986. This will help cloud computing fully deliver on its promise of increased efficiency, cost savings, and innovation to governments, businesses, and individual users alike.

Thank you for giving us the opportunity to testify today. We look forward to working with you on this important issue.

Mr. NADLER. Thank you.

The witnesses having completed their initial statements, we will turn to questions. And I will begin by recognizing myself for 5 minutes.

Mr. Dempsey, are any of the Digital Due Process principles intended to change a service provider's ability to share information with law enforcement in an emergency?

Mr. DEMPSEY. Absolutely not. We make it clear that there are emergency exceptions in the law right now, which permit disclosure of information without a warrant, without a subpoena, in emergency circumstances, and we would leave those untouched.

Mr. NADLER. Thank you.

Ms. Levins, you indicated in your testimony that ECPA relies on outdated notions of how individuals and businesses interact with information technology. I assume among other things you are talking about—well, we know you are talking about cloud computing, because you mentioned it specifically.

Can you tell us more about cloud computing and why this technology is "transformative?" And what benefits does it offer to society? And how do we support such technological progress as we attempt to balance the interests of privacy and law enforcement? All in about 5 minutes.

Ms. LEVINS. Thank you, Mr. Chairman. I would be happy to address that.

Cloud computing is important, because it opens the door for everyone to use the most powerful computer capabilities there are. It used to be that you couldn't afford to buy that kind of computing capability and storage unless you were a big company, but now you can use your desktop, your laptop, and use storage facilities that are maintained by a third party to do that kind of computing and storage that was previously unavailable on your home network.

Mr. NADLER. Storage or storage and computing capacity?

Ms. LEVINS. Both.

Mr. NADLER. Both.

Ms. LEVINS. Both.

So that is the first part. I mean, and I think that that opens doors to all kinds of businesses to expand the way they do business in ways that weren't even thinkable when ECPA was passed in 1986.

Mr. NADLER. And what do you think the implications for the development of cloud computing are if government access to e-mail content stored in the cloud continues to be subject to a legal standard different from that applied to other forms of data storage?

Ms. LEVINS. And I think that is a critical question, because what we found and what our poll showed is that people are very concerned that by putting data in the cloud, are they going to have the same level of privacy and security that they would have if they maintained it within their own four walls of their company or home. I think that they will be reluctant to move to the cloud and take advantage of this opportunity, if they aren't assured of what the standard of that privacy is and it doesn't meet their reasonable expectations.

Mr. NADLER. So we have to make sure that there is a standard of privacy equal to what they would be on your own personal hard drive, or just a certainty of letting people know at some other level?

Ms. LEVINS. Well, certainty is important, but I think in fact if you are talking about content, people expect that what they would have on their hard drive, in their personal hard drive, should be

protected in the same way. Put the other way, the information in the cloud should be protected in the same way that their——

Mr. NADLER. And to the same legal standard.

Ms. LEVINS [continuing]. Hard drive would. And that is particularly true, I think, of corporations, I would guess.

Mr. NADLER. Now, but the importance of maintaining privacy in the cloud is what you just said, but we have to maintain security in the cloud, too. How do you balance them?

Ms. LEVINS. Well, I don't think they are inconsistent. And Microsoft, for example, has taken lots of steps to make sure that we have the best security that we can, and we are constantly working toward meeting the highest standards that are recognized in the industry.

We think one of the most important things that could happen in this area is to have greater transparency about the security practices that companies offering cloud services are adopting and using. So it goes hand-in-hand with privacy. Users want to know that their information is safe, and they want to know that it is being secured and their privacy is being secured.

Mr. NADLER. Thank you.

Professor Gidari—Mr. Gidari—you indicated in your testimony with respect to location-based information that there has been a magistrate's revolt for several years. Can you describe what you mean by this phrase and in what ways, if any, it has been fomented by the government's interpretation of ECPA?

Mr. GIDARI. Yes, Mr. Chairman.

Over the last 3 or 4 years, a number of magistrates have objected to automatically approving, as part of pen register orders, requests to disclose the location of a cell phone in real time prospectively on an ongoing basis. They objected to using the pen register standard alone or in combination with what is known as a specific and articulable facts order, or as the government calls it, a hybrid order, to authorize that disclosure.

Other magistrates disagree and believe that the standard is acceptable. But about three to one ratio, these magistrates have believed that a probable cause standard is necessary to track and follow an individual.

And that mini revolt, if you will, has resulted in very inconsistent standards within judicial districts, as a magistrate sitting next to another magistrate could completely disagree, and have disagreed, issuing orders that have different standards. So one person might be tracked according to one standard, another one to a higher standard. And then within the states themselves, the ECPA, of course, that is the floor.

Mr. NADLER. But you would get that in any event. Even if we wrote a standard in law, a more specific standard, you would get judges disagreeing with that, and until it went up to the circuit or Supreme Court, you would have judges sitting next to each other issuing different decisions, no?

Mr. GIDARI. You certainly would, from a service providers' perspective. Which rule applies? Which order should pertain? What responsibilities do they have to their users to object to that order? The rules for location information today just simply don't state under——

Mr. NADLER. They should state it more specifically.

Mr. GIDARI. Absolutely.

Mr. NADLER. Mr. Dempsey, you look like you wanted to comment on that.

Mr. DEMPSEY. I am just saying that right now you sort of have an open field, a green field—sort of no guidance at all.

Mr. NADLER. So we need statutory guidance.

Mr. DEMPSEY. The statute would—we would try to make it as specific as possible and precise as possible, but at least it would provide some context within which the courts would operate.

Mr. NADLER. Okay. Thank you.

My final question is to Professor Kerr. In some of your recent scholarship in applying the Fourth Amendment to the Internet, you talk about replacing the inside-outside distinction common to Fourth Amendment jurisprudence with the content-noncontent distinction.

Can you tell us what this means and how you believe it extends consistent application of the Fourth Amendment principle to cyberspace? And is the analogy perfect, or does it give rise to any notable exceptions we should be aware of?

Mr. KERR. The basic idea here is when courts are considering how to apply the Fourth Amendment, which was created for a physical space, to a network environment, they should think about how to create a set of rules that tries to replicate how the Fourth Amendment applies in the physical world to this network space. And the basic idea is that the contents of some of these communications, these actual messages, are the online equivalent of stuff that would happen inside and would be protected by the Fourth Amendment in the physical world.

On the other hand, the non-content information that a network creates is essentially the online equivalent to transactional information that would have occurred outside in the physical world. Now, if you follow that idea, the basic idea is that networks are doing for us what we used to do in the physical world. Basically, the network is coming to us instead of us having to go out into the world. And the idea is it creates a rough parallel between how the Fourth Amendment should apply in the physical world and how the Fourth Amendment should apply in the Internet.

Now, of course, it is just a Law Review article. We don't know whether courts are ever going to follow this. And in fact, there is a Supreme Court case right now, Quon versus City of Ontario, in which the Supreme Court is trying to figure out for the first time how does the Fourth Amendment apply to text messages. I went to the oral argument, and the justices were as puzzled about this question as anyone could be.

So we are just trying to figure out these issues, and the idea that content-noncontent distinction is just an initial first start to try to figure out how the Fourth Amendment should apply, and by analogy, how the statute could be drafted to recognize the stronger protection for content and for noncontent.

Mr. NADLER. Thank you very much.

My time has expired. I will now recognize the distinguished gentleman from North Carolina.

Mr. WATT. Thank you, Mr. Chairman.

I think I will acknowledge at the outset how ill prepared technologically I feel to engage in this discussion, and ill prepared, yes. I feel like a Neanderthal in this area. So let me—I want to ask a couple of questions that—and then I just want somebody to give me some examples of the kinds of things that are going out there that we should be worried about, given the failure to update the statute. But let me talk about process first.

Mr. Dempsey, you talked in your testimony about a long period of dialogue and consensus building being needed.

Mr. Gidari, you seemed to suggest, although not explicitly, that clarity was more important than substance of where you get to, so I am trying to figure out how long we should be working on this before we get to some kind of legislative solution. Is clarity of a rule more important than getting the rule right, the new standard right?

What kind of time are you talking about for dialogue and consensus building, Mr. Dempsey, and does that fit with your urgency for clarity, even if the clear standard is the wrong standard?

Mr. DEMPSEY. Well, honestly, I think, you know, my own timeframe is if a year from now we could be here with that piece of legislation that would be, you know, a markup or something a year from now would be a good target. But I think it is going to take a while. We are not pushing, as I said, for introduction of legislation immediately.

I think we do have, and as we go through this process here, we do have some touchstones, and we can think about some of the analogies. They only take you so far, but they help. Take what we are talking about in terms of cloud computing. If you have a document on your computer in your office, or if you have that document printed out, that is protected by the Fourth Amendment—a person's house, his papers and effects. I think nobody has any doubt that "papers" includes your laptop.

If, however, as now—and by the way, if you——

Mr. WATT. Wait a minute, now. You are going to take my whole 5 minutes talking about something that I am trying to find—you say a year from now, and I—let me give——

Mr. DEMPSEY. Okay, but I do want to come back to the question here of what are the guideposts we have that get us both the clarity and the substance.

Mr. WATT. I am just talking about the timeframe now. I am not even talking about what the content is. Is a year from now too long from a clarity perspective, Mr. Gidari?

Mr. GIDARI. I think lawyers will find ambiguity in a No Smoking sign for the rest of our lives, but if that is the case, fix it, fix it right. If it takes a little longer to do that, we would rather have it right than wrong. But that doesn't mean they are inconsistent.

Mr. WATT. So the real question I am trying to get to is what risk do we run in this interim? And that is where I get to the second part of the question. I mean, what are the horror stories that are going on out there? I mean, give me a couple of concrete horror stories that is going on in this interim while we are trying to either build consensus or get the standard right.

Mr. DEMPSEY. Well, here is one example. Every one of us probably has 5, 6, maybe 10 years worth of e-mail stored, either stored

on our local computer or often stored with a service provider like MSN or Gmail or another provider.

Mr. WATT. That is somewhere in a cloud stored.

Mr. DEMPSEY. That data is stored on a remote——

Mr. WATT. Which I had never heard of until today, but that is all right.

Mr. DEMPSEY. We are talking here just about, you know, when people used to draw a picture with a computer over here and a computer over here and then a cloud in the middle, that Internet server is in the cloud.

Mr. WATT. I get the concept.

Mr. DEMPSEY. And that is where a lot of our data is going.

The way ECPA now works, it says that that e-mail 180 days old or less is protected by the Fourth Amendment warrant standard. The minute it turns 180 days old, it is available with a mere subpoena issued without judicial approval.

The Justice Department takes the position that the minute that e-mail is opened at all—in fact, from the sender's perspective, the minute it is sent, it loses its warrant protection. Fully protected passing over the wire, the minute it reaches—you finish sending it or the minute the user, the intended recipient, opens it and looks at it, it falls outside of the protection of the warrant.

Same document, if you print it out, leave it on your desk, protected. Same document, you put it in a box and you lock it in one of those storage lockers out in the suburbs, protected by the Fourth Amendment. But locked up in the cloud, not protected by that requirement.

In the Ninth Circuit, the Ninth Circuit has rejected the Justice Department view and has said that a warrant is required. So what happens now is if the warrant is subject to the jurisdiction or the subpoena is subject to the jurisdiction of the Ninth Circuit, it is rejected, and a warrant is required. If it is outside of that, it is a little unclear.

In Colorado a month ago the Justice Department sought e-mail without a warrant. Yahoo said, "No, go get a warrant, even though we are outside of the Ninth Circuit." The Justice Department backed down, said okay, withdrew the request.

That is the kind of uncertainty you are getting. And there is overarching it all the possibility that these cases will percolate up through the courts and that the statute will be held unconstitutional, if the Justice Department pushes its position.

Mr. WATT. Because it is too vague?

Mr. DEMPSEY. No, because the warrant is not. Where the statute currently permits access without a warrant, if Professor Kerr is right that a warrant is required, that content is like a letter, it is like a phone call, it should be protected, so you do run that constitutional risk.

I still agree with Mr. Gidari and my initial statement that, you know, we have lived with that ambiguity now for 5, 10 years. I just don't see how we are going to push this forward. Given the law of unintended consequences, we want to make sure we don't screw things up worse.

Mr. WATT. Thank you.

I am way over my time, so I will yield back.

Mr. NADLER. In that case, we will recognize the gentleman from Virginia for 5 minutes.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. Dempsey, it seems to me that a person doesn't think any different about an e-mail as saved in the cloud as on the computer. Why would the e-mail in the cloud be any different than the e-mail stored in that storage bin in the suburbs that you talked about?

Mr. DEMPSEY. I don't think it should, and the conclusion that we came to in our preliminary dialogue is that it shouldn't.

If you go back to 1986, I think what you end up with is this was a distinction based upon the way the technology worked in 1986. Storage was expensive, and service providers did not store e-mail. If you go back to the early days of AOL, you read that, you downloaded it, it was deleted from the computer of the service provider.

Congress thought 180 days would be the absolute conceivable outside limit, and after that it was sort of like abandoned property or a——

Mr. SCOTT. Well, once it gets into the cloud, can anybody get access to it?

Mr. DEMPSEY. The——

Mr. SCOTT. I mean, beside—I mean, could I look into Representative Watts' cloud?

Mr. DEMPSEY. No, no, no, no. It really is—the cloud actually is potentially more secure in some ways than local storage. You have the service providers of cloud storage capabilities making a lot of effort to secure that information.

Mr. SCOTT. So this is being kept in a place that is secure from anybody else, and it is just I am the only one that can access my part of this cloud.

Mr. DEMPSEY. You or the person to whom you give consent.

Mr. SCOTT. And so I have an expectation that this is private information.

Mr. DEMPSEY. That is certainly the way the average person looks at it. That is one of these changes that has occurred, the technology changes that have occurred in the past 10 years that we are talking about.

Mr. SCOTT. Ms. Levins, when Microsoft has to respond to a lot of warrants and subpoenas, it costs money. Does the government incur any of the expense, or they just let you worry about it?

Ms. LEVINS. Congressman Scott, that is not my area of expertise. I would have to get back to you with that information. I know my colleagues do know that. I don't have that with me.

Mr. SCOTT. Does anybody know who—what——

Mr. GIDARI. The statute authorizes reimbursement for non-toll records, so phone companies give them away for free in large amounts, but electronic communication service providers are entitled to charge for them. Not all of them do. Many provide that service to law enforcement for free. Others charge a reasonable cost.

Mr. SCOTT. But some information can be obtained fairly easily. Some takes a little complication where you have to program the computer and pay expenses to get the information, and some of it, I imagine, gets kind of expensive after a while.

Mr. GIDARI. That is right.

Mr. SCOTT. And you can charge for that expense?

Mr. GIDARI. That is correct.

Mr. SCOTT. Does anybody have any concern, if we keep talking about how government does all this surveillance, that we might publicize their techniques and compromise investigations?

Mr. DEMPSEY. I have always thought that we could have the discussion without compromising techniques. I think we can talk at the level of specificity necessary to draft a clear statute, incorporate the Fourth Amendment principles, and do that in a way that doesn't get into the technology at all. In fact, technology neutrality, I think, is one of the principles that we are trying to achieve here.

Mr. SCOTT. Okay.

And with the pinging the cell phone, can anybody ping somebody else's cell phone, or is that just something the company can do?

Mr. GIDARI. Something only the company can do.

Mr. SCOTT. And I think there is an expectation that you are not being followed, because the company isn't supposed to be following you around, and the only way the government can do it is—what does the government need to order the company to find out where you are?

Mr. GIDARI. Depends on which magistrate you visit, but at least a pen register order and a specific and articulable facts order combined, but in many jurisdictions, a probable cause order—a probable cause warrant issued under Rule 41.

Mr. SCOTT. But for a government request, I should have an expectation that I am not being pinged and shown up on somebody's computer screen. Is that a reasonable expectation, or, you know, should——

Mr. GIDARI. It is more than a reasonable expectation.

Mr. DEMPSEY. And that is the way I think that carriers have designed their services. A number of carriers offer services whereby parents, for example, can—who are the subscribers to the service—can find out, for example, where their children are. But that is the case of the subscriber controlling their account.

There are a variety of services now being offered where I can share my location with my friends. The companies who have designed those services have been very, very careful to design them in a way so that the user has control. To override that user control, the company has to be involved. The company has to be compelled to do something.

And some of those services offer very, very precise location capability, in a sense almost pinpointing a person on a map. A number of those companies have said that they will insist upon a warrant for disclosure of that information, and I think they have strong constitutional argument for that. But the statute, as we have said, it is completely unclear.

Mr. NADLER. Thank you.

I now recognize the gentleman from Georgia.

Mr. JOHNSON. Thank you, Mr. Chairman.

If I were someone's wife, and I was out on the town running around with all kinds of males and females and engaged in doing my own thing pretty much, and I am wanting to keep all of that secret, I am certain that no one on the panel would want the husband of—or they would not want my husband to be able to go to

the phone company and say, "Look, I need to find out where my wife is, because I am going to kill her when I find her." None of you all would want that to happen, would you?

And so no one is saying anything, so I assume——

Mr. DEMPSEY. No.

Mr. JOHNSON. Okay. All right.

And now, what if I were a law enforcement officer—the husband. Or what if my husband was a law enforcement officer? Is there any—and only thing this law enforcement officer did was to go get a subpoena, which he carries around blank subpoenas, and comes to a cell phone provider and says, "Look, I am conducting an investigation, and you must provide this information to me." Should that law enforcement officer, or any other law enforcement officer, be able to obtain that information, the whereabouts of his wife?

Mr. GIDARI. They would be shown the door with that request, the door to the courthouse, where they would have to ask a judge to approve an order to get it.

Mr. JOHNSON. But that may be true at your cell phone company, but it is not necessarily compelled by law that the cell phone company refrain from producing those documents. Is that correct?

Mr. DEMPSEY. Congressman, there is actually an interesting case that has emerged in the 11th Circuit recently, which dealt not with the location information, but instead with some e-mails.

And the case clearly involved a certain amount of favoritism on the part of the prosecutor and the sheriff in that area, who at least allegedly were doing a favor for a friend in defending that friend against some civil litigation or some civil controversy, issued a subpoena, like you say, served the subpoena on the service provider, and the service provider did turn over that e-mail.

The case has gone up to the 11th Circuit, and unfortunately, this is one of the cases that I think went in the wrong direction. Professor Kerr has also written about it, criticizing the decision in this case, but the 11th Circuit held that there was zero constitutional privacy interest in that e-mail and that the sheriff and the prosecutor, in essence acting off on their own, had not violated anybody's rights.

Mr. JOHNSON. So, and the reason why it was not private is because it was in the cloud somewhere?

Mr. DEMPSEY. Yes, there was this notion that they had, which we think is wrong, that privacy was lost because of the use of that technology.

Mr. JOHNSON. Yes.

Is there anybody who would agree with the 11th Circuit decision in that case that is sitting on this panel?

Yes, okay. All right. Well, you know, I have been sitting here all day trying to find something that someone on the panel would say that would incite me to issue forth with tough questions, but you all have deprived me of that option, and I am pretty much, I guess, singing to the choir when I say that I would hate to see either with content or with noncontent information requested by law enforcement, to use your analogy, Mr. Kerr—or not your analogy, but your terminology, I would hate to see a company turned into a agent for law enforcement at the expense of their customer.

To me the issues that we confront are easily dealt with by legislatively extending the Fourth Amendment. And I do believe that there is an inherent right to privacy, which is implied in really the first nine amendments, but certainly the Fourth Amendment. All we have to do is just extend it to these new areas that have come to the fore since we have been embarked on this pursuit of intellectual supremacy, if you will.

This is just human nature, but if we stick with the ideals of the founding fathers, particularly with respect to the Fourth Amendment, I think that our job should be easy.

And I guess there could be an argument that we just leave each case up to the the courts to flesh out and ultimately to the U.S. Supreme Court, but I am afraid that we would—I am afraid to leave it up to the U.S. Supreme Court when we can put those things into legislation, which clears up the ambiguities that may arise.

So I think this is a very important hearing. It bears upon the individual rights that we in this country oftentimes take for granted, but they are what made America what it is. So thank you very much.

And I notice that the Chairman is now thinking about—thinking pensively as we proceed.

Mr. NADLER. And you yield back?

Mr. JOHNSON. At this time, yes.

Mr. NADLER. Then I will recognize the gentlelady from California.

Ms. CHU. So, Mr. Dempsey, I would like to ask a question about the fate of an e-mail that I would send out, but under different circumstances with regard to privacy and the Fourth Amendment.

Let us just say I e-mail a friend, Sarah, and what would happen to the fate of that e-mail if she has read it versus hasn't read it or with regard to if 8 months have passed versus tomorrow, whether it is on a Gmail account or whether it is on her hard drive? Or what if I took the content of that information and put it in a letter and just mailed it?

Mr. DEMPSEY. In the Appendix A to my testimony, I talk about this example, and if I was better at graphics, I would have tried to it do a chart that showed this, because it really does almost take a matrix to explain this.

While the e-mail is in transit, moving over the wires, so to speak, or moving through the network, it can be intercepted only with a warrant, a wiretap order issued under the Wiretap Act.

Once it reaches the inbox, so to speak, the computer of the service provider of Sarah, the intended recipient, it comes under the Stored Communications Act and at least until she opens it, that e-mail sitting in her e-mail box is protected again by the warrant requirement.

After she reads it, under my reading of ECPA, for 180 days it remains protected by the warrant requirement. After 180 days, on day 181, it loses the warrant protection. So you go from warrant to non-warrant.

An interesting example is if you are using Gmail, by the way, and you—or any other remote Web-based e-mail service—and you draft your e-mail and don't send it, because you haven't finished it,

you are going to come back the next and finish it and send it, while that e-mail is sitting on the server of Google, it is available regardless of age.

It is available with a mere subpoena. It is not protected by the warrant at all, because Google is at that time acting as a provider of remote computing services, not as a provider of electronic communication services. They are storing the e-mail.

Once 180 days passes, then Google again reverts to its status as a remote computing service. It is available with the subpoena. The Justice Department argues that the copy of the e-mail that you might store, since you store all your outgoing e-mail, if it is stored in the cloud, loses its protection as soon as you send it, because it is no longer in transit in temporary storage incident to transmission. It is sort of your copy.

Now if you had printed out a copy and kept a copy in your office, that is protected by the Fourth Amendment. If you have a copy on your desktop or laptop, that is protected by the Fourth Amendment. But the copy that is stored in your account, according to the Justice Department, from the minute you push "send," that is not protected by the warrant.

Mr. NADLER. Will the gentlelady yield for a moment?

Ms. CHU. Yes.

Mr. NADLER. And the Justice Department in effect is saying that because you pressed the "send" button, the Fourth Amendment doesn't apply, because it is no longer your papers?

Mr. DEMPSEY. It applies only—I think everybody would admit that it applies to the e-mail in transit.

Mr. NADLER. But why doesn't it apply continuing?

Mr. DEMPSEY. They argue, I think, that it is—it is hard to articulate their theory. It is a stored record, in their opinion, that has been entrusted to a third-party in such a way that you have surrendered your privacy interest in it.

Now, I think the correct analogy is the storage locker analogy, in which a warrant is required to go into the storage locker. There are cases having—they analogize it to something like a check, a cancelled check which goes to the bank.

Mr. NADLER. That is even more strange, when they say that it is not protected by the Fourth Amendment before you finished it.

Mr. DEMPSEY. If you store it with some—if you leave it on some remote server.

Mr. NADLER. I thank the gentlelady for yielding.

Ms. CHU. And so if you have it on the hard drive, it is protected, but if it is in the cloud, it is not protected. And if it is a letter, I am presuming you are saying it is protected.

Mr. DEMPSEY. The letter is interesting, because the letter is protected, of course, in the hands of the post office. This goes back to 1877, when the Supreme Court ruled that the Fourth Amendment does protect the letter moving through the mail system. The copy of the letter that I retained is protected. The copy of the letter that the recipient has is protected vis-a-vis the recipient. They can always voluntarily turn it over, but to force them to disclose it would require a warrant or subpoena served directly on them.

So you have got this crazy quilt that the average individual has absolutely no idea about. And increasingly, the services are being

designed in a way to make all this completely seamless and completely non-apparent to the user.

So we have these increasingly powerful Black Berries and handheld mobile Internet devices. We are constantly accessing information remotely. Sometimes it is on the device. Sometimes it isn't. Increasingly, it becomes even less clear where it is. And it is time to dispense with these technology-based, platform-based rules by which people do not lead their lives, people do not base their lives on these distinctions from 1986.

Ms. CHU. Thank you.

I yield back.

Mr. NADLER. I thank the members of the panel, unless any member of the panel wants to say anything else.

In which case without objection, all Members will have 5 legislative days to submit to the Chair additional written questions for the witnesses, which we will forward and ask the witnesses to respond as promptly as they can so 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.

Mr. Dempsey, you wanted to make a statement.

Mr. DEMPSEY. Yes, Mr. Chairman. Sorry, I did have one thing. I have a very good memo that was prepared by Becky Burr at the WilmerHale law firm, talking about some of these issues, and I would like to, with your permission, enter this into the record of the hearing as well.

Mr. NADLER. Well, if you will give it to us, without objection, it will certainly be entered into the record, and I thank you.

[The information referred to follows:]

The Electronic Communications Privacy Act of 1986: Principles for Reform

J. Beckwith Burr[1]

Background

Congressional enactment of the Electronic Privacy Information Act (ECPA)[2] in 1986 was a remarkably forward-looking effort to govern the compelled disclosure of electronic communications data to the government by balancing law enforcement needs with the personal privacy safeguards needed in the digital age.[3] As communications technology developed, and its contribution to the U.S. economy became clear, Congress also consciously endeavored to find a balance that would nurture communications technologies.[4] The wisdom of this attempt to balance privacy rights and law enforcement needs in an innovation-friendly environment is evident today: the Internet has evolved from a research network with a few thousand academic hosts into a global platform for communications, commerce, and civic activity used by four out of five adults in the United States on a daily basis.[5] Information technology has driven the U.S.

---

1 J. Beckwith Burr is a partner at Wilmer Cutler Pickering Hale and Dorr, LLP, and a member of the firm's Regulatory and Government Affairs Department, based in Washington, D.C.

2 The term "ECPA" is used in this paper to describe both Title I of the Electronic Communications Privacy Act, which protects wire, oral, and electronic communications in transit, as well as Title II, referred to as the Stored Communications Act, which protects communication held in electronic storage.

3 The stated goal of ECPA was to preserve "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement." House Committee on the Judiciary, Electronic Communications Privacy Act of 1986, H. Rep. No. 99-647, 99th Cong. 2d Sess. 2, at 19 (1986).

4 In addition to the goals of privacy and law enforcement, ECPA sought to advance the goal of supporting the development and use of these new technologies and services. *See* S. Rep. No. 99-541, at 5 (noting that legal uncertainty over the privacy status of new forms of communications "may unnecessarily discourage potential customers from using innovative communications systems"). It was the intent of Congress to encourage the proliferation of new communications technologies, but it recognized that consumers would not trust new technologies if the privacy of those using them was not protected. *Id.*; H.R. Rep. No. 99-647, at 19 (1986).

5 Pew Internet & American Life Project: *Wireless Internet Use*, at 8 (July 2009) , *available at* http://www.pewinternet.org/~/media//Files/Reports/2009/Wireless-Internet-Use.pdf

economy in the past two decades,[6/] and is expected to remain the engine of growth for years to come.[7/]

As forward-looking as ECPA was in 1986, there is broad consensus that today's technology has outpaced the Act. In 1983, Apple Computer introduced the "Lisa"—the first mass-marketed microcomputer with a graphical user interface. The Lisa cost $10,000 and featured 1 megabyte of RAM and a 5 megabyte hard drive.[8/] Today, for $999, consumers can purchase a Mac Book with 2 gigabytes of memory, a 250 gigabyte hard drive, and built in wireless Internet access and communications technology.[9/] In 1995—nearly a decade *after* Congress enacted ECPA—only 9% of American adults used the Internet, compared to 81% today.[10/] Prototype mobile telephones from the 1980s—the size and shape of "bricks"—are now

---

6/ *See* Robert D. Atkinson & Andrew S. McKay, *Information Technology & Innovation Foundation, Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution* at 11-14 (March 2007) ("[T]he mid-1990s were a turning point that marked the move from the sluggish U.S. economy of the 1970s, 1980s, and early 1990s to the dynamo of the last decade… [T]here is a now a strong consensus among economists that the IT revolution was and continues to be responsible for the lion's share of the post '95 rebound in productivity growth.").

7/ *See id.* at 53 ("It is not clear how long IT will power growth, but it seems likely that for a[t] least the next decade or two IT will remain the engine of growth. The opportunities for continued diffusion and growth of the IT system appear to be strong. Many sectors, such as health care, education, and government, have only begun to tap the benefits of IT-driven transformation. Adoption rates of e-commerce for most consumers, while rapid, are still relatively low. And new technologies (*e.g.*, RFID, wireless broadband, voice recognition) keep emerging that will enable new applications. In short, while the emerging digital economy has produced enormous benefits, the best is yet to come. The job of policymakers in developed and developing nations alike, is to ensure that the policies and programs they put in place spur digital transformation so that all their citizens can fully benefit from robust rates of growth.").

According to the Bureau of Labor Statistics, "Two of the fastest growing detailed occupations are in the computer specialist occupational group. Network systems and data communications analysts are projected to be the second-fastest-growing occupation in the economy. Demand for these workers will increase as organizations continue to upgrade their information technology capacity and incorporate the newest technologies. The growing reliance on wireless networks will result in a need for more network systems and data communications analysts as well. Computer applications software engineers also are expected to grow rapidly from 2008 to 2018. Expanding Internet technologies have spurred demand for these workers, who can develop Internet, intranet, and Web applications." *Occupational Outlook Handbook: 2010-2011 Edition, available at* http://www.bls.gov/oco/oco2003.htm.

8/ Lisa/Lisa 2/Mac XL, *available at* http://www.apple-history.com/lisa.html.

9/ Apple—MacBook: Technical Specifications, *available at* http://www.apple.com/macbook/specs.html (last visited Feb 2010).

10/ Harris Interactive. The Harris Poll, *available at* http://www.harrisinteractive.com/harris_poll/index.asp?PID=973.

collector's items on eBay,[11] while in 2009 palm-sized smart phones[12] double as sophisticated computing platforms with the potential to bridge the digital divide.[13] Communications technology in the United States is evolving—and will continue to evolve—more rapidly and in more directions than we currently imagine. ECPA, which served us remarkably well for many years, is today unwieldy and unreliable as a law enforcement tool, immensely difficult for judges and investigators to apply, confusing, costly, and full of legal uncertainty for communications and other technology tools and service providers, and an unpredictable guardian of our country's long cherished privacy values.

A coalition of communications, equipment, and online services, as well as members of the legal and advocacy communities[14] have come together over the last year with the goal of developing a set of principles to simplify, clarify, and unify ECPA—without constraining important law enforcement activities. The result of this effort is a set of consensus principles for updating ECPA that are designed to:

- **Establish consistent, predictable privacy protections** for communications and other electronic information services used by Americans every day to handle their personal communications and operate their businesses — building user trust and supporting the full extension of Constitutional values to the networked world, while providing clarity for law enforcement and service providers.
- **Achieve technologically neutral solutions** and avoid arbitrary distinctions that become hard to apply over time, inhibit innovation, and skew the Internet marketplace.

---

[11] For example, Motorola's Dynatax 8000x was the first cell phone to receive FCC approval (in 1983). It weighed 28 ounces and was 10 inches high, not including its flexible "rubber duck" whip antenna. *Available at* http://www.retrowow.co.uk/retro_collectibles/80s/motorola_8000X.php.

[12] For example, the Google Nexus One is less than 5 inches tall and weighs less than 5 ounces. *Available at* http://www.google.com/phone/static/en_US-nexusone_tech_specs.html.

[13] According to the Pew Internet & American Life Project, lower levels of home broadband access coupled with lower levels of desktop and laptop computers explains the traditional access gap between white and black Americans. But the gap in online engagement "largely dissipates" according to Pew, when access on handheld and mobile devices is considered: under those circumstances, "use among African Americans matches or exceeds that of white Americans. Two measures of engagement with the wireless online—accessing the [I]nternet on a handheld on the typical day or ever—shows that Africans Americans are *70% more likely* to do this than white Americans." The report concludes, "To an extent notably greater than that for whites, wireless access for African Americans serves as a substitute for a missing onramp to the Internet—the home broadband connection." Pew Internet & American Life Project: *Wireless Internet Use*, at 32-35 (July 2009), *available at* http://www.pewinternet.org/~/media//Files/Reports/2009/Wireless-Internet-Use.pdf (emphasis in original).

[14] Coalition members currently include: American Civil Liberties Union, AT&T, Center for Democracy and Technology, Electronic Frontier Foundation, Google, Microsoft, IBM, Net Coalition, Loopt, and Salesforce.com.

- **Preserve the legal tools necessary to conduct criminal investigations and protect the public**, including through preservation of the ECPA exceptions and exemptions relied upon by law enforcement today.

The consensus principles reflect the working group's commitment to *change no more than strictly necessary to achieve these important goals*. Implementation of the consensus principles would not affect surveillance or privacy law relating to national security, including the Foreign Intelligence Surveillance Act and the national security letter authority in ECPA. The principles would not deny the government information needed to conduct investigations, and no information would be rendered off limits to government investigators with appropriate process. Indeed, adoption of the principles would facilitate cooperation between business and law enforcement by clarifying the rules under which the parties interact. The principles preserve all of the building blocks of criminal investigations—subpoenas, court orders, pen register/trap and trace orders, and warrants, and would carry forward ECPA's sliding scale approach that ties the level of process required to the level of investigative intrusiveness. The recommended changes would not disturb fundamental elements of ECPA, including the distinctions between content, subscriber identifying information, and less sensitive transactional data. Finally, these recommendations preserve the exceptions for compelled disclosure that have been written into ECPA over the years, including those permitting emergency disclosures.

Principles

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

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

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

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

Principle 1: Access to Content in Transit and in Storage

Recommended Approach: Under the consensus principles, a governmental entity may require the provider of wire or electronic communications services to produce the non-public content of communications only with a search warrant issued based on a showing of probable cause, regardless of the age of the communication, the means or status of its storage or the provider's access to or use of the content in its business operations. This change would bring all stored communications content under the same probable cause standard set forth in the Fourth Amendment, accessible to law enforcement with an ordinary warrant. For example, a showing of probable cause would be required to compel production of email, regardless of whether it is "opened" or not, and regardless of how old it is. The principle also would apply to documents and other private data stored by or on behalf of individuals on remote servers.[15/]

Need for Change: Americans have embraced email in their professional and personal lives and use it daily for confidential communications of a personal or business nature. Most people save these emails, just as they previously saved letters and other correspondence.[16/] In fact, many Americans now have accumulated years' worth of email, much of which is stored on the computers of trusted third-party service providers. Likewise, businesses and individuals are

---

[15/] These changes are premised on the understanding that the definition of "electronic communications" is broad enough to include such items as a draft document stored on a service such as Google Docs. We interpret the current definition of remote computing service as broad enough that it does not need to be amended to cover technologies such as cloud computing, which are expected to keep America competitive by reducing business costs, enhancing productivity, and facilitating collaboration and innovation.

[16/] Companies often impose email retention policies that require employees to preserve emails for several months before deletion. Contoural White Paper, *How Long Should Email Be Saved?*, at 5 (2007), *available at* http://www.umiacs.umd.edu/~oard/teaching/708x/spring09/11.pdf. ("Most companies come to the conclusion that many messages should be retained for a few years for business productivity purposes.").

Moreover, unlike a paper letter, often an email remains in existence long after the sender or recipient attempts to delete it. *See* Applied Discovery, at 3, *available at* http://www2.acc/chapters/program/dallas/documentretention.pdf. ("Even when a computer user intends to discard electronic data, the task is much easier said than done. The 'delete' key creates a false sense of security for many people. A deleted document may no longer be available to the user, but copies remain in temporary files, on backup tapes, and, in the case of email, in other recipients' in-boxes.")

now increasingly storing other data "in the cloud,"[17] with huge benefits in terms of productivity, cost, security, flexibility and the ability to work with collaborators around the world.[18] This data includes highly personal information such as medical and financial data, digital calendars, photographs, diaries, and correspondence.[19] It also includes commercially sensitive, proprietary and trade secret materials, such as business plans, research and development, and commercial collaboration.

The privacy rights of an individual with respect to all of this information, if stored on his or her hard-drive[20]—or indeed on a CD in a safe deposit box—would be fully protected by the warrant clause.[21] Under ECPA, however, a single email or electronic document could be subject to multiple legal standards in its lifecycle, from the moment it is being typed to the moment it is opened by the recipient or uploaded into a user's "vault" in the cloud, where it might be subject to an entirely different standard.[22] A warrant is required to access the content of an email while

---

17 "Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flow charts and diagrams." Cloud Computing Definition, *available at* http://searchcloudcomputing.techtarget.com/sDefinition/0,,sid201_gci1287881,00.html.

18 As an example of the potential savings from cloud computing, the Obama Administration's Chief Information Officer, Vivek Kundra, "pointed to a revamping of the General Services Administration's USA.gov site. Using a traditional approach to add scalability and flexibility, he said, it would have taken six months and cost the government $2.5 million a year. But by turning to a cloud computing approach, the upgrade took just a day and cost $800,000 a year." Daniel Terdiman *White House Unveils Cloud Computing Initiative*, cnet News, Sept. 15, 2009, *available at* http://news.cnet.com/8301-13772_3-10353479-52.html

19 These materials are, as one author has noted, "the same materials deemed 'highly personal' by the Supreme Court, a sentiment later echoed by the Eighth Circuit to justify Fourth Amendment protection for schoolchildren despite their otherwise diminished expectations of privacy. [They] also mirror [ ] the list of materials that the Eleventh Circuit used as a basis for asserting that 'few places outside one's home justify a greater expectation of privacy than does the briefcase.'" *See* David A. Couillard , *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 Minn. L. Rev. 2205, 2219-2220 (2009) (internal footnotes omitted).

20 *See, e.g.*, *Trulock v. Freeh*, 275 F.3d 391 (4th Cir. 2001); *United States v. Crist*, No. 1:07-cr-211, 2008 WL 4682806 (M.D. Pa. Oct. 22, 2008).

21 See, *e.g.*, *Kyllo v. United States*, 533 U.S. 27, 31 (2001) ("At the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion. With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no." (internal quotations and citations omitted)).

22 Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, at 13 (Feb. 23, 2009). "Distinctions recognized by ECPA include electronic mail in transit; electronic mail in storage for less than or more than 180 days; electronic mail in draft; opened vs. unopened electronic mail; electronic communication service; and remote computing service.... The precise characterization of an activity can make a significant difference to the protections afforded under ECPA." *Available at* http://www.scribd.com/doc/12805751/Privacy-in-Cloud-Computing-World-Privacy-Council-Feb-2009.

it is in storage waiting to be read by the recipient.[23] The nanosecond the email is opened by the recipient, however, it may lose that high standard of protection and become accessible with a subpoena, issued with no judicial intervention, with (concurrent or delayed) notice to the affected individual.[24] One Court of Appeals has rejected this distinction between opened and unopened communications for purposes of determining whether or not a communication is in "electronic storage,"[25] while in other areas of the country the question remains unsettled.[26] In all cases, the Justice Department believes law enforcement can compel disclosure of the content of the same email with a mere subpoena after the email is more than 180 days old.[27] Likewise, while as a

---

[23] 18 U.S.C. § 2703(a).

[24] 18 U.S.C. § 2703(b)(1)(B). Alternatively, it can be acquired with prior notice to the subscriber based upon a court order supported by specific and articulable facts demonstrating reasonable grounds to believe the communication is relevant to an ongoing criminal investigation. *Id.* In either case, notice to the subscriber is required unless the government secures a warrant. *Id.* The Department of Justice Computer Crimes and Intellectual Property Section argues in the 2009 edition of its Computer Search and Seizure Manual, at 123-124: "As traditionally understood, 'electronic storage' refers only to temporary storage made in the course of transmission by a service provider and to backups of such intermediate communications made by the service provider to ensure system integrity. It does not include post-transmission storage of communications. For example, email that has been received by a recipient's service provider but has not yet been accessed by the recipient is in 'electronic storage.' *See Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 461 (5th Cir. 1994). At that stage, the commnnication is stored as a temporary and intermediate measure pending the recipient's retrieval of the communication from the service provider. Once the recipient retrieves the email, however, the communication reaches its final destination. If the recipient chooses to retain a copy of the accessed communication, the copy will not be in 'temporary, intermediate storage' and is not stored incident to transmission. *See Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2003) (stating that email in post-transmission storage was not in "temporary, intermediate storage"). By the same reasoning, if the sender of an email maintains a copy of the sent email, the copy will not be in 'electronic storage.' Messages posted to an electronic 'bulletin board' or similar service are also not in 'electronic storage' because the website on which they are posted is the final destination for the information. *See Snow v. DirecTV, Inc.*, 2005 WL 1226158, at *3 (M.D. Fla. May 9, 2005), *adopted by* 2005 WL 1266435 (M.D. Fla. May 27, 2005), *aff'd on other grounds*, 450 F.3d 1314 (11th Cir. 2006). http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf.

[25] *Theofel v. Farey Jones*, 359 F.3d 1066 (9th Cir. 2004).

[26] The Department of Justice Computer Crimes and Intellectual Property Section Manual describes the holding of the Ninth Circuit in *Theofel* as follows: "[T]he court held that email messages were in 'electronic storage' regardless of whether they had been previously accessed, because it concluded that retrieved email fell within the backup portion of the definition of 'electronic storage.' *Id.* at 1075-1077. Although the Ninth Circuit did not dispute that previously accessed email was not in temporary, intermediate storage within the meaning of § 2510(17)(A), it insisted that a previously accessed email message fell within the scope of the 'backup' portion of the definition of 'electronic storage,' because such a message "functions as a 'backup' for the user." *Id.* at 1075. The discomfort of some courts with the Justice Department's interpretation of the Stored Communications Act is evident in the Sixth Circuit's (now vacated) ruling in *Warshak v. United States* that "individuals maintain a reasonable expectation of privacy in emails that are stored with, or sent or received through, a commercial ISP." 532 F.3d 521, 536-537 (6th Cir. 2008). Specifically, the panel court upheld a preliminary injunction enjoining the government from "seizing the contents of a personal e-mail account" under 18 U.S.C. § 2703(d) unless the government provides prior notice to the e-mail user or shows that the e-mail user had no reasonable expectation of privacy vis-à-vis the e-mail service provider.

[27] *See* DOJ, *Electronic Surveillance Manual*, at 25 (2005), *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf.

practical matter law enforcement must secure a warrant to access documents on a personal computer, under ECPA, a mere subpoena issued to a third party will suffice to access confidential documents stored remotely on the computers of a cloud computing service provider.[28/]

The different standards are the unanticipated byproduct of technology changes, and not a careful balancing of the needs of law enforcement and the privacy rights of individuals. Nor do they reflect a substantive difference in the nature of the information; rather they reflect the fact that ECPA was enacted in 1986—six years before Congress authorized commercial activity on the Internet,[29/] and seven years before the first web browser was introduced.[30/] In 1986, very few Americans had e-mail accounts, and those who did typically downloaded email from a server onto their hard drives, and email was automatically and regularly overwritten by service providers grappling with storage constraints.[31/] Even eight years later, when Congress enacted the Communications Assistance for Law Enforcement Act (CALEA),[32/] the commercial Internet

---

28/ 18 U.S.C. § 2703(b). While the government requires a warrant under Rule 41 to forcefully enter and seize someone's personal computer, it could theoretically choose to use a subpoena to compel production of the same computer or its contents, resorting to court enforcement if the recipient failed to comply with the subpoena. As a practical matter, however, concerns about compromising the investigation or destruction of evidence normally lead law enforcement to secure a warrant in this situation. The same concerns about compromise and loss of evidence are not normally present when the subpoena is served on a third party service or storage provider, however.

29/ Prior to 1992 the National Science Foundation's mandate was to support access to the Internet for research and education, and it had no authority to permit or promote commercial activity on the networks connecting research and academic institutions. This authority was conveyed to the NSF only in 1992, with passage of The Scientific and Advanced-Technology Act, 42 U.S.C. § 1862(g) (1992), which directed the National Science Foundation "to foster and support access by the research and education communities to computer networks which may be used substantially for purposes in addition to research and education in the sciences and engineering, if the additional uses will tend to increase the overall capabilities of the networks to support such research and education activities."

30/ The Mosaic web browser was released in 1993, a graphical browser developed by a team at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign (UIUC), led by Marc Andreessen.

31/ Achal Oza, *Amend the ECPA: Fourth Amendment Protection Erodes as E-Mails Get Dusty*, 88 B.U. L. Rev. 1043, 1072 (Note 2008) ("In 1986, e-mail technology was still very new. Most e-mail users dialed-up to their e-mail servers using a modem and downloaded their communications to a home computer, with the server acting only as a medium for temporary storage. Using this rationale, the ECPA draws a distinction between e-mails in electronic storage on third-party servers for 180 days or less and those in electronic storage longer than 180 days." Citing *Electronic Communications Privacy Act: Hearing on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary*, 99th Cong. 475, at 24 (1986) (testimony of Philip M. Walker, General Regulatory Counsel, GTE Telenet Inc., and Vice Chairman, Electronic Mail Association)).

32/ Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001-1021).

was in its infancy, digital storage was expensive,[33] and email was automatically and regularly overwritten by service providers grappling with storage constraints.

Today, the distinctions between and among data in transit, data in electronic storage, data stored by a remote computing service, and data more them 180 days old no longer conform to the reasonable expectations of Americans, nor do these distinctions serve the public interest. A growing chorus of academics argues that these distinctions do not make sense,[34] and courts have had increasing difficulty applying ECPA. The Fifth Circuit described efforts to interpret the Wiretap Act as a "search for lightning bolts of comprehension [that] traverses a fog of inclusions and exclusions which obscures both the parties' burdens and the ultimate goal."[35] The Ninth Circuit described this as a "complex, often convoluted, area of the law."[36] In 2002 the Ninth Circuit said that Internet surveillance was "a confusing and uncertain area of the law" that is so out-dated that it is "ill-suited to address modern forms of communication."[37] A district court in Oregon recently opined that email is not covered by the Constitution, while the Ninth Circuit has

---

[33] Matt Komorowski, *A History of Storage Cost*, *available at* http://www.mkomo.com/cost-per-gigabyte (concludes that "space per unit cost has doubled roughly every 14 months," and states that "[s]everal terabyte+ drives have recently broken the $0.10/gigabyte barriers."); *see also* Digital Prosperity *supra* Note 5, at 8 (The falling cost of storage is "why Web companies like Google, Yahoo, and Microsoft are providing consumers with large amounts of free Web-based storage for their email, photos, and other files. For example, Google provides around 2.7 gigabytes (2,700 megabytes) of free storage for users of their Gmail e-mail service. If Google were to provide this service today using the technology of 1975 (in 2006 prices), it would cost them over $50 million per user! But because memory is now so cheap, Google and other companies can afford to give vast amounts of it away for free, paying for it through unobtrusive advertisements.").

[34] *See, e.g.*, Patricial L. Bellia, *Surveillance Law through Cyberlaw's Lens*, 72 Geo. Wash. L. Rev 1375, 1396-1397 (2004) (stating that "[s]tored communications have evolved in such a way that [ECPA's layer of statutory protection for stored communications], often referred to as the Stored Communications Act ("SCA"), are becoming increasingly outdated and difficult to apply."); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1234 (2004) (stating that the "strange" 180-day distinction "may reflect the Fourth Amendment abandonment doctrine at work," but concluding that "[i]ncorporating those weak Fourth Amendment principles into statutory law makes little sense").

[35] *Briggs v. Am. Air Filter Co.*, 630 F.2d 414, 415 (5th Cir. 1980) (Goldberg, J.). In a case involving the Wiretap Act and the Stored Communications Act, the same court said that the law is "famous (if not infamous) for its lack of clarity." *Steve Jackson Games, Inc. v. United States Secret Serv.*, 36 F.3d 457, 462 (5th Cir. 1994).

[36] *United States v. Smith*, 155 F.3d 1051, 1055 (9th Cir. 1998).

[37] *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002). The Ninth Circuit blamed this confusion on Congress's failure to update the law to take into account modern technologies. In particular, the court complained that: "the difficulty [in construing the surveillance statutes] is compounded by the fact that the ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication.... Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results." *Id.* While the Internet (but not the World Wide Web) did exist in 1986, it is entirely true that the Internet of 2010 bears very little resemblance to the Internet of 1986.

held that it is.[38/] Last year, a panel of the Sixth Circuit first ruled that email was protected by the Constitution and then a larger panel of the court vacated the opinion.[39/] The degree of uncertainty surrounding judicial application of ECPA requirements in any given situation makes it difficult for law enforcement and service providers alike to act with confidence. The absence of clear, intuitive rules necessarily complicates—and slows—business review of law enforcement requests. The absence of clear rules also makes businesses hesitant to embrace emerging Internet hosted services and complicates efforts to consolidate global data repositories.

As the Supreme Court has noted, clarity in the Fourth Amendment context benefits the public and law enforcement alike.[40/] Without clear rules, law enforcement personnel must either take the chance of stepping over the line-risking suppression of evidence or even personal sanctions - or shy away from the line to avoid overstepping.[41/] Neither law enforcement nor the public are well served when law enforcement cannot make appropriate use of an investigative tool because they do not know what is and is not allowed. A dramatic example of the negative consequences of the lack of clarity was cited by the Foreign Intelligence Surveillance Court of Review in *In Re Sealed Case*, where the court noted that the rules set forth in prior judicial decisions had been "very difficult... to administer."[42/] As the 9/11 Commission explained, in the days leading up to the 9/11 attacks, certain intelligence information was not shared with FBI agents who were familiar with al Qaeda because an intelligence analyst misunderstood those decisions and misapplied the Justice Department's rules implementing them.[43/] Lack of statutory

---

38/ *Compare In re United States*, 2009 WL 3416240 (D. Or. June 23, 2009), *with Quon v. Arch Wireless Operating Co.*, 529 F.3d. 892, 895-899 (9th Cir. 2008), *cert. granted* 130 S. Ct. 1101 (2009).

39/ *Warshak v. United States*, 490 F.3d 455, 467 (6th Cir.2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008).

40/ *See, e.g., Arizona v. Roberson*, 486 U.S. 675, 681-682 (1988); *Oliver v. U.S.* , 466 U.S. 170, 181-182 (1984) ("This Court repeatedly has acknowledged the difficulties created for courts, police, and citizens by an ad hoc, case-by-case definition of Fourth Amendment standards to be applied in differing factual circumstances. The ad hoc approach not only makes it difficult for the policeman to discern the scope of his authority; it also creates a danger that constitutional rights will be arbitrarily and inequitably enforced." (citations omitted)).

41/ Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 Stan. L. Rev 503, 527-528 (2007) ("The Fourth Amendment's suppression remedy ... generates tremendous pressure on the courts to implement the Fourth Amendment using clear ex ante rules rather than vague ex post standards.... Clear rules announce ex ante what the police can and cannot do; so long as the police comply with the clear rules, the police will know that the evidence cannot be excluded.").

42/ *In re Sealed Case*, 310 F.3d 717, 743-744 (FISA Ct. Rev. 2002).

43/ *See id.* at 744; National Commission Terrorist Attacks Upon the United States, The 9/11 Commission Report at 78-80, 271, *available at* http://www.gpoaccess.gov/911/pdf/fullreport.pdf.

clarity also causes judicial uncertainty. When unclear statutory terms are interpreted differently in different federal jurisdictions, prosecutors are left with two choices: create different practices and procedures in each jurisdiction or adopt the most restrictive interpretation throughout the whole country. The first option can lead to confusion and arbitrary results, and the second can cause agents to forego the use of important investigative tools even where their use would be permissible.

As email has become a key means of personal and proprietary communications, and as users interact seamlessly with locally stored content and content stored on the Internet, ECPA's rules defy user expectation. Today, tens of millions of consumers enjoy free email and data storage services on the Internet.[44/] These services are normally advertising-supported, and service providers use automated tools to scan the communications in order to deliver relevant advertising or other services.[45/] Many service providers also examine content for security and anti-spam purposes.[46/] All of these activities are undertaken in connection with providing the communication service, and users do not expect that these activities somehow render their private communications less private. Indeed, the average webmail user would be surprised to learn that the government believes this to be the case. Applying ECPA to normal business practices in a manner that deprives users of basic privacy protections threatens to undermine information technology innovations such as cloud computing, which, "by altering the basic economics of access to computing and storage … has the potential to reshape how U.S. and global businesses are organized and operate."[47/]

[44/] *See* Byron Acohido, *Microsoft takes notice as more people use free Google Docs*, USA Today, Sep. 22, 2009 (reporting that by July 2010 27% of companies plan to widely use Google Docs in the workplace).

[45/] *See* Google, More on Gmail and privacy, *available at* http://mail.google.com/mail/help/about_privacy.html#scanning_email

[46/] *See id.* ("Google scans the text of Gmail messages in order to filter spam and detect viruses, just as all major webmail services do.")

[47/] Jeffrey Rayport & Andrew Heyward, Andrew: *Envisioning the Cloud: the Next Computing Paradigm* (Mar. 20, 2009). According to the authors, cloud computing will lower capital requirements for technology start-ups, permit businesses to manage IT resources without tying up capital in IT capacity, while managing energy resources more efficiently; facilitate consumer access to an endless array of powerful applications at low cost; support innovation by reducing the human investment needed to build and maintain IT infrastructure; and foster cooperation and collaboration, without the coordination costs typically associated with bringing people and work together. *See* http://www.marketspaceadvisory.com/cloud/Envisioning-the-Cloud.pdf

As presently applied, ECPA does not comport with user expectations, does not meet law enforcement or judicial needs for clarity, creates non-trivial costs for businesses seeking to comply with law enforcement requests, and erects barriers to the adoption of innovative, productivity enhancing technology by American business. To address these deficiencies in a technology neutral manner, the consensus principles would bring all communications content, whether in transit or in storage (as commonly defined), notwithstanding the age of that content or the ordinary uses of that content by providers, under the basic probable cause standard set forth in the Fourth Amendment, accessible to law enforcement with a warrant.

Effect on Law Enforcement: This proposal would do no more than strictly necessary to reflect the reasonable expectations of privacy of communications technology users today, and to serve the public interest in facilitating innovation in the cloud. For example, the change:

- Would *not* extend to stored content the full range of protections that apply to real-time interception of communications content under the Wiretap Act, and would not require a "super warrant" for access to that data. Rather, this proposal does not modify the Wiretap Act,[48] and under the proposal, a search warrant supported by probable cause would suffice to require a provider to disclose stored content;

- Would *not* further restrict the authority to access communications that are readily accessible to the general public, such as remarks posted on a blog or website available to the public;[49]

- Would *not* modify the right of any authorized recipient of a communication, other than

---

[48] In 2000, the Justice Department supported legislation that would have extended the procedural protections accorded to voice interceptions to the real-time interception of electronic communications under the Wiretap Act, a change that the Justice Department supported in 2000. *See* Testimony of Kevin V. DiGregory, Deputy Assistant Attorney General, United States Department of Justice, Before the Subcommittee on the Constitution of the House Committee on the Judiciary on H.R. 5018 and H.R. 4987 (Sep. 6, 2000) ("For example, the Administration's package proposes that wiretaps for electronic communications should be treated just the same as voice wiretaps, including approval by a high-level Justice Department official, limited to the list of predicate crimes under §2516, and with the availability of suppression under §2515."), *available at* http://judiciary.house.gov/Legacy/digr0906.htm.

[49] 18 U.S.C. § 2511(2)(g)(1).

the service provider, to disclose data to the government without process. Thus, for example, anyone other than the service provider with authorized access to shared photos could voluntarily disclose those photos to anyone else, including a government agent;[50/]

- Would *not* change or eliminate any of the current exceptions permitting disclosures to the government by ECS and RCS providers, including those regarding inadvertently discovered evidence of a crime and emergency disclosures;

- *Would* establish uniform, clear, and easily understood rules about when and what kind of judicial review is needed by law enforcement to access electronic content; and

- *Would*, by clarifying the applicable rules, enable business to respond more quickly and with greater confidence to law enforcement requests and to avail themselves of hosted productivity technology.

Principle 2: Access to Mobile Location Data

Recommended Approach: Under the consensus principles, a governmental entity may require the provider of wire or electronic communications services to produce, prospectively or retrospectively, non-public information regarding the location of a mobile communications device only with a search warrant supported by probable cause.

Need for Change: Cell phones and mobile Internet devices generate location data to support both the underlying service and a growing range of location-based services of great convenience and value. A cell phone that is turned on—whether or not it is in use—is in near

[50/] One of the current exceptions—user consent—poses special issues, because, if broadly applied, consent would overwhelm all privacy protection. For government access, consent should not be inferred from, for example, Terms of Service that allow non-governmental entities to access content for various purposes. The recommendations are based on the presumption that the fact that a service provider has access to information in the cloud for purposes of providing the service, for offering value-added services or for delivering advertising does not diminish the user's expectation of privacy as against the government nor otherwise create any exception to the probable cause warrant requirement. This should be the case regardless of whether it is the provider or a third party contractor that is getting access for these business purposes. Rather, consent that would defeat the warrant requirement should have to be knowing, explicit, and specific both to the person who created the content and the content to be disclosed. If this is not clear, a further amendment may be appropriate.

constant communication with nearby cell towers,[51] and, as a result, site tower information always reveals something about a user's location (*i.e.*, what tower or towers are nearby). In urban areas, where there are many cell towers, a mobile communications device may communicate its location to more than one tower. By triangulating information received by two or more cell towers, it is possible to establish a user's location within a matter of yards.[52] This location data can be intercepted in real time and is often stored for research and development, resolution of billing disputes, and other business purposes;[53] it can reveal a very full picture of a person's movements, leading to inferences about activities and associations. In a growing number of devices, this automatically generated location data is augmented by very precise GPS data.[54]

The requirements governing access to location information are not clearly set out in ECPA. For years law enforcement treated cell site information as "signaling" or "addressing" information, obtained by simply certifying that the information—both retrospective and

---

[51] *See* DOJ, *Electronic Surveillance Manual*, at 40 (2005), *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf. ("A cell site simulator, digital analyzer, or a triggerfish can electronically force a cellular telephone to register its mobile identification number ('MIN,' *i.e.*, telephone number) and electronic serial number ('ESN,' *i.e.*, the number assigned by the manufacturer of the cellular telephone and programmed into the telephone) when the cellular telephone is turned on. Cell site data (the MIN, the ESN, and the channel and cell site codes identifying the cell location and geographical sub-sector from which the telephone is transmitting) are being transmitted continuously as a necessary aspect of cellular telephone call direction and processing. The necessary signaling data (ESN/MIN, channel/cell site codes) are not dialed or otherwise controlled by the cellular telephone user. Rather, the transmission of the cellular telephone's ESN/MIN to the nearest cell site occurs automatically when the cellular telephone is turned on. This automatic registration with the nearest cell site is the means by which the cellular service provider connects with and identifies the account, knows where to send calls, and reports constantly to the customer's telephone a read-out regarding the signal power, status and mode.")

[52] *See id.* at 41. The Global Positioning System (GPS), cell towers, and Wi-Fi positioning service (WPS) are the three techniques to identify a mobile device geo-location.

[53] *See* Declan McCullagh, *Feds Push for Tracking on Cell Phones*, Feb. 10, 2010, *available at* http://news.cnet.com/8301-13578_3-10451518-38.html ("Verizon Wireless keeps 'phone records including cell site location for 12 months,' [said] Drew Arena, Verizon's vice president and associate general counsel for law enforcement compliance.").

[54] The FCC's Enhanced 9-1-1 service will by 2012 require wireless carriers to have the ability to report information about a caller's location to within 50 to 300 meters when the caller makes an emergency call, and within 100 meters for most such calls. 47 C.F.R. § 20.18(h)(1); *see* FCC Enhanced 9-1-1—Wireless Services, *available at* http://www.fcc.gov/pshs/services/911-services/enhanced911/Welcome.html. Wireless carriers often meet this requirement by installing GPS capabilities in their devices. For example, all Verizon devices sold after 2003 are GPS-capable. *See* http://aboutus.vzw.com/wirelessissues/enhanced911.html.

prospective—was "relevant to an ongoing investigation."[55/] In 1994 Congress amended the Pen Register statute to preclude the collection of information disclosing location "solely pursuant" to that statute.[56/] Notwithstanding this change, until 2005 judges routinely issued orders based on the "relevant to an ongoing investigation" certification so long as the request identified any additional authority for the request.[57/] Generally law enforcement cited the Stored Communications Act for this additional authority—even when the location information was sought on a prospective basis, on the theory that nothing in the Stored Communications Act "requires that the provider possess the records at the time the order is executed."[58/]

In 2005, a magistrate judge in the Southern District of Texas rejected this so-called "hybrid-theory," holding – as most cell phone users would assume - that prospective collection of cell site data amounted to "tracking." Citing the standard for installing a mobile tracking device under 18 U.S.C. § 3117, the magistrate judge determined that law enforcement could access prospective cell site data only with a warrant supported by probable cause.[59/] According

---

55/ *See* DOJ, *Electronic Surveillance Manual*, at 45 (2005), *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf. ("In 1994, the Office of Enforcement Operations opined that investigators did not need to obtain any legal process in order to use cell phone tracking devices so long as they did not capture the numbers dialed or other information 'traditionally' collected using a pen/trap device. This analysis concluded that the 'signaling information' automatically transmitted between a cell phone and the provider's tower does not implicate either the Fourth Amendment or the wiretap statute because it does not constitute the 'contents' of a communication. Moreover, the analysis reasoned—prior to the 2001 amendments—that the pen/trap statute did not apply to the collection of such information because of the narrow definitions of 'pen register' and 'trap and trace device.' Therefore, the guidance concluded, since neither the constitution nor any statute regulated their use, such devices did not require any legal authorization to operate.")

56/ Pub. L. 103-414, Title I, § 103 (1994) (codified at 47 U.S.C. § 1002(a)(2)). This preclusion is subject to an exception that applies to the extent the number itself provides the location, *i.e.*, for pay phones or wireline phones.

57/ *See* DOJ, *Electronic Surveillance Manual* at 41, 43-44, *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf. ("Because of the 1994 prohibition, law enforcement authorities have sought other means to compel providers to supply this information prospectively. Most commonly, investigators have used orders under section 2703(d) to obtain this information. Although section 2703(d) generally applies only to stored communications, nothing in that section requires that the provider possess the records at the time the order is executed. Moreover, use of such an order does not improperly evade the intent of the CALEA prohibition. Section 2703(d) court orders provide greater privacy protection and accountability than pen/trap orders by requiring (1) a greater factual showing by law enforcement and (2) an independent review of the facts by a court. Indeed, the very language of the CALEA prohibition—limiting its application 'to information acquired solely pursuant to the authority for pen registers and trap and trace devices'—indicates that Congress intended that the government be able to obtain this information using some other legal process. Public Law 103-414, sec. 103 (a) (emphasis supplied). Thus, 2703 (d) orders are an appropriate tool to compel a provider to collect cell phone location information prospectively." According to the DOJ Manual "[l]aw enforcement investigators may use ... an order under section 2703(d) of title 18 in order to obtain historical records from cellular carriers.")

58/ *Id.*

59/ *In Re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority United States District Court*, Southern District of Texas, Houston Division, Magistrate No. H-05-557M (Oct. 14, 2005).

to Judge Smith, "While the cell phone was not originally conceived as a tracking device, law enforcement converts it to that purpose by monitoring cell site data." Magistrate judges around the country followed Judge Smith's lead on this, including a majority of the opinions published since 2005.[60]

Although Judge Smith's opinion applied only to the *prospective* collection of cell-site information, he noted that an individual might have "an objectively reasonable privacy interest in caller location information,"[61] based on the Fourth Amendment as well as the Wireless Communication and Public Safety Act of 1999.[62] He rejected the notion that there is no reasonable expectation of privacy in cell site location data, as well as the government's attempt to analogize cell site data to telephone numbers found unprotected in *Smith v. Maryland*, 442 U.S. 735 (1979): "Unlike dialed telephone numbers, cell site data is not "voluntarily conveyed" by the user to the phone company. As we have seen, it is transmitted automatically during the registration process, entirely independent of the user's input, control, or knowledge … location information is a special class of customer information, which can only be used or disclosed in an emergency situation, absent express prior consent by the customer."[63]

More recently, courts have rejected government requests for retrospective location data without a warrant, citing the language of the Stored Communications Act that "expressly sets movement/location information outside its scope by defining "electronic communications" to exclude "any communication from a tracking device" (as defined in 18 U.S.C. § 3117) and noting that the "electronic communications statutes, correctly interpreted, do not distinguish

---

60 *See* Declan McCullagh, *Feds Push for Tracking on Cell Phones*, Feb. 10, 2010, *available at* http://news.cnet.com/8301-13578_3-10451518-38.html ("Only a minority [of judges] has sided with the Justice Department [on rules regarding prospective cell phone tracking]."); Transcript of Town Hall Record, *Beyond Voice: Mapping the Mobile Marketplace*, at 177-178 (May 6, 2008) (Session 4, "Location-Based Services"), *available at* http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/050608_sess4.pdf.

61 *In Re Application for Pen Register*, supra note 58 at 16.

62 Pub. L. No. 106-81, § 5, 113 Stat. 1288 (Oct. 26, 1999) (codified at 47 U.S.C. § 222(f)).

63 *In Re Application for Pen Register*, supra note 58 at 15; http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf.

between historic and prospective [cell site location information]."[64] Under these holdings, law enforcement can no longer assume that they will be able to acquire location data without a warrant based on probable cause.

Courts that require law enforcement to secure a warrant based on probable cause to access mobile location data recognize that users are likely to assume that tracking, however accomplished, is still tracking. To comport with reasonable expectations and serve the public interest, the current uncertainty should be resolved by applying the probable cause standard to disclosure of relatively precise location information.

There are already a number of innovative, socially beneficial "location aware" applications that employ technologies such as GPS, cell phone infrastructure, or wireless access points to locate electronic devices and provide "resources such as a 'you are here' marker on a city map, reviews for restaurants in the area, a nap alarm triggered by your specific stop on a commuter train, or notices about nearby bottlenecks in traffic."[65] More applications such as these are emerging every day, and in short order "systems which create and store digital records of people's movements through public space will be woven inextricably into the fabric of everyday life."[66] These applications will enhance quality of life, further important economic and social goals, and—with appropriate safeguards—serve law enforcement. Absent clear standards, privacy concerns could discourage consumer use, which could in turn make it less likely that location data will be available to law enforcement with proper authority.

---

[64] *In the Matter of the Application of the United States of America for an Order Directing the Provider of Electronic Communications Service to Disclose Records to the Government*, U.S. District Court for the Western District of Pennsylvania. Magistrate's No. 07-524M Magistrate Judge Lisa Pupo Lenihan , *aff'd* Sep. 2008, ("Government's requests for Court Orders mandating a cell phone service provider's covert disclosure of individual subscribers' (and possibly others') physical location information must be accompanied by a showing of probable cause."). The case has been appealed to the Third Circuit, which heard oral arguments on February 12, 2010. Case 08-4227.

[65] *See* Educause Learning Initiative, *7 Things You Should Know About ... Location Aware Applications*, *available at* http://net.educause.edu/ir/library/pdf/ELI7047.pdf.

[66] Andrew J. Blumberg & Peter Eckersley, Electronic Frontier Foundation, *On Locational Privacy, and How to Avoid Losing it Forever*, at 1 (Aug. 2009), *available at* http://www.eff.org/files/eff-locational-privacy.pdf. The sensitivity of precise geographic location information was also discussed at a panel on mobile "location-based services" during the FTC's 2008 Town Hall on mobile marketing. *See* Transcript of Town Hall Record, *Beyond Voice: Mapping the Mobile Marketplace* (May 6, 2008) (Session 4, "Location-Based Services"), *available at* http://ftc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/050608_sess4.pdf.

Effect on Law Enforcement: Information that reveals an individual's precise location can be highly sensitive, and collection of this information without proper safeguards implicates the exercise of a variety of rights protected by the Constitution, including important expression and association rights. To facilitate innovation, encourage the uptake of emerging location-aware technologies, and ensure that law enforcement access to location information generated by these products and services comports with the reasonable privacy expectations of Americans, ECPA should be amended to require a warrant based on probable cause to support access to location information, whether it is sought on a retrospective or prospective basis.[67] This standard is consistent with Fourth Amendment safeguards against unreasonable search and seizure. In many cases, law enforcement must already meet the probable cause standard when requesting location data,[68] and certain service providers are taking the position that location data is subject to higher standards under ECPA for content.[69]

Principle 3: Access to Transactional Data

Recommended Approach: Under the consensus principles, a governmental entity could require the provider of wire or electronic communications services to produce, prospectively or in real time, transactional information (*i.e.*, dialed number information, IP address, Internet port information, email to/from information and similar communications traffic data)[70] only with a judicial finding that the entity has offered specific and articulable facts demonstrating reasonable

---

[67] This would be subject, of course, to the exception for telephone numbers that themselves provide location information.

[68] Most courts have held that prospective information requires a showing of probable cause. See *supra* note 63. Law enforcement requests for retrospective location data are often combined with requests for prospective data. *See, e.g., In re 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 (W.D. Pa. 2008); *In re Application of U.S. for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone*, 460 F. Supp. 2d 448, 453 (S.D.N.Y. 2006).

[69] For example, the Loopt service "shows users where friends are located and what they are doing via detailed, interactive maps on their mobile phones.... Users can also share location updates, geo-tagged photos and comments with friends in their mobile address book or on online social networks, communities and blogs." The provider clearly understands the privacy implications of this technology, and reassures users that "Loopt was designed with user privacy at its core and offers a variety of effective and intuitive privacy controls." About Loopt, *available at* http://www.loopt.com/about.

[70] DOJ, *Electronic Surveillance Manual*, at 39 (2005), *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf. ("Pen register and trap and trace devices may obtain any noncontent information—all 'dialing, routing, addressing, and signaling information'—utilized in the processing and transmitting of wire and electronic communications. Such information includes IP addresses and port numbers, as well as the 'To' and 'From' information contained in an e-mail header.")

grounds to believe the information sought is relevant and material to an ongoing criminal investigation.

Need for Change: Transactional data—records of who is calling whom, when and for how long, and records of all the "to" and "from" information associated with one's email, including date, time, message length (including subject line length)—can be highly revealing. Transactional records for e-mail and cell phone usage may contain far more information about an individual's communications than "pen register" data in the wireline environment of the 1980s.[71] As technology has evolved, transactional data has become ever more detailed and revealing, but remains available to law enforcement without effective judicial supervision. In fact, under ECPA, a court *must* issue an order for a pen register[72] or trap and trace device[73] whenever a prosecutor files a document stating that the information sought is relevant to an ongoing investigation.[74] Thus, read literally, a judge cannot even assess whether the information is in fact relevant; the only question is whether the government says that it is. As communications technology evolves and produces increasingly detailed and rich transactional

---

[71] For example, the transactional record of an outgoing phone call to someone in a large office likely only contains the general office phone number and does not specify which person in the office has been contacted. However, the transactional record of an email to that person contains the recipient's unique email address. *See* Center for Democracy & Technology's Analysis of S.2092 (Apr. 4, 2000), *available at* http://cld.cdt.org/security/000404amending.shtml.

It is not yet clear whether information such as URL's that include search terms or specific website addresses are "content" information that must be excluded from transactional records. Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 Wm. & Mary L. Rev 2105, 2105 (2009) ("Courts and Internet law scholars have yet to offer a means of determining the content/envelope status of unique aspects of Internet communications-from email subject lines to website URLs."). If transactional records for e-mail or Internet-enabled cell phones include this information, then they would be far more revealing than traditional wireline telephone records. *E.g.*, *United States v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008) ("Surveillance techniques that enable the government to determine not only the IP addresses that a person accesses but also the uniform resource locators ("URL") of the pages visited might be more constitutionally problematic. A URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person's Internet activity.").

[72] A "pen register" is defined as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication...." 18 U.S.C. § 3127(3).

[73] A "trap and trace device" is defined as a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, [or] signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however that such information shall not include the contents of any communication. 18 U.S.C. § 3127(4).

[74] 18 U.S.C. § 3123(a).

information, it is appropriate to afford judges a meaningful role in assessing whether the government's claim of relevance is substantiated.

Effect on Law Enforcement: The Justice Department has in the past acknowledged that the approach taken by the recommended principle is appropriate.[75] Nonetheless, the consensus principles call for a modest change only: The standard proposed is significantly less than probable cause: "specific and articulable facts showing that there are reasonable grounds to believe that the information ... is relevant and material." Drawn from the *Terry* decision of the U.S. Supreme Court,[76] the language is identical to the formulation in the Stored Communications Act, which currently provides:

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers 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.[77]

The marginal burden on law enforcement from this change should be minimal because law enforcement rarely asks for a pen register order without already possessing information sufficient to satisfy a "specific and articulable facts" standard.[78] The change will enhance business

---

[75] *See* DOJ's View on H.R. 5018 (Electronic Communications Privacy Act of 2000), Testimony of Kevin Digregory, Deputy Associate Attorney General, *available at* http://commdocs.house.gov/committees/judiciary/hju67343.000/hju67343_0.htm ("H.R. 5018, like the Administration's bill, would introduce the requirement of judicial review of the factual basis for such orders. Specifically, H.R. 5018 would require such applications to contain 'specific and articulable facts' that would justify the collection of the data. While the Justice Department can comply with the added administrative burdens imposed by increasing this standard, we have concerns about the amendments. Specifically, the technology-specific manner in which the bill would implement this change, the lack of an emergency exception, and the unrealistic geographic limitations that restrict such orders in the present law all raise serious concerns that should be addressed.").

[76] *Terry v. Ohio*, 392 U.S. 1, 21 (1968).

[77] 18 U.S.C. § 2703(d).

[78] Orin S. Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother That Isn't*, 97 Nw. U. L. Rev. 607, 639 & 673 n. 154 (2003) ("[A] higher 'specific and articulable facts' threshold would not add substantial burden for law enforcement.... [I]n my government experience I never knew or even heard of any law enforcement agent or lawyer obtaining a pen register order when the agent did not also have specific and articulable facts, which would satisfy the higher threshold. My experience is narrow, but it suggests that the practical burden of obtaining the order combined with the certification to a federal judge and potential for criminal liability effectively regulates government officers and deters them from obtaining pen register orders in bad faith. On the other hand, there may be rogue officers out there, if not now then in the future, and a higher threshold combined with judicial review could potentially provide an extra barrier to abuse.").

responsiveness by clarifying the obligations of both law enforcement and business, and preserves the distinction between content and transactional data, and maintains the reduced burden needed to acquire the latter.

Principle 4: Access to Subscriber Identifying Data and Stored Transactional Information

Recommended Approach: Under the consensus principles, a governmental entity may use a subpoena to require the provider of wire or electronic communications services to produce information related to a specified account or individual. Judicial approval would be necessary only where such requests do not relate to a specified account or individual.

Need for Change: Under ECPA, law enforcement may use an administrative, grand jury or trial subpoena to acquire certain information pertaining to a "subscriber to or [a] customer" of an electronic communications service or remote computing service.[79] The information that may be acquired under this provision includes name, address, call or session records, length of service and type of service utilized, and method of payment.[80] Using the administrative subpoena authority, law enforcement makes an independent determination that certain records are needed and then issues and serves the subpoena without input from a grand jury or even an assistant U.S. Attorney. Such administrative subpoenas are subject to judicial review only if the recipient of the subpoena challenges it. With administrative, grand jury or trial subpoenas, the government has no obligation to notify the subscriber or customer to whom the records relate.[81] A carrier or ISP will rarely have the incentive to challenge a subpoena, so this information is routinely disclosed without any judicial review whatsoever.

The absence of judicial review or any meaningful opportunity to challenge a request for subscriber identifying records and stored customer records suggests that the scope of the subpoenas in these cases should be appropriately tailored. Indeed, the language of the statute itself suggests that such subpoenas may be issued for information pertaining to "a subscriber" or "a customer" identified with some particularity, for example, by a phone number or an IP

---

[79] 18 U.S.C. § 2703(c)(2).

[80] *Id.*

[81] 18 U.S.C. § 2703(c)(3).

address at a specific time. This principle would make it clear that a subpoena cannot be used to compel production of, for example, information identifying "*all* subscribers" whose device registered on a specified cell tower on a specified date, or information identifying "*all* subscribers" who accessed a particular web site during a specified period of time. Nothing in the legislative history of ECPA suggests that the provision should be read to authorize such broad use of subpoenas. Rather, the absence of judicial review argues for a narrow interpretation to avoid misuse of the subpoena for "fishing expeditions."[82]

Effect on Law Enforcement: The principle is intended to clarify that the government may use a subpoena to obtain the subscriber information specified in the statute if the investigator can identify the subscriber with particularity (*e.g.* phone number, IP address used at a specific time). Otherwise, the investigator would obtain the information after securing a §2703(d) order based on specific and articulable facts demonstrating reasonable grounds to believe that the information is relevant to an ongoing criminal investigation, or a search warrant. The consensus principles would leave the current standard found in ECPA untouched when the records sought by law enforcement pertain to a specific subscriber or customer. Only if the government sought records about groups of subscribers or customers, would judicial review be required.

Conclusion

The United States leads the world in bringing innovative, ground-breaking communications technology to market, and enjoys the many social and economic benefits that technology produces. The United States also enjoys the many benefits flowing from Constitutional safeguards designed to preserve individual liberties, including the right to be free from unreasonable search and seizure. The U.S. has consistently balanced those values with the

---

[82] Without a narrow interpretation, law enforcement can subpoena a list of all visitors to a news website on a particular day, and order that the recipient of the subpoena not disclose the subpoena's existence. The Department of Justice recently attempted this before withdrawing its subpoena after the website owners objected publicly. *See* Declan McCullagh, *Justice Dept. Asked for News Site's Visitor Lists*, Taking Liberties Blog (Nov. 10, 2009), *available at* http://www.cbsnews.com/blogs/2009/11/09/taking_liberties/entry5595506.shtml; Copy of Subpoena, *available at* http://www.eff.org/files/subpoena.pdf. *See also* Nymity Interview, *Where Did Due Process Go? Government Access to Personal Information in the Cloud* (Interview with Scott Shipman, eBay) (Feb 2010), http://www.nymity.com/Free_Privacy_Resources/Privacy_Interviews/2010/Scott_Shipman.aspx ("[W]e're starting to see a new wave of requests. These new requests are a broad request for a large group of unnamed customers. For example, we see requests from authorities that state, 'please provide all information on all sellers who have sold in the following jurisdiction (zip code) within the last year.' Requests like those arguably flip the notion of due process upside down.").

needs of law enforcement in the communications environment, and both U.S. consumers and the U.S. economy have benefitted from the trust and confidence that this balance inspires in our electronic communications and information technology services providers, including among businesses and individuals located outside our borders. Changes in technology since 1986 have made it difficult to apply ECPA in a manner that comports with the reasonable expectations of individuals, potentially eroding user willingness to entrust private information to third party service providers in the United States. The principles recommended by the working group would, if implemented, align ECPA with current and emerging technology without unduly constraining or imposing significant burdens on law enforcement.

Mr. NADLER. With that, I thank the witnesses. And the hearing is adjourned.

[Whereupon, at 4:06 p.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

May 5, 2010

Thank you, Mr. Chairman, for holding this hearing and giving Members the opportunity to examine the Electronic Communications Privacy Act.

The internet has grown and transformed the way Americans communicate, work, and live. We are increasingly living our lives online. We go online to learn, shop, pay our bills, and to connect with family and friends.

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.

The ability to monitor communications has grown enormously. As technology continues to expand, we must adjust our laws to keep up with modern technology.

The primary statutory protection for the privacy of electronic communications is the Electronic Communications Privacy Act, which became effective in 1986. The World Wide Web, however, was not designed and distributed until 1992. In 1993, there were almost two million web sites. As of 2007, it was estimated that there were over 100 million web sites.

As the World Wide Web and technology continue to expand, our laws must evolve to keep up with current trends.

As I think about this issue, several questions come to mind. How can Congress reform the Electronic Communications Privacy Act to ensure that individuals retain their right to privacy and that the government has the tools it needs to conduct investigations? How can Congress reform the Act to provide service providers with clarity so that they can effectively communicate with their customers and gain their trust? Is it premature for Congress to legislate with unresolved Fourth Amendment issues?

I hope that our witnesses can shed light on these questions.

Thank you, Mr. Chairman, for scheduling this hearing. I look forward to hearing from our witnesses today, and yield back the balance of my time.

Written Testimony of Richard Salgado
Senior Counsel, Law Enforcement and Information Security, Google Inc.
House Judiciary Subcommittee on the Constitution, Civil Rights, and Civil Liberties
Hearing on Electronic Communications Privacy Act Reform
May 5, 2010

Google thanks Chairman Nadler, Ranking Member Sensenbrenner, and honorable members of the Subcommittee for examining the need to modernize the Electronic Communications Privacy Act of 1986 (ECPA). My name is Richard Salgado. As a Senior Counsel for Law Enforcement and Information Security at Google, I oversee the company's response to government requests for user information under various authorities including ECPA. I am also responsible for working with teams across Google to protect the security of our networks and user data. I have also served as a Senior Counsel in the Computer Crime and Intellectual Property Section in the U.S. Department of Justice.

It is vital for Google and for Internet users that Congress update ECPA to address the tremendous technological advances in communications and computing technology that the world has witnessed since the statute was passed. This is why Google is playing a lead role in the Digital Due Process coalition (www.digitalddueprocess.org), an ECPA reform advocacy coalition that includes other technology companies, non-governmental organizations, and academics. We need to make sure that ECPA protects individuals from unwarranted government intrusion as communications and computing technology continue to advance. At the same time, ECPA must offer law enforcement the tools necessary to perform its important work.

ECPA was designed for the communications and computer technology of 1986. The ways in which we communicate and compute today, however, bear little resemblance to those of a quarter century ago. When ECPA became law in 1986, communication through the Internet was the province of academic researchers and government agencies. There was no commercial World Wide Web. Commercial email had not yet been offered to the general public. Instant messaging wasn't widely used until the late 1990s. Only 340,000 Americans subscribed to cell phone service -- the equivalent of one line for every citizen of Tampa, Florida -- and not one of them was able to send a text message.

Since ECPA was signed into law, we have experienced unprecedented advances in communications technology and services, and a fundamental shift in how people communicate. The web, search engines, video sharing sites, and voice-over-IP services are only a few of the technologies that have become commonplace and part of everyday life, yet would have seemed like science fiction at the time ECPA was enacted.

We've also seen a profound transformation in the way we store, access, and transfer data. In 1986, holding and storing data was expensive, and storage devices were limited by

technology and size. A 10 megabyte hard drive that had room to store about two high resolution photos cost $650 (or 10 dollars per megabyte). In 2010, thanks to innovation and advances in technology, a 1.5 terabyte hard drive can be purchased for $99 (0.000094 dollars per megabyte) and hold 300,000 photos. Complimenting the growth in storage capacity, average data transfer rates are nearly one hundred and sixty times faster than in 1986 -- making it possible to share richer data and to perform more complicated tasks in a fraction of the time it took when ECPA became law. This massive drop in cost and increase in the speed of storing and accessing data has had a huge and positive impact on all classes of online users, fostering improvements in efficiency and innovation. The development of Internet-based computing and storage -- widely known as "cloud computing" -- is one direct benefit.

Companies like Google are now able to offer individuals, businesses, educational institutions, government entities, and others the ability to store, access, use and share their data from remote servers. This provides enormous cost, scalability, and security advantages over home or workplace data storage that was the norm twenty-five years ago. Rather than invest in expensive and specialized IT equipment and personnel, customers can rely on the scale and security offered by the cloud providers to access data anywhere Internet access is available. The cloud is about much more than email; it enables services like online video, shared document collaboration among people in different time zones, and many other services. The "virtual" services offered in the cloud have created enormous and tangible value in the economy, cultivating new businesses and a spurring the creation of an entirely new tech sector. As communications and networks become faster and more data intensive, this sector will continue to create new jobs and more opportunities for investors and innovators.

The movement to the cloud will continue to increase as its benefits are widely felt. This is a valuable and important trend that shouldn't be slowed artificially by outdated technology assumptions baked into parts of ECPA. Nor should the progression of innovation and technology be hobbled by ECPA provisions that no longer reflect the way people use the services or the reasonable expectations they have about government access to information they store in the cloud.

Applying the statute to new, widely used services that didn't exist in 1986 has resulted in complex, often baffling rules that are difficult to explain to users and difficult to apply. This mismatch between privacy expectations and privacy protection, combined with counter-intuitive rules, threatens to hinder the benefits of cloud services to our economy.

The rules around compelled production of communications content, like email, provide a good example of the current complexity. ECPA provides that the government can compel a service provider to disclose the contents of an email that is older than 180 days with nothing more than a subpoena (and notice to the user, which can be delayed in certain circumstances). If the email is 180 days or newer, the government will need a search warrant. (The U.S. Department of Justice also takes the position that a subpoena is appropriate to compel the service provider to disclose the contents of an email even if it's not older than 180 days if the user has already retrieved it. The Ninth Circuit Court of Appeals has rejected this view.) It's difficult to imagine a justification for a rule that lowers

the procedural protection for a message merely because it is six months old or has been viewed by the user.

The Digital Due Process coalition has put forward principles that are designed to help ensure that content stored in the cloud gets no less due process protection as data held on computers at home or in the office, to adjust the rules to match the reasonable privacy interests of today's online citizens, and to ensure that government has the legal tools needed to enforce the laws.

There are four key ways ECPA should be updated:

- **Create a consistent process for data stored online:** Treat private communications and documents stored online the same as if they were stored at home and require the government to get a search warrant before compelling a service provider to access and disclose the information.

- **Create a consistent process for location information:** Require the government to get a search warrant before it can track movements through the location of a cell phone or other mobile communications device.

- **Clarify the process for real-time monitoring of when and with whom communications are being made:** To require a service provider to disclose information about communications as they are happening (such as who is calling whom, "to" and "from" information associated with an email that has just been sent or received), the government would first need to demonstrate to a court that the data it seeks is relevant and material to a criminal investigation.

- **Clarify the process for bulk data requests:** A government entity investigating criminal conduct could compel a service provider to disclose identifying information about an entire class of users (such as the identity of all people who accessed a particular web page) only after demonstrating to a court that the information is needed for the investigation.

Modernizing ECPA will benefit everyone who uses cloud services including individual users, businesses small and large, and enterprise customers -- all of whom depend on having their data available everywhere, safe, secure, and at low cost. It will also make users of cloud services confident that the privacy of what they store virtually in the cloud is respected no less than the privacy of information stored at home. As confidence grows and users put more of their data on the cloud, those benefits will be felt throughout the American economy as lower costs and higher productivity. Further, these updates will provide clear guidance and consistency to law enforcement agencies, and will not impede the ability of law enforcement agents to obtain evidence stored in the cloud.

The issue of due process in the cloud is one of increasing interest to our users. Last month, Google released a new government requests transparency tool that gives our users information about the requests for user data or content removal we receive from

government agencies around the world (www.google.com/governmentrequests). This tool has served to raise attention to the issue of what rights users have when it comes to their data. We hope that the U.S. leads the way in ensuring that data requests for online data receive the kind of due process that citizens expect and deserve.

Advances in technology rely not just on the smart engineers who create the new services, but also on smart laws that provide the critical legal underpinning for this new world. We look forward to working with Congress to strengthen the legal protections for individuals and businesses that rely on our services.

Written Statement of the
American Civil Liberties Union

Laura W. Murphy
Director
ACLU Washington Legislative Office

Christopher Calabrese
Legislative Counsel
ACLU Washington Legislative Office

Nicole A. Ozer, Esq.
Technology and Civil Liberties Policy Director
ACLU of Northern California

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

May 5, 2010

Hearing on

Electronic Communications Privacy Act Reform

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

Written Statement of the
American Civil Liberties Union

Laura W. Murphy
Director
ACLU Washington Legislative Office

Christopher Calabrese
Legislative Counsel
ACLU Washington Legislative Office

Nicole A. Ozer, Esq.
Technology and Civil Liberties Policy Director
ACLU of Northern California

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

Chairman Nadler, Ranking Member Sensenbrenner, and Members of the Committee:

The American Civil Liberties Union (ACLU) has over 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. Throughout our history, we have been one of the nation's foremost protectors of individual privacy. We write today to urge the committee to take the first steps toward modernizing the Electronic Communications Privacy Act (ECPA).

The Founding Fathers recognized that citizens in a democracy need privacy for their "persons, houses, papers, and effects." That remains as true as ever. But our privacy laws have not kept up as technology has changed the way we hold information. Thomas Jefferson knew the papers

and effects he stored in his office at Monticello would remain private. Today's citizens deserve no less protection just because their "papers and effects" might be stored electronically.

The main statutory protection for the privacy of communications, ECPA, was written in 1986 before the Web was even invented. Technology has not only advanced tremendously since 1986, it has also become an essential part of our lives. It impacts how we learn, share, shop and connect. We need an updated ECPA to match our modern online world.

Americans Have Embraced Technology

Technology has changed immensely since ECPA was written in 1986—and Americans have adopted these changes into their lives:

- Over 50% of American adults use the Internet on a typical day.[1]
- 62% of online adults watch videos on video-sharing sites, [2] including 89% of those aged 18–29.[3]
- 69% of online adults use "cloud computing" [4] services to create, send and receive, or store documents and communications online.[5]
- Over 70% of online teens and young adults[6] and 35% of online adults have a profile on a social networking site. [7]
- 83% of Americans own a cell phone and 35% of cell phone owners have accessed the Internet via their phone.[8]

---

[1] Common daily activities include sending or receiving email (40+% of all American adults do so on a typical day), using a search engine (35+%), reading news (25+%), using a social networking site (10+%), banking online (15+%), and watching a video (10+%). Pew Internet & American Life Project, *Daily Internet Activities, 2000–2009*, http://www.pewinternet.org/Trend-Data/Daily-Internet-Activities-20002009.aspx.

[2] A "video-sharing site" or "video hosting site" is a website that allow users to upload videos for other users to view (and, often, comment on or recommend to others). Wikipedia, *Video Hosting Service*, http://en.wikipedia.org/wiki/Video_sharing (as of May 1, 2010, 04:21 GMT). YouTube is the most common video-sharing site today.

[3] Pew Internet & American Life Project, *Your Other Tube: Audience for Video-Sharing Sites Soars*, July 29, 2009, http://pewresearch.org/pubs/1294/online-video-sharing-sites-use

[4] The term "cloud computing" has many definitions, but generally refers to services that offer applications or data storage accessible via the web. Pew Internet & American Life Project, *Use of Cloud Computing Applications and Services*, Sep. 2008 [hereinafter Pew Cloud Report], http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services.aspx.

[5] Pew Internet & American Life Project, *Use of Cloud Computing Applications and Services*, Sep. 2008 [hereinafter Pew Cloud Report], http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services.aspx . 56% of Internet users use webmail services, 34% store photos online, and 29% use online applications such as Google Docs or Adobe Photoshop to create or edit documents.

[6] Pew Internet & American Life Project, *Social Media & Young Adults*, Feb. 3, 2010, http://www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx.

[7] "Social networking sites" allow users to construct a "semi-public" profile, connect with other users of the service, and navigate these connections to view and interact with the profiles of other users. danah m. boyd & Nicole B. Ellison, *Social Networking Sites: Definition, History, and Scholarship*, 13 J. of Comp.-Mediated Comm. 1 (2007); Pew Internet & American Life Project, *Adults & Social Network Sites*, Jan. 14, 2009, http://www.pewinternet.org/Reports/2009/Adults-and-Social-Network-Websites.aspx.

Companies continue to innovate and create new ways for Americans to merge technology with daily activities. Google has spent the last five years building a new online book service and sales of digital books and devices have been climbing.[9] Americans increasingly turn to online video sites to learn about everything from current news to politics to health.[10] Location-based services[11] are a burgeoning market.[12]

These services provide many benefits, but they also have the ability to collect and retain detailed information about individuals: their interests, concerns, movements, and associations. This information can be linked together, allowing a user's Internet searches, emails, cloud computing documents, photos, social networking activities, and book and video consumption to be collected into a single profile.[13]

Americans Still Expect Privacy

This rapid adoption of new technology has not eliminated Americans' expectations of privacy. To the contrary, Americans still expect and desire that their online activities will remain private, and express a desire for laws that will protect that privacy.

- 69% of Internet users want the legal right to know everything that a Web site knows about them.[14]
- 92% want the right to require websites to delete information about them.[15]
- A large percentage of users of cloud computing are "very concerned" about how their personal information may be used and disclosed to law enforcement and third parties.[16]

---

[8] Pew Internet & American Life Project, *Internet, Broadband, and Cell Phone Statistics*, Jan. 5, 2010, http://www.pewinternet.org/Reports/2010/Internet-broadband-and-cell-phone-statistics.aspx.

[9] *See generally* ACLU of Northern California, *Digital Books: A New Chapter for Reader Privacy*, Mar. 2010, *available at* http://www.dotrights.org/digital-books-new-chapter-reader-privacy.

[10] "More Americans are watching online video each and every month than watch the Super Bowl once a year.." Greg Jarboe, *125.5Million Americans Watched 10.3 Billion YouTube Videos in September*, SEARCHENGINEWATCH.COM, Oct. 31, 2009, http://blog.searchenginewatch.com/091031-110343.

[11] "Location-based services" is an information service utilizing the user's physical location (which may be automatically generated or manually defined by the user) to provide services. Wikipedia, *Location-Based Service*, http://en.wikipedia.org/wiki/Location-based_service (as of May 1, 2010, 04:35 GMT).

[12] Recent location-based service Foursquare built a base of 500,000 users in its first year of operation. Ben Parr, *The Rise of Foursquare in Numbers [STATS]*, MASHABLE, Mar. 12, 2010, http://mashable.com/2010/03/12/foursquare-stats/.

[13] *See* ACLU of Northern California, *Digital Books*, *supra* note 9 ("[I]f a reader has logged in to other Google services such as Gmail at the time he searches for a book, Google can link reading data to the reader's unique Google Account [and] retains the right to combine all this information with information gleaned from its DoubleClick ad service, which tracks users across the Internet.") More information is available at the ACLU's Demand Your dotRights campaign website. Demand Your dotRights, http://dotRights.org.

[14] Joseph Turow, et al., *Americans Reject Tailored Advertising* 4 (2009), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[15] *Id.*

[16] Cloud computing users are "very concerned" about law enforcement access to data (49%); services retaining files after users delete them (63%); services using personal data for targeted advertisements (68%) or marketing (80%); services selling files or data to third parties (90%). See Pew Cloud Report, *supra* note 5, at 11.

When user privacy is not protected, users are slower to adopt new technology. A recent poll revealed that 50% of Americans polled have little or no interest in using cloud computing and that 81% of these respondents are reluctant, at least in part, because they are concerned about the security of their information in the cloud.[17]

Americans want and need legal protections for privacy that reflect the technology they use every day. The time has come to modernize ECPA to reflect our 21st century digital world.

ECPA Rules Are Confusing and Outdated

In the face of rapid technological change and Americans' continuing expectation of privacy, ECPA has fallen behind. Distinctions in ECPA have become increasingly confusing and arbitrary, based on an understanding of technology that is a generation behind that which we use today.[18] Many new technologies, particularly those dealing with location information, are not addressed by ECPA. These failures not only leave holes in the privacy protections in place for individuals, but pose a threat to continuing innovation and business development. We need to update ECPA to encompass all of the ways that Americans use technology today.

E-mail exemplifies the gap between the language of ECPA and today's technology. In 1986, e-mail was typically downloaded to a recipient's computer upon receipt and immediately deleted from the e-mail provider's storage. ECPA was written with this behavior in mind: it requires a search warrant to retrieve a message from an e-mail provider's storage only if the message is less than 180 days old, and provides for lower standards if the email is left on the server for more than 180 days.[19] Today, however, e-mail is often both stored on and accessed from remote servers belonging to the e-mail provider, and many people "archive" their e-mail on their provider's server rather than deleting old messages. Basing legal protection on how long an e-mail has been stored is incongruous with current e-mail use. Instead, ECPA should provide full protection for all online documents and communications and dispose of these artificial and outdated distinctions.

Similarly, the state of technology in 1986 resulted in more legal protection in ECPA for the content of communication—the body of an e-mail or the contents of a letter or phone conversation—than for the transactional information. Historically, transactional information was easy to distinguish from content: the number dialed on a telephone as opposed to the voice call itself, or writing on the outside of an envelope as opposed to the message within. The digital world, however, blurs the line between content and transactional data. Internet search terms, browser history, e-mail subject lines and location information do not fit neatly into either category and can reveal sensitive data like political and religious affiliations. Most people

---

[17] Harris Interactive, *Cloud Computing: Are Americans Ready?*, Apr. 21, 2010, http://news.harrisinteractive.com/profiles/investor/ResLibraryView.asp?BzID=1963&ResLibraryID=37539&Category=1777

[18] *See Steve Jackson Games v. U.S. Secret Service*, 36 F.3d 457 (5th Cir. 1994) (The Wiretap Act, as amended by ECPA, is "famous (if not infamous) for its lack of clarity.").

[19] Even this limited protection is in doubt. The Department of Justice has argued that, once email is opened, it is no longer in "electronic storage" and thus no longer subject to a warrant requirement under ECPA even if it is less than 180 days old. *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. §2703(d), D. Colo., No. 09-80.*

consider such information to be private. The law should match these expectations and require a warrant for disclosure.

In addition to the difficulty in anticipating modern uses of technologies existing in that era, lawmakers in 1986 could not predict technological innovations. Mobile phones provide a glaring example, along with the location information gleaned from them. Modern cell phones have become, in essence, portable tracking devices. Technologies including GPS[20] and cell tower triangulation[21] allow mobile phone providers to determine our physical locations in real time—and these providers can retain records of this location information for various purposes. The legal standard for access to these records is currently being litigated, and Congress has never weighed in on what the appropriate standard should be.[22] In the meantime, litigants regularly demand these sensitive records in government investigations and civil suits. A company employee recently admitted that Sprint received a staggering eight million requests for mobile phone location information from law enforcement in just over a year.[23]

Outdated digital privacy law is not only a threat to individual privacy; it also affects businesses and hinders innovation. User perception of inadequate privacy is one threat that companies face. For example, Microsoft recently announced that its future lies in online cloud computing services, but its own poll found that more than 90 percent of the general population is "concerned about the security, access, and privacy of personal data" stored online,[24] leading the company to explicitly ask Congress for better online privacy protection to promote cloud computing.[25]

Companies are also affected when they receive demands to turn over the personal information of users. Google just released data that it received over 3,500 demands from law enforcement involving criminal investigations in the last six months of 2009.[26] If Google is receiving thousands of demands digging into the intimate details of individual lives that are captured in emails, search histories, reading and viewing logs, and the like, how many more are going out to Yahoo, Microsoft, Facebook and the thousands of other online services that Americans use every day? And how can companies hope to respond to these requests without improperly over- or

---

[20] GPS, or Global Positioning System, is a satellite-based navigation system that allows a GPS receiver to determine its own location. *Global Positioning System*, http://gps.gov.

[21] Cell tower triangulation allows the location of a mobile device to be determined by "triangulation" based on its calculated distance from two or more cell towers within the phone's range. *See* Chris Silver Smith, *Cell Phone Triangulation Accuracy Is All Over the Map*, SearchEngineLand.com, Sep. 22, 2008, http://searchengineland.com/cell-phone-triangulation-accuracy-is-all-over-the-map-14790.

[22] *See, e.g., In re Application of the United States for an Order Directing a Provider of Electronic Communications Service to Disclose Records to the Government*, No. 08-4227 (3d. Cir. oral argument heard Feb. 12, 2010).

[23] Kim Zetter, *Feds 'Pinged' Sprint GPS Data 8 Million Times Over a Year*, WIRED, Dec. 1, 2009.

[24] Microsoft News Center, *Cloud Computing Flash Poll—Fact Sheet*, http://www.microsoft.com/presspass/presskits/cloudpolicy/docs/PollFS.doc. More information is available at http://www.microsoft.com/presspass/presskits/cloudpolicy/materials.aspx.

[25] Microsoft News Center, *Press Release: Microsoft Urges Government and Industry to Work Together to Build Confidence in the Cloud*, Jan. 20, 2010, *available at* http://www.microsoft.com/presspass/press/2010/jan10/1-20BrookingsPR.mspx.

[26] Government Requests Tool, http://www.google.com/governmentrequests. Note this does not include National Security letters or demands received outside of criminal investigations. It also does not count the actual number of users whose records disclosed pursuant to each demand. All of this means this number likely only reflects a fraction of the number of users whose records were demanded.

under-disclosing information when faced with outdated, confusing laws with questionable applicability to their products or services?

Key Principles for Updating ECPA

Because these inadequate legal standards create difficulties for Internet users and businesses alike, a coalition of privacy advocates and businesses—from the American Civil Liberties Union to Google and AT&T—has formed to urge Congress to update electronic privacy law to provide clear rules and better protection for electronic data. The coalition believes that just as the law recognized that storing information in digital form on a computer hard drive should have the same probable cause warrant protection as information stored in paper form in a filing cabinet, the time has come to ensure that these same privacy protections apply to digital information stored in the cloud.

The ACLU believes the efforts being urged by the coalition to update ECPA are critical first steps but believes a full review of ECPA should involved all of the following issues:

1. Robustly Protect All Personal Electronic Information.
2. Safeguard Location Information.
3. Institute Appropriate Oversight and Reporting Requirements.
4. Require a Suppression Remedy.
5. Craft Reasonable Exceptions.

Robustly Protect All Personal Electronic Information.

In the modern world, just as in Jefferson's time, our personal, private information—whether paper documents and correspondence or records of what we search and read online—reveals a tremendous amount about us. Our right to privacy and our rights to free expression and free association require that this information be protected from disclosure to the government without notice and without a warrant based on probable cause. Changing technology must not erode these protections. Our e-mail, online spreadsheets and photos, and other digital documents need strong legal protections regardless of how, where, or how long they are stored.

Congress has long-recognized the privacy interests in the transactional records of users of expressive material. The Video Privacy Protection Act prohibits disclosure of video viewing records without a warrant or court order, requires notice prior to any disclosure of personally identifiable information to a law enforcement agency, and requires the destruction of personally identifiable information one year after it becomes unnecessary.[27] The Cable Communications Policy Act similarly prohibits disclosure of cable records absent a court order.[28] Similarly, to safeguard autonomy, privacy, and intellectual freedom, our laws extend protection to library and

[27] 18 U.S.C. § 2710(b)(2)(B), (b)(3),(e) (2009).
[28] 47 U.S.C. § 551(c) (2008).

book records.[29] We need the same protection for digital records that implicate our First Amendment freedoms by recording our expressive actions and choices.

Current loopholes in our privacy laws need to be closed to protect electronic information without regard to its age, whether it is "content" or "transactional" in nature, or whether companies or individuals can use this information for other purposes. ECPA must be modernized to provide robust protection for all personal electronic information and require a probable cause warrant and notice prior to disclosure.

Safeguard Location Information.

The vast majority of Americans own cell phones. The location information transmitted by these phones every minute of every day reveals not only where we go but often what we are doing and who we are talking to. Americans take cell phones everywhere: to gun rallies, to mental health clinics, to church, and everywhere else we go. Ubiquitous tracking is a reality in the United States. We must protect this sensitive information from inappropriate government access. Location information, whether current or historical, is clearly personal information. The law should require government officials to obtain a warrant based on probable cause before allowing access.

Institute Appropriate Oversight and Reporting Requirements.

Electronic recordkeeping enables easy collection and aggregation of records, and the insufficient and outdated standards applied by ECPA provide little barrier should the government wish to engage in a "shopping spree" through the treasure trove of personal information held by private companies. In addition to updating the standards for access to electronic information, ECPA should ensure adequate oversight by Congress and adequate transparency to the public by extending existing reporting requirements for wiretap orders to all types of law enforcement surveillance requests.

The House Judiciary Committee recognized this need when it passed HR 5018 (106th Congress) by a vote of 20-1.[30] The proposed bill would have required reporting on all orders, warrants, or subpoenas issued by government entities seeking electronic communications records or content information. Current efforts to modernize ECPA should include this requirement as well.

---

[29] 48 states protect library reading records by statute, *see, e.g.*, N.Y. C.P.L.R. § 4509; Cal. Gov. Code §§ 6267, 6254(j), and federal and state courts have also often frowned upon attempts by the government or civil litigants to gain access to such records, *see, e.g.*, *In re Grand Jury Subpoena to Amazon.com*, 246 F.R.D. 570, 573 (W.D. Wis. 2007) (quashing a government subpoena seeking the identities of 120 book buyers because "it is an unsettling and un-American scenario to envision federal agents nosing through the reading lists of law-abiding citizens while hunting for evidence against somebody else."); *In re Grand Jury Subpoena to Kramerbooks & Afterwords, Inc.*, 26 Media L. Rep. (BNA) 1599, 1601 (D.D.C. 1998) (First Amendment requires government to "demonstrate a compelling interest in the information sought . . . [and] a sufficient connection between the information sought and the grand jury investigation" prior to obtaining book records); *Tattered Cover v. City of Thornton*, 44 P.3d 1044, 1059 (Colo., 2002) (government access to book records only passes muster under Colorado Constitution if "warrant plus" standard is met by the government—i.e. prior notice, adversarial hearing, and showing of a compelling need).

[30] H.R. Rep. No. 106-932 to accompany H.R. 5018 (2000) at 23.

Require a Suppression Remedy.

Both the Fourth Amendment and the Wiretap Act provide for an exclusionary remedy: if a law enforcement official obtains information in violation of a defendant's constitutional privacy rights or the Act, that information usually cannot be used in a court of law.[31] The same rule, however, does not apply to electronic information obtained in violation of ECPA. Without an exclusionary rule, there is a lack of deterrence for government overreaching. Unlawfully obtained electronic information should be barred from use in court proceedings. A suppression remedy provision passed the House Judiciary Committee in 2000 as part of HR 5018 and should be included in any current Congressional language to modernize ECPA.[32]

Craft Reasonable Exceptions.

Overbroad exceptions and the abuse of "voluntary disclosure" procedures are also depriving Americans of their rightful privacy protection. ECPA needs to be revised to close these loopholes and ensure that private information is only released outside of the standard process when truly necessary.

Under previous law, a company could only turn records over if it had a "reasonable belief" that there was an emergency involving "imminent harm" of death or injury to any person. However, in 2001 that standard was lowered so that the company's belief only needed to be held in "good faith" and that the harm no longer needed to be imminent. This lowered standard reduced a company's obligation to ensure that its decision to release private information about a user was balanced by the exigency of the situation.

In addition, exceptions to prohibitions on "voluntary" disclosure need to be revised to prevent coercive abuse by law enforcement. For example the Inspector General for the Department of Justice has reported that the FBI circumvented its National Security Letter (NSL) authority by using "exigent letters" to obtain information with the promise that the agent had already requested a grand jury subpoena or an NSL.[33] To prevent such abuse, all requests for "emergency" voluntary disclosures under ECPA should clearly state that compliance with the request is voluntary and ECPA should require thorough documentation and reporting of all such requests.

Exceptions to the procedural requirements for government access to electronic records should be just that: exceptional. ECPA reform should restore the original emergency exception for ECPA and require documentation and reporting to ensure that these exceptions are used properly and not abused.

---

[31] 18 U.S.C. 2515.

[32] Electronic Communications Privacy Act of 2000, H.R. 5018, 106th Cong. § 2 (2000).

[33] Dep't. of Justice, Office of Inspector General, A Review of the Federal Bureau of Investigation's Use of National Security Letters (March 2007), at 86–97, *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf.

Conclusion

We applaud the Committee for holding this hearing and for beginning to undertake the task of reforming ECPA. Changes in the way we communicate with each other in today's world are wondrous viewed through 1980's spectacles. That wonderment should not be tempered by the realization that our personal privacy is slipping away. Comprehensive reform of ECPA is a needed legislative initiative that will help preserve the real innovative value of the technology boom and set us on a path for even greater innovation to come.

Federal Bureau of Investigation
Agents Association

May 6, 2010

The Honorable Jerrold Nadler
Chair
Subcommittee on the Constitution,
Civil Rights, and Civil Liberties
House Judiciary Committee
2138 Rayburn House Office Building
Washington, DC 20515

The Honorable F. James Sensenbrenner
Ranking Member
Subcommittee on the Constitution,
Civil Rights, and Civil Liberties
House Judiciary Committee
2142 Rayburn House Office Building
Washington, DC 20515

Re: ***Hearing on Electronic Communications Privacy Act Reform***

Dear Mr. Chairman and Mr. Sensenbrenner:

On behalf of the FBI Agents Association (FBIAA), a professional association comprised of active and retired FBI Agents with a membership of nearly 12,000 Agents nationwide, I write to express our appreciation for your investigation into the need to reform the Electronic Communications Privacy Act ("ECPA"), and our hope that you will take the necessary actions to ensure that ECPA is reformed in a manner that best protects privacy and facilitates effective law enforcement efforts.

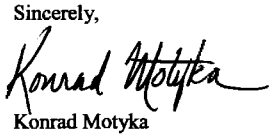
The FBIAA understands that ECPA needs to be reformed as a result of the significant changes in technology and privacy concerns that have occurred since its adoption. FBI Agents are committed to protecting our Constitution and the civil liberties of citizens who fear that technological changes have resulted in new threats to their privacy. FBI Agents are also aware of the fact that criminal and terrorist enterprises are able to exploit privacy protections to advance their criminal ends, just as they have been able to exploit weaknesses in privacy protections to take advantage of US citizens. Therefore, laws such as ECPA must always carefully balance these interests in order to ensure that the goals of safety and privacy are both served by legislation.

As you move to reform ECPA, we hope that you will carefully consider the law enforcement implications of any changes, and propose changes that can help law enforcement become more effective without sacrificing civil liberties. The FBIAA and its members will be pleased to assist in this effort as you move forward.

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

The FBIAA appreciates your efforts and thanks you for considering these concerns.

Sincerely,



Konrad Motyka

President

○