AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

ECPA REFORM AND THE REVOLUTION IN CLOUD COMPUTING

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

SEPTEMBER 23, 2010

Serial No. 111–149

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

58–409 PDF WASHINGTON : 2010

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

COMMITTEE ON THE JUDICIARY

JOHN CONYERS, JR., Michigan, *Chairman*

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

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

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

SUBCOMMITTEE ON THE CONSTITUTION, CIVIL RIGHTS, AND CIVIL LIBERTIES

JERROLD NADLER, New York, *Chairman*

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

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

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

CONTENTS

SEPTEMBER 23, 2010

Page

OPENING STATEMENTS

The Honorable Jerrold Nadler, a Representative in Congress from the State of New York, and Chairman, Subcommittee on the Constitution, Civil Rights, and Civil Liberties 1
The Honorable Trent Franks, a Representative in Congress from the State of Arizona, and Member, Subcommittee on the Constitution, Civil Rights, and Civil Liberties 3
The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, Chairman, Committee on the Judiciary, and Member, Subcommittee on the Constitution, Civil Rights, and Civil Liberties 4

WITNESSES

Mr. Edward W. Felten, Director, Center for Information Technology Policy, Princeton University
Oral Testimony 10
Prepared Statement 12
Mr. Richard Salgado, Senior Counsel, Law Enforcement and Information Security, Google, Inc.
Oral Testimony 17
Prepared Statement 19
Mr. Mike Hintze, Associate General Counsel, Microsoft Corporation
Oral Testimony 24
Prepared Statement 26
Mr. David Schellhase, Executive Vice President and General Counsel, Salesforce.Com
Oral Testimony 39
Prepared Statement 41
Mr. Perry Robinson, Associate General Counsel, Rackspace Hosting
Oral Testimony 55
Prepared Statement 57
Mr. Paul Misener, Vice President for Global Public Policy, Amazon.Com
Oral Testimony 64
Prepared Statement 66
Mr. Kevin Werbach, Professor, The Wharton School, University of Pennsylvania
Oral Testimony 78
Prepared Statement 80
Mr. Fred H. Cate, Professor, Director, Center for Applied Cybersecurity Research, Indiana University
Oral Testimony 91
Prepared Statement 93
Mr. Thomas B. Hurbanek, Senior Investigator, Computer Crime Unit, New YorK State Police
Oral Testimony 101
Prepared Statement 104
Mr. Kurt F. Schmid, Executive Director, Chicago High Intensity Drug Trafficking Area Program
Oral Testimony 109
Prepared Statement 112

Page

Mr. Marc J. Zwillinger, Zwillinger Genetski, LLP
Oral Testimony 118
Prepared Statement 121

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Prepared Statement of the Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, Chairman, Committee on the Judiciary, and Member, Subcommittee on the Constitution, Civil Rights, and Civil Liberties 6

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the Honorable Henry C. "Hank" Johnson, Jr., a Representative in Congress from the State of Georgia, and Member, Subcommittee on the Constitution, Civil Rights, and Civil Liberties 137
Response to Post-Hearing Questions from Richard Salgado, Senior Counsel, Law Enforcement and Information Security, Google, Inc. 139
Response to Post-Hearing Questions from Mike Hintze, Associate General Counsel, Microsoft Corporation 143
Letter from the Federal Law Enforcement Officers Association 147
Prepared Statement of the Competitive Enterprise Institute (CEI), The Progress & Freedom Foundation, Citizens Against Government Waste, Americans for Tax Reform, and the Center for Financial Privacy and Human Rights 150

ECPA REFORM AND THE REVOLUTION IN CLOUD COMPUTING

THURSDAY, SEPTEMBER 23, 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 11:08 a.m., in room 2141, Rayburn House Office Building, the Honorable Jerrold Nadler (Chairman of the Subcommittee) presiding.

Present: Representatives Nadler, Conyers, Watt, Johnson, and Franks.

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

Mr. NADLER. This hearing of the Subcommittee on the Constitution, Civil Rights, and Civil Liberties will come to order. To begin with I will recognize myself for an opening statement.

Today's hearing is the third in which this Subcommittee will consider the statutory framework Congress established in the 1986 Electronic Communications Privacy Act, ECPA, in light of the enormous technological advances in electronic communications in the 24 years since ECPA's passage. At the last hearing we learned about advancements in cellular location-based technologies and related services and how such technologies, while enriching our lives, could provide law enforcement with more precise, and to many of us more sensitive, information about where we may be located at any given time.

Today we will continue our examination of whether ECPA still strikes the right balance among the interests and needs of law enforcement, industry, and the privacy interests of the American people by discussing a new technology commonly referred to as cloud computing. It is important that the law sustain the public's confidence in the security and privacy of their communications and information. That confidence is absolutely essential to fostering the emerging market for cloud computing services and the rapid innovation that is fundamental to that market's health.

This Subcommittee's exploration of where the appropriate balance may lie with respect to the content and associated transactional information of electronic communications and data stored by certain third party providers must begin with a lesson about cloud computing technologies and capabilities. When ECPA was

passed back in 1986 few of us used e-mail or imagined a world where we could securely share information and edit electronic documents online with our colleagues or where, again online, a business could input, store, process, and access all data necessary for the management of its business processes, from sales to customer service.

That world is here and it promises tremendous efficiencies for government, private industry, and individuals. It is an exciting technological advance and we must ensure that the law keeps pace in a manner that protects this market, protects the rights of consumers and the government's law enforcement responsibilities.

We are fortunate to have two distinguished panels of witnesses who bring a great deal of expertise to both the legal and technological issues before us, including witnesses who represent five major U.S. cloud computing companies.

I should mention at this point that—and if I am wrong someone will correct me, I am sure, at some point today—cloud computing simply means—or the cloud simply means where the data is stored on a third party's server—not in your home, but on somebody else's server, so it is not given as much privacy protection under current law as if it were on your own computer at home.

Along with other experts our witnesses today will educate us about what is happening in the cloud today and discuss the type of laws and rules that industry needs to promote the continuing innovation and growing efficiency that cloud computing affords to individuals and businesses of all types and sizes. This initial educational effort is, in my view, not only warranted but essential before we undertake any effort at amending or otherwise reforming ECPA.

In many respects, at least for the moment, the testimony we hear and discussions we have today may raise more questions than they answer. Since we are to hear about technologies, both existing and perhaps yet to come, that are revolutionary—certainly by 1986 standards—I want to acknowledge that our task will be a challenge to find the appropriate balance between privacy and law enforcement interests, to protect the public while preserving consumer privacy and confidence, to support rapid technological innovation and growth yet discern standards for law enforcement access that will not become outdated with each new generation of technology, which is to say every 6 months or so.

Just as it would not have been possible for Congress to anticipate the exciting technologies we will be discussing today it is more than likely that in the years to come new technologies will present us with equally vexing legal questions. We must learn to take advantage of these emerging technologies without ushering in a new privacy-free civilization, to boldly go toward the creation of a new productive balance among the interests of law enforcement, personal privacy, and industry that no legislation has quite stricken before.

This Subcommittee needs the assistance and input of all stakeholders—law enforcement, private industry, and civil liberties groups alike—to get this balance right, hopefully for at least another generation. I look forward to the testimony of our witnesses

today and to working with all stakeholders on this very timely mission.

I yield back the balance of my time and I now represent the distinguished—I now recognize, rather, the distinguished gentleman from Arizona.

Mr. FRANKS. Well, thank you, Mr. Chairman.

Thank all of you for being here.

And we are grateful that you are holding this hearing examining the need to update the Electronic Communications Privacy Act of 1986, or ECPA, as it relates to cloud computing. This is the third in a series of hearings to examine ECPA and possible ECPA reforms. I can say, if there is one thing I hope or believe we can all agree upon it is that we don't have a precise definition of cloud computing, and as someone said, there is an old quote that said, "The secret to the universe is in the true naming of things." It often means different things to different people.

Today we will hopefully learn exactly what the cloud is and have a better understanding of how, if at all, ECPA falls short of addressing this new technology. Some proponents of ECPA reform propose requiring a search warrant for communications in the cloud, regardless of the age of those communications, how they are stored, or how they are accessed. This would be a fairly significant departure from current law.

The information possessed by law enforcement in the very early stages of an investigation does not always have to lend itself to establishing probable cause for the purposes of obtaining a search warrant. A blanket warrant requirement for communications in the cloud, regardless of how or where they are stored, could potentially deprive law enforcement officials of essential building blocks for criminal investigations and may actually deprive them of their ability to establish probable cause for wire taps, physical searches, or arrests.

I am always mindful of the potential encroachment on individual liberty and privacy by new technologies and I have tried to be one of the first to defend those rights. However, I will also be one of the first to protect the legitimate needs of law enforcement, including their ability to keep pace with rapidly changing technologies.

Now, I am not aware of any of the practices by law enforcement that have inhibited the use of the development of these services. I am also not aware of any practices by the law enforcement authorities that have discouraged the willingness of individuals or businesses to store data in the cloud.

There may very well be a need to clear up statutory ambiguities so that the police know what they have to do to obtain certain information and service providers know what they have to do, in terms of the law, to provide that information. But I am concerned that the increasing—I am concerned that increasing the evidentiary standard to such a degree as some have proposed would create a hurdle that is simply too high to clear.

Cloud technology is a significant advancement in how we send, store, and process a very large array of data. Companies that provide these services have a vested interest in assuring a certain level of privacy to their customers, and obviously this has to be

weighed against the government's legitimate need to access this data.

And while we consider these issues I believe we must also be cognizant of other privacy-related issues. We should not simply focus on revising or restricting law enforcement access to the cloud; we must also be aware of who owns the cloud, who has access to the cloud, and whether there are sufficient safeguards to protect the cloud against criminal and foreign adversaries.

Creating barriers to law enforcement in the name of privacy may have the unintended consequence of inhibiting law enforcement investigations into data breaches and other privacy intrusions by hackers and spies and the like. ECPA reform is simply not about Federal investigations—or I should say it is not simply about those things. These laws govern every criminal investigation in the country.

For this reason this Committee must be thoroughly balanced and informed in any ECPA reform it undertakes, and I hope all of you can help us understand the best way to move forward. I am grateful that you are here. I thank every one of you, look forward to your testimony, and yield back.

Mr. NADLER. I thank the gentleman.

I will now recognize for an opening statement the distinguished Chairman of the full Committee, the gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Thank you, Chairman Nadler, and Trent Franks. I am always glad to be here with us three and the staff.

As if this is not an important issue, I think it is being very undervalued by many on our Committee, certainly not those of you that have taken time to join us here in the hearing room today.

It just so happens that I was the only one here in 1986, and that is not to date myself, but the one thing I can't remember right now is whether the Chairman of the Committee was Jack Brooks or Peter Rodino. I am inclined to think it was Jack Brooks, of Texas, but we are researching it right now.

Now, so far when we start talking about the reform and how—what we ought to consider it turns on whether or not we are going to restrict privacy or, in the name of law enforcement, we are going to be able to be more invasive. And sure enough, Trent Franks runs right into the conservative position of wanting to let the law enforcement people have their way more. And I am just predicting this; he didn't really come out and say it, but we have been listening to each other now for a growing period of years.

But is there something else involved here? And I am so glad we have got the witnesses here today.

Of course we are going to have to balance it, but, you know, I am listening to questions of whether or not we are going to be able to work out agreements over cyberspace differences that are now becoming more discussed in our world. We now find out that not only do we have arms race control and nuclear control, we now have the whole question of how we can create severe damage to civilian populations through dismantling and disabling their cyber connections in terms of conflict.

And so we move into this, I hope, not just worrying about how much law enforcement leeway are we going to get? Of course we

want to protect our people's privacy as much as possible, but at the same time there seem to me to be other issues that I am hoping that you will bring up that are related to who is going to control and what happens—is this an infinite growth situation that we are in? Are there limits? Are we going to run out of what we need to work with or not? Or are there other considerations?

And it is in that spirit that I join you today, and also ask unanimous consent to put my written statement in the record.

Mr. NADLER. Without objection.

Mr. CONYERS. Thank you, Mr. Chairman.

[The prepared statement of Mr. Conyers follows:]

Statement of the Honorable John Conyers, Jr.

for the Hearing on
ECPA Reform and the Revolution in Cloud Computing
Before the Subcommittee on the Constitution, Civil Rights and Civil Liberties

Thursday, September 23, 2010, at 11:00 a.m.
2141 Rayburn House Office Building

E-mail and other Internet-based communication services offered by cloud computing companies have provided all of us with new and innovative ways of communicating and accessing information. Clearly, most Americans consider these technologies to have generally enriched their lives.

Many of us no longer store things on hard drives. And, we don't worry about our computers crashing and losing our work when we store our information "in the cloud."

Cloud computing technology – an Internet-based computing system where shared resources, software, and information are provided to computers and other devices on demand – is also emerging as an important engine for economic growth.

The growth of Internet-based communications, business applications, and storage has also provided law enforcement agencies with new capabilities they can use to locate and obtain information about criminal activity and actors.

Of course, with the appearance of such enhancements in investigative capabilities – particularly through tools that can reveal the actual content of communications – comes an increased need to assess the pressures such new technologies place upon our civil liberties, and to attempt to strike an appropriate balance of interests.

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

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

The more I learn about how the Electronic Communications Privacy Act gives less privacy protection to content stored "in the cloud," than content stored "at home," the more I think the balance is out of kilter.

If we can strike the correct balance here, we will not only ensure that the public is protected from unreasonable government intrusions upon its privacy.

We will also enhance the continued growth of cloud computing services themselves by ensuring that law enforcement cannot obtain access to private information without first meeting an appropriate, clearly expressed legal standard.

As this hearing examines the Electronic Communications Privacy Act Reform with respect to cloud computing, I would like to raise several key issues for consideration.

First, has the growth of cloud computing technology, which allows more and more individuals and businesses to store their information on third-party servers, rendered important content protections in the Electronic Communications Privacy Act less effective?

For example, does the Electronic Communications Privacy Act provide a lower level of protection for content stored on third-party servers than it does for the same information stored on a personal laptop, desktop, or local business server?

Second, if there are disparities in the level of privacy protections provided to information stored on a third-party server versus a local server, how does this affect the long-term growth of cloud computing technologies?

Is there a danger that consumers will lose confidence in cloud computing technologies if there are not clear, consistent, technology-neutral rules governing law enforcement access to information stored by third-party providers?

Do inconsistencies of this kind have a potential to skew the market for cloud computing services detrimentally?

Third, does the growth of cloud computing services and technologies – where, for example, documents can be edited by multiple users via the Internet – make application and compliance with the Electronic Communications Privacy Act a challenging endeavor for cloud computing companies?

Has technology so outpaced the law that some of the concepts and legal distinctions envisioned by the Electronic Communications Privacy Act of 1986 now have the unintended effect of frustrating business efficiency and innovation, both for cloud computing companies and their business customers?

I understand that we will hear today from several distinguished witnesses, including representatives from five major U.S. cloud computing companies.

Many of these companies are competitors, and I appreciate your willingness to come together today and educate us about important privacy, law enforcement, and business issues concerning the Electronic Communications Privacy Act.

It is my belief that your willingness to participate in this process – openly and on the record – will help us produce a more objective, more universally beneficial and acceptable piece of legislation in the end.

These are challenging issues, and I want to thank my good friends, Jerry Nadler and Jim Sensenbrenner, for addressing them today, and to thank all our witnesses for helping us to continue our dialogue about Electronic Communication Privacy Act reform by contributing their testimony and expertise.

Mr. NADLER. Thank you.

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 at any point. We will now turn to our first panel of witnesses, and instead of reading the usual boilerplate about our procedures

we will follow the Committee's usual procedures of questioning witnesses.

Our first witness will be Edward Felten, who is a professor of computer science and public affairs at Princeton University and is the founding director of Princeton's Center for Information Technology Policy. His research interests include computer security and privacy, especially relating to the Internet and computer product—and consumer products, and technology law and policy.

He received his Ph.D. in computer science and engineering from the University of Washington, an M.S. in computer science and engineering from the University of Washington, and then his B.S. in physics with honors from the California Institute of Technology.

Richard Salgado, our next witness, is a senior counsel with Google for information, security, and law enforcement matters. Prior to joining Google Mr. Salgado worked at Yahoo, focusing on international security and compliance.

He also served as senior counsel in the computer crime and intellectual property section of the United States Department of Justice. Mr. Salgado received his law degree from Yale Law School.

Michael Hintze is an associate general counsel in Microsoft Corporation's legal and corporate affairs group. He joined Microsoft in 1998 and his practice currently includes a number of regulatory and public policy issues, including privacy, security, telecom, online safety, and free expression matters worldwide. Mr. Hintze is a graduate of Columbia University School of Law.

David Schellhase is—I hope I got that right—thank you—David Schellhase is executive vice president and general counsel of Salesforce.com, Inc., where he leads the legal, internal audit, and public policy teams. Mr. Schellhase joined Salesforce.com in 2002 and has practiced law in the technology industry for 20 years. Mr. Schellhase is a graduate of Cornell Law School.

Perry Robinson is associate general counsel at Rackspace Hosting. Mr. Robinson oversees Rackspace's program for compliance with state and Federal law enforcement agency requests and leads their legal team on contractual matters relating to the provision of services to Rackspace's customers. Mr. Robinson earned his J.D. from Baylor Law School.

Paul Misener is Amazon.com's vice president for global public policy and has served in this position for a decade. He is responsible for formulating and representing the company's public policy positions worldwide as well as for managing policy specialists in Asia, Europe, and North America. Mr. Misener received his J.D. from George Mason University.

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.

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

Before we begin it is customary—well, let me just say before we do this, the Chair reserves for himself the right to recess the hearing, which I anticipate doing only if there are votes on the floor. Before we begin it is customary for the Committee to swear in its witnesses.

If you would please stand and raise your right hands to take the oath?

Let the record reflect that the witnesses answered in the affirmative, and you may, of course, be seated.

I will now recognize for 5 minutes our first witness, Professor Felten, and use your mic please.

TESTIMONY OF EDWARD W. FELTEN, DIRECTOR, CENTER FOR INFORMATION TECHNOLOGY POLICY, PRINCETON UNIVERSITY

Mr. FELTEN. A lot has changed on the Internet since ECPA was passed in 1986. Back then there were only a couple thousand computers online. Commercial activity was strictly forbidden; the Net was only for research and education purposes. And several of the companies represented on this panel did not even exist. The eventual founder of Facebook was 2 years old.

The computers at that time would not even be recognizable to today's teenagers; the equipment is vastly different. Today's cell phones are vastly better than the super-computers of 1986. But more important than these changes in equipment and sheer numbers of computers has been the change in the way people use the Internet, and one of the big changes there has been the move to cloud computing.

As you said before, Mr. Chairman, the defining characteristic of cloud computing is that a person is—a person or company is taking their data and moving it onto someone else's computer, and along with that taking the computation and other management functions and putting those as well onto someone else's computer, typically a service provider's computer. Cloud computing is used both by individuals and by businesses large and small.

To give an example of the use of cloud computing by an individual let me talk about my own use of my personal calendar. I keep my calendar in the cloud. I have a deal with the service provider in which they support that.

And that provides a number of advantages to me. First, it means that the data and the systems are professionally managed.

The computers that store the master copy of my calendar are run by the service provider and not by me; the service provider's employees take care of backing up the data, maintaining security, keeping everything up-to-date, and keeping everything running. I don't have to worry about that at all.

The second advantage is that my calendar is accessible to me anywhere—on my desktop computer, on my laptop computer, on my mobile phone. The service provider gives me software that runs on all of those devices and that software always gets an up-to-date copy of my calendar. If I change something in one of those places it is immediately reflected in the master copy and then in the other copies so that there is a single view of my calendar which I always see regardless of where I am.

And the third main advantage is that it is easily shareable. I can give my wife, and my colleagues, and my students access to my calendar and they can see what I see in real time. Some of them, with my permission, can modify the calendar; others can just see.

Any kind of service which would benefit from these advantages of professional management, accessibility anywhere, and sharing can be put in the cloud and typically is, and there are many examples of different kinds of services that happen in the cloud—e-mail, document management, investment tracking, photo sharing, project management, hard drive backup, and many more.

Cloud computing is also valuable for businesses. A business can take some of their back office computing operations—things like payroll, sales, and inventory—and move those into the cloud.

They can also move their consumer facing technology infrastructure into the cloud. For example, an ecommerce company might take these servers that provide their image to customers and that customers interact with and put those in the cloud by hiring out that function to someone else.

Even companies that are technically sophisticated often do this because they find it cheaper, due to the economies of scale, in having things centrally managed. As another example, I wrote my written testimony that was submitted earlier in a cloud document-editing system, and I did that because it was easy for me to use across devices, and because when I wanted someone to review the document and give me feedback they could easily do that by using the same cloud service, and we could interact and edit in real time.

Now, in an ideal world people would be making the decision to use the cloud or not use the cloud based on considerations of technical efficiency and cost. They would be balancing those factors and deciding to do whatever was best in their individual case. But to the extent that a law like ECPA puts its thumb on the scale and pushes people toward putting their data and functions in the cloud or moving them out of the cloud you end up with solutions that are less technically efficient, more expensive, and harder to use, and you end up ultimately with less innovation in technology and in business processes.

Thank you.

[The prepared statement of Mr. Felten follows:]

PREPARED STATEMENT OF EDWARD W. FELTEN

Testimony of Edward W. Felten
Professor of Computer Science and Public Affairs, Princeton University

United States House of Representatives, Committee on the Judiciary
Subcommittee on the Constitution, Civil Rights, and Civil Liberties
Hearing on
ECPA Reform and the Revolution in Cloud Computing
September 23, 2010

Chairman Nadler, Ranking Member Sensenbrenner, and members of the committee, I thank you for the opportunity to testify about cloud computing and the Electronic Communications Privacy Act (ECPA).

My name is Edward W. Felten. I am a Professor of Computer Science and Public Affairs at Princeton University. I also serve as the founding Director of the Center for Information Technology Policy, an interdisciplinary research and teaching center at Princeton that focuses on public policy issues relating to computing, communications, and the Internet. My primary background is in computer science, and my main subfields in computer science include security and privacy, and Internet technologies. I have served as an advisor or consultant to the U.S. Departments of Defense, Homeland Security, and Justice, and the Federal Trade Commission. I have testified several times previously before House hearings and once before a Senate hearing. I am a Fellow of ACM, the leading professional society for computer scientists, and I serve as Vice-Chair of USACM, which is ACM's U.S. Public Policy Council.

I have been asked to testify about cloud computing technology and its impact on the security and privacy issues implicated by ECPA.

Changes Since 1986

In 1986, when ECPA was passed, the Internet consisted of a few thousand computers. The network was run by the U.S. government for research and education purposes, and commercial activity was forbidden. There were no web pages, because the web had not been invented. Google would not be founded for another decade. Twitter would not be founded for another two decades. Mark Zuckerberg, who would grow up to start Facebook, was two years old.

In talking about advances in computing, people often focus on the equipment. Certainly the advances in computing equipment since 1986 have been spectacular. Compared to the high-end supercomputers of 1986, today's mobile phones have more memory, more computing horsepower, and a better network connection—not to mention a vastly lower price.

But even more important than changes in the equipment have been the changes in how people use the Internet and the role it plays in their everyday lives. From wedding photos to financial records, from love letters to business plans, from grocery lists to boarding passes, the records of our lives are increasing created and archived online. Even those few who don't use the Internet and don't have mobile phones will leave extensive electronic trails online, including their health records and financial transactions.

Cloud Computing for End Users

One of the biggest changes, driven by the vast improvements in storage and networks, has been the shift to cloud computing. At the most basic level, cloud computing means that your data is stored on somebody else's computer. Rather than keeping the only copy of your data on your own computer, you rent computing resources from a service provider, and that provider keeps the primary copy of your data and manages its use. You access the data across the Internet, using your own computer(s).

For example, I use a cloud service to manage my calendar. Keeping my calendar in the cloud has several advantages:

- *professionally managed:* The computers that store the master copy of my calendar are managed by the service provider's employees. They take care of backing up data, maintaining security, and updating software.
- *accessible anywhere:* I can access my calendar from my desktop computer, my laptop, or my mobile phone. If I make a change to my calendar on one of these devices, the change is visible instantly on the others. I don't have to worry about keeping the copies "in sync" because that happens automatically. I can even work while disconnected from the Internet (on an airplane, or in the subway); when I reconnect, any changes made while I was disconnected will be reconciled.
- *easily sharable*: I can give others access to my calendar. My wife can see everything; my students can see when I'm scheduled to be in my office. If I schedule a new appointment, this is visible to all of them right away.
- *supports collaboration*: People can share a calendar, to schedule access to a shared resource such as a conference room or piece of equipment.

Technologically, this kind of cloud service is implemented by cooperation between a server and a set of end-user devices. The server computer sits in the service provider's data center, and acts as the "boss," coordinating the participating devices and storing the archival, master copy of my calendar. People interact with the system on end-user devices such as my desktop computer, my laptop computer, and my mobile phone. The end-user devices get information as necessary from the server, display the information to the user, and tell the server about any modifications that the user makes to the information, such as any new appointments added to the calendar. Together, the server and devices provide the user with the illusion that all of the end-user devices have a view onto a single, shared calendar.

From the standpoint of user experience, a cloud service might look a lot like a traditional local service: information is viewed and manipulated using the local device's display and keyboard, and the information is always available just as if it were stored locally. A less sophisticated user might not even realize that he is using a cloud service, unless he notices that the same data is also available on another device and he stops to think about how this is accomplished.

Many types of services are provided in the cloud. Common examples include email (Yahoo Mail, Microsoft's Hotmail, Google's Gmail), document management (Google Docs, Microsoft Office Live, Zoho Office), investment tracking (Mint, Wesabe), photo-sharing (Flickr, Picasa), project management

(Basecamp, Goplan), hard-drive backup (Mozy, Dropbox), and many more. Any computer-based activity that will benefit from the advantages listed above can be, and probably is, offered via the cloud.

Services provided via the cloud often substitute for traditional packaged software. Rather than buying a software product, installing it on my computer, and using it to manage data locally on my computer, I might subscribe to a cloud service that provides similar functionality via the cloud. This latter approach is sometimes called "Software as a Service" (abbreviated "Saas"). Alternatively, a user might choose to use a cloud service in conjunction with traditional desktop software.

Cloud Computing for Businesses

End users are not the only ones who can benefit from outsourcing their information management. A business can put its back-office (i.e., payroll, sales, inventory, etc.) and customer-facing computing infrastructures "in the cloud" by contracting with a service provider to lease access to resources in the provider's data center. In the limiting case, the business would not run its own data center at all, but would build all of its computing functionality (other than employees' desktop computers) to operate in the service provider's data center. The business would essentially be putting its computing infrastructure into the cloud, in the same way I put my calendar into the cloud. This approach is sometimes called "Infrastructure as a Service" or "IaaS."

Doing this poses obvious trade-offs for the business. On the one hand, it loses some control over its computing infrastructure and becomes vulnerable to failures by the service provider. On the other hand, it benefits from the economies of scale inherent in the service provider's larger data center operation, which can lead to lower cost, higher reliability, better energy efficiency, and more professional security management.

Even high-tech start-up companies often turn to the cloud for their computing resources. Although a start-up might have the engineering expertise needed to build and run a data center, it might prefer to outsource that function and have its engineers work on product development instead. An additional benefit is scaling: if the start-up's business grows rapidly and it needs to expand its computing capacity dramatically to handle a flood of new customers, this is easily done in the cloud, by simply increasing the number of servers the start-up is renting from the provider. Some cloud providers allow their customers to change their resource allocations in nearly real time, something that would not be possible for a customer that operated its own data center.

The point of this discussion is not that everyone should be using the cloud, but that cloud computing offers important advantages which, despite its disadvantages, will make the cloud the right choice for many businesses.

An Example: My Own Use of the Cloud

To illustrate the usefulness of cloud computing, and the variety of cloud services available, let me describe how I use the cloud, as an end user and as the manager of a research group.

As an end user, I keep essentially all of my personal and business data in the cloud. (The only exceptions are a few documents and emails which colleagues or clients ask me to store locally.) Because of the nature of my job I am often on the move, either across the campus or across the country. The ability to access all of my data wherever I am, without having to remember to copy data from here to there or to do an explicit "sync" operation before switching devices, is key to working efficiently while on the move.

By keeping my information in the cloud I can have access to it anywhere, and as a bonus I don't have to worry about backing up the data because I know there is always a safe copy on the cloud provider's system. If my laptop computer were destroyed today, I could carry on without loss of data. I would simply get a new laptop, log it in to my accounts on various cloud services, and get back to work, confident that my data would be streamed across the Internet to my new laptop as needed.

I use commercial cloud services to manage my email and calendar. My calendar is shared with my family, colleagues, and students (with appropriate levels of access for each person) as described above. I often use a commercial cloud service to store and edit documents. Any software code and technical reports on which I'm working are stored in the cloud via a version-management tool called "git." I manage other miscellaneous files using a cloud backup/synchronization service which automatically copies new or modified files to a cloud server and then onto my other computers. My wife and I store our grocery shopping list in the cloud; if my wife adds milk to the shopping list, this will show up on my mobile phone when I get to the store; when I check the box to say I have bought milk, this will be visible on her phone so she won't accidentally buy milk too.

I wrote this testimony using a cloud editing and document management service. I did some of the writing on my desktop computer and some on my laptop; the editing windows on the two devices were always in sync. When I wanted to ask a few colleagues for feedback on a draft, I shared the cloud document with them, and they wrote comments in the (virtual) margins. I could see their comments in real time, and my colleagues could see me editing to address their comments.

Beyond my personal use of the cloud, I also use the cloud in my research and administration role. My group at Princeton builds various public web sites and tools, which are typically run or hosted using cloud resources that we rent. Although we could run our own servers, this is not cost-effective for us—we can save money and be more agile by renting cloud space for many research purposes.

The Cloud and ECPA

I am not a lawyer, so I will not offer testimony on how ECPA should, or does, apply to data kept in the cloud. However, I understand that the legal treatment of information under ECPA can depend on whether that data is held directly by the user or business, or by a third-party.

In some cases it may be difficult for a user to tell whether or not his data is stored in the cloud, because cloud services can offer nearly the same user experience as local services. This could cause legal uncertainty if the legal status of data depends on whether or not it is stored in the cloud. Even if a user or business knows that data is stored in the cloud, it might not be clear exactly where the data is stored.

From the standpoint of technical and economic efficiency, the cloud offers substantial advantages for at least some users and businesses. Ideally, customers would choose to use the cloud or not by comparing the inherent technical and economic advantages of the cloud approach against its inherent disadvantages, rather than making the decision in order to stay on one side or the other of a legal distinction. To the extent that ECPA considerations dictate decisions to use the cloud or not, this makes computing less efficient and impedes progress toward better technology.

Mr. NADLER. I thank the gentleman.
I now recognize Mr. Salgado?

TESTIMONY OF RICHARD SALGADO, SENIOR COUNSEL, LAW ENFORCEMENT AND INFORMATION SECURITY, GOOGLE, INC.

Mr. SALGADO. Thank you, Chairman Nadler, Ranking Member Sensenbrenner, and Members of the Subcommittee. As Google's senior counsel for law enforcement and information security I oversee Google's response to government requests for user information under many authorities, including the Electronic Communications Privacy Act of 1986. I have also worked with ECPA extensively from a law enforcement perspective as a senior counsel in the criminal division in the Department of Justice.

ECPA was a forward-looking statute for 1986, and much of it remains relevant today. But over my many years of experience in implementing, in trying to interpret, and frankly often wrestling with the statute I have seen large gaps grow between the technological assumptions of that earlier era and the reality of how electronic communication works today.

As a result of those gaps, providers, users, law enforcement agents, investigators, and prosecutors, as well as judges often face complex and baffling rules that are difficult to explain and challenging to apply. Even more significant, however, in important respects ECPA now fails to provide the privacy protection that people reasonable expect, and that is why Google helped found and strongly supports the Digital Due Process coalition.

The coalition, which many of you may have heard of, is a broad coalition. It includes telecommunications companies like AT&T; we have Internet companies, many of whom are represented on the panel today; and other organizations, including Americans for Tax Reform and the ACLU, among many other members that I haven't mentioned.

The coalition has proposed a set of common sense principles for updating ECPA. The reforms seek to preserve the structure of the statute and certainly the tools needed by law enforcement to perform their important functions, but are intended to ensure that the protections afforded to data stored in the cloud are no less than those extended to data stored in the home or in the office.

Cloud computing is a new term, as has been noted, but most of us use cloud services every day even if the label isn't particularly familiar to us. When you use the Web to send an e-mail, to edit a document, or to manipulate a calendar, as Professor Felten has reflected to us, you are actually using cloud computing services.

The services now are very robust and very feature-rich. In fact, many companies are moving their entire I.T. infrastructure into the Internet-based cloud and getting the functionality through service providers. Shifting all of these computing tasks from our desktops to cloud providers offers tremendous social benefits, tremendous economic benefits, and security benefits.

Today's technology bears little resemblance to the mainframe computers of the 1980's. Back then remote computing and storage were rare luxuries for companies, usually used for bulk processing, like payroll services or data backup. ECPA has not kept pace with the rapid technological advances that we have enjoyed in the last few years, and as a result the problems are becoming obvious.

One example that has been alluded to already: Under ECPA the government must obtain a warrant to get the content of an e-mail

that is no older than 6 months, but for older messages the government can simply issue a subpoena, obviously without a judge's approval, to compel the production of the e-mail's content from a provider. Under the Department of Justice's interpretation of ECPA, which has been rejected by the 9th Circuit, opened e-mail, regardless of the age, can be obtained using that lower subpoena standard.

Distinguishing the privacy protections of e-mail based on age and by access of the user makes no sense today. In 1986 perhaps it did. Remote storage was so expensive that users rarely stored messages for very long; they either downloaded or deleted the messages soon after receiving them. Today people often keep messages and mail for indefinite periods of time, possibly forever.

With Gmail, which is Google's free mail service, Google offers enough free storage that space constraints are not a reason ever to delete an old mail. Many of our users have messages going back to when Gmail was launched over 6 years ago. Gmail accounts have essentially become the filing cabinets of today.

The example reveals how parts of ECPA need to be updated for the 21st century. The Digital Due Process proposal would go far toward achieving that goal. Advances in technology depend not just on smart engineers, but also on smart laws that will not stand in the way of continued innovation and adoption of technology.

I thank the Subcommittee for giving the attention to this issue and urge you to help bring ECPA into the Internet age. Thank you.

[The prepared statement of Mr. Salgado follows:]

PREPARED STATEMENT OF RICHARD SALGADO

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 "ECPA and the Cloud"
September 23, 2010

Google thanks Chairman Nadler, Ranking Member Sensenbrenner, and members of the Subcommittee for examining the need to modernize the Electronic Communications Privacy Act of 1986 (ECPA).

My name is Richard Salgado. As the 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, and have taught and lectured on these issues at Georgetown University Law Center, George Mason University Law School, and Stanford Law School.

It is vital for online providers and for Americans who use Internet communications services that Congress update ECPA to address the tremendous technological advances in communications and computing technology that the world has witnessed since 1986, when the statute was passed. This is why Google played a lead role in founding the Digital Due Process coalition (www.digitalducprocess.org), an ECPA reform advocacy coalition that includes other technology companies, public interest organizations, and academics. The coalition believes that our laws should protect individuals from unwarranted government intrusion in the online world no less than they do in the home, even 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 reflects the pre-Internet computing landscape of the 80s

ECPA was written 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, communication through the Internet was the province of academic researchers and government agencies. There was no generally available way to browse the World Wide Web. Commercial email had yet to be offered to the general public. Instant messaging wasn't widely used until the late 1990s. In 1986, 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 1986, we have experienced unprecedented advances in communications technology and

services, and a fundamental shift in how individuals communicate with each other. The web, search engines, video sharing sites, social networks 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 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 less that $100 (under $0.000094 per megabyte) and hold 300,000 photos. Complimenting the growth in storage capacity, data transfer rates are nearly one hundred and sixty times faster than in 1986 -- making it possible to share richer data, to collaborate among many users, 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.

The growth of the cloud

Cloud computing is a relatively new term for some, but the cloud is being used today by significant numbers of consumers, businesses, and the public sector. Companies like Google are now able to offer their users the ability to store, access, use and share their data from servers located in offsite data centers, rather than on the user's premises. Instead of loading various software packages onto their computers, users access applications and services over the Internet.

For example, Google's cloud applications, including Gmail, Google Docs, and Google Calendar, allow our users to store data or run programs on our geographically distributed, secure data centers. Businesses increasingly are choosing to use such data centers -- managed by Google and many other technology companies -- the same way they used to use their desktop computers or on-premise file servers. In the process they are saving money, becoming more efficient, and improving their security.

Leading analysts confirm an acceleration of adoption of cloud computing, with the scale of deployments growing. As Google just announced, over three million businesses now use our cloud service, Google Apps, and every day more than 3,000 businesses sign up. Other providers appearing before the Subcommittee today can tell similar stories about their growth and the benefits seen by their customers.

In the cloud, everyday processes and information that are typically run and stored on local computers -- email, documents, calendars -- can be accessed securely anytime, anywhere, and with any device through an Internet connection. 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 also enables services like online video, shared document collaboration among people across the country or around the world, and many other services. As a customer's needs grow, the cloud services she uses can expand as needed without the customer having to go through a slow procurement process.

The "virtual" services offered in the cloud have created enormous and tangible value in the economy, spawning new businesses and a spurring innovation and further growth of the 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 need for an ECPA update

Millions of Americans already use the cloud every day -- to send messages, to collaborate with co-workers, to store important records and documents. More and more computing functions and communications will move to the cloud as its benefits are more 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 pre-Internet 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.

ECPA worked well for many years, and much of it remains vibrant and relevant. In significant places, however, a large gap has grown between the technological assumptions made in ECPA and the reality of how the Internet works today, leaving us in some circumstances with complex and baffling rules that are both difficult to explain to users and difficult to apply.

The current complexity can be demonstrated by the requirements to compel production of communications content such as email. 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 is 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 inconsistent, confusing and uncertain standards raised by examples like this one reveal how ECPA fails to preserve the reasonable privacy expectations of Americans today. Moreover, providers, judges and law enforcement alike have difficulty understanding and applying the law to today's technology and business practices. By creating inconsistent privacy protection for users of cloud services and inefficient, confusing compliance hurdles for cloud providers, ECPA has perversely created an artificial and unnecessary disincentive to move to a more efficient, more

productive business model. ECPA must be updated to help encourage the continued growth of the cloud.

A roadmap for reform: Digital Due Process

The Digital Due Process coalition has put forward principles that are designed to help ensure that content stored in the cloud receives no less due process protection as data held on computers at home or in the office, to simplify and 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, or "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 along these lines 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, kept secure, and offered 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 in the form of 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. Earlier this year, 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/transparencyreport). This week we updated the tool to reflect more recent data. This tool has served to raise attention to the issue of what rights users have when it comes to their data. We believe that the U.S. should lead 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 continued innovation and adoption of the technology. We look forward to working with this Subcommittee and with Congress as a whole to strengthen the legal protections for individuals and businesses that rely on our services so that technology innovation can continue to lead our economic recovery, while ensuring that law enforcement continues to have the legal tools needed to satisfy it's important responsibilities.

Thank you.

Mr. NADLER. I thank the gentleman.
I now recognize Mr. Hintze?

TESTIMONY OF MIKE HINTZE, ASSOCIATE GENERAL COUNSEL, MICROSOFT CORPORATION

Mr. HINTZE. Chairman Nadler, Congressman Franks, Chairman Conyers, honorable Members of the Committee, thank you for the opportunity to discuss Microsoft's perspectives on ECPA reform. We appreciate the attention with which this Subcommittee has approached the issue and we are committed to working with you, law enforcement agencies, and other stakeholders to ensure that we responsibly update ECPA for the era of cloud computing.

ECPA was enacted into law in 1986 to address the issues being raised by new digital technologies. What are the appropriate standards under which law enforcement can compel service providers to disclose customer content and account information? ECPA addressed this issue by striking a balance between the legitimate needs of law enforcement and the public's reasonable expectations of privacy.

Technology has changed dramatically since 1986. Today we are in a new era of computing, one in which users are empowered to store unprecedented amounts of digital information online.

This cloud computing revolution creates numerous benefits. It makes businesses more efficient and competitive by enabling companies of all sizes to access cutting-edge computing resources. It facilitates collaboration through anytime, anywhere access. And it provides new opportunities for innovation and job creation.

Microsoft has participated actively in this transformation. We come to the issue of ECPA reform as a provider of desktop and server software that has moved into hosting online cloud-based services.

Our history gives us a clear perspective on how ECPA has failed to keep pace with the technological time. Take the example of e-mail. As we have heard, ECPA extends greater privacy protections to e-mail stored less than 180 days than e-mail stored for more than 180 days.

For many years this distinction made sense. Even 10 years after the enactment of ECPA Microsoft was offering the first version of Microsoft Exchange, software in which a user typically would download e-mail to a local machine for it to be read and stored, after which it would no longer reside on the server. Because the e-mail typically was downloaded to a local drive it was reasonable to conclude that e-mail left with a service provider for more than 180 days was abandoned with little expectation of privacy.

But shortly thereafter, in 1997, we acquired Hotmail, a Web-based e-mail service that enabled e-mails to be stored online or in the cloud for longer periods of time. This ability to retain e-mails online even after they were read began to call into question the justification for the 180-day distinction. Even then, however, the amount of storage available online was quite limited.

But since 1997 the amount of online storage available to consumers has progressively increased to the point where it has become essentially unlimited. Today users regularly store e-mails and attachments, including photos, documents, and other data, online for years, and these users reasonably expect that this data will be just as private on day 181 as it was on day 179.

These concerns are not limited to individual consumers. Enterprises of all sizes are increasingly using products like Microsoft Business Productivity Online Suite to store their e-mail and confidential business documents in the cloud, but we regularly hear from enterprises considering the move to the cloud that doing so could negatively impact their privacy protection.

In short, the balance Congress struck in 1986 has fallen out of alignment, putting more and more user data within the reach of law enforcement tools that require lower burdens of proof. This trend has serious potential consequences.

Users will be deterred from adopting cloud services if they do not trust their data and will be kept private and secure in the cloud. In addition, cloud service providers will hesitate to invest in new innovation if there are not clear rules that make sense in the context of this evolving technology.

To restore the balance the Congress struck in 1986 Congress should revisit ECPA and ensure that users do not suffer a decrease in their privacy protections when they move their data to the cloud. We believe that the principles advanced by the Digital Due Process coalition will enable citizens to trust their data will be subject to reasonable privacy protections while at the same time preserving the ability of law enforcement to collect the information necessary to protect the public. The principles will also provide greater clarity for all stakeholders, and we see them as a good starting point for the discussion.

As Congress takes up the important issue of ECPA reform we believe it should also look at privacy and security issues related to cloud computing in the broader policy context. Users of cloud computing services must have confidence that their data will be kept secure and private not just vis-a-vis the government but also with respect to service providers and other third parties. The importance of protecting privacy and security also extends beyond the United States and can be impacted by the laws of other governments.

To address these concerns Microsoft has proposed that Congress consider comprehensive legislation that advances privacy and security in the context of cloud computing, and in turn helps to promote confidence in the cloud.

Thank you for the opportunity to testify today. Microsoft appreciates the Subcommittee's leadership, and we look forward to working with you on these important issues.

[The prepared statement of Mr. Hintze follows:]

PREPARED STATEMENT OF MICHAEL HINTZE

STATEMENT OF MICHAEL HINTZE
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

"REALIZING THE BENEFITS OF CLOUD COMPUTING:
MICROSOFT'S PERSPECTIVE ON ECPA REFORM"

SEPTEMBER 23, 2010

Chairman Nadler, Ranking Member Sensenbrenner, and honorable Members of the Committee, thank you for the opportunity to discuss Microsoft's perspectives on reform of the Electronic Communications Privacy Act of 1986 (ECPA). We appreciate the attention and seriousness of purpose with which this Subcommittee has approached the issue of ECPA reform, and we are committed to working with you, law enforcement agencies, privacy advocates, and other stakeholders to ensure that we responsibly update ECPA for the era of cloud computing.

ECPA was enacted into law in 1986 to strike a balance with respect to an issue that new digital technologies were increasingly bringing to the fore: under what circumstances is it appropriate for law enforcement to compel telecommunications and Internet service providers to disclose customer content and account information. ECPA addressed this issue by striking a balance between the legitimate needs of law enforcement and the public's reasonable expectations of privacy.

It is an understatement to say that technology has changed since 1986. We at Microsoft have witnessed first-hand the successive revolutions in computing technologies that have transformed our economy and generated whole new forms of social interaction. Indeed, in many ways Microsoft's own history reflects this transformation: we come to the issue of ECPA reform as a provider of desktop software that has since moved into providing software for servers and networks and, from there, into hosting online "cloud-based" services.

The industry-wide move to cloud computing has enabled businesses and individuals to store online orders of magnitude more data than was the case when ECPA was first passed in 1986, including some of the most confidential and sensitive business and personal information. The law, however, has failed to keep up with changes in technology. As a result, when applied to today's online services, ECPA is complex and often unclear. More importantly, when law enforcement officials seek data or files stored in the cloud, such as Web-based e-mail

applications or online word processing services, the privacy standard that is applied is often lower than the standard that applies when law enforcement officials seek the same data stored on an individual's hard drive in his or her home or office.

The failure of ECPA to keep pace with the technological times – and the ensuing uncertainty of privacy protection in the cloud computing environment – has serious potential consequences. Users will be deterred from adopting cloud services if they do not trust that their data will be kept private and secure in the cloud. In addition, those considering whether to move a service to the cloud may hesitate to invest in innovation if the rules of the road are not clear in the context of the evolving technology. In all, the full benefits of cloud computing will not be realized without a legal structure that is up-to-date and that protects users' reasonable expectations of privacy.

To restore the balance that it struck in 1986, we urge Congress to revisit ECPA and ensure that users do not suffer a decrease in their privacy protections when they move their data to the cloud. We believe that the principles advanced by the Digital Due Process ("DDP") Coalition will enable citizens to trust that their data will be subject to reasonable privacy protections – as is already true for data stored on their home computers – while at the same time preserving the ability of law enforcement to collect the information necessary to protect the public. The DDP Coalition principles are also aimed at providing greater clarity for all stakeholders.

In recommending these changes, Microsoft also recognizes the legitimate needs of government investigators in obtaining access to data that may be stored 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. Our Digital Crimes Unit 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 is threatened even without being compelled to do so. The DDP Coalition's proposal would in no way threaten this cooperation.

Finally, as Congress takes up the important issue of ECPA reform, we believe it also should look at privacy and security issues related to cloud computing in a broader policy context. Potential users of cloud computing services are concerned not only about the privacy and security of their data vis-à-vis the government, but also in relation to their service providers and other third parties. Further, the importance of protecting privacy and security extends beyond the United States and can be impacted the laws of foreign governments. To address these concerns, we urge Congress to consider comprehensive legislation to address a range of privacy and security issues relating to cloud computing.

I. The Benefits of Cloud Computing and the Challenge of Privacy in the Cloud

We have entered a new era in computing, one in which software running on users' own PCs and local networks increasingly is complemented by applications and services accessed over the Internet from remote data centers. The technologies which have enabled this new era of computing – commonly referred to as "cloud computing" technologies – are empowering users to store unprecedented amounts of digital information online.[1] The benefits for users of these new computing technologies include:

- ***Greater efficiencies for organizations to customize and rapidly scale their IT systems for their particular needs.*** With cloud computing, users pay only for the

[1] *See* "Building Confidence in the Cloud: The Need for Prompt Industry and Government Action for Cloud Computing," Speech of Brad Smith, General Counsel, Microsoft Corporation, at the Brookings Institution Policy Forum (Jan. 20, 2010), *available at*: http://www.microsoft.com/presspass/presskits/cloudpolicy/docs/speech0120.doc

services they need, and they can add or reduce computing capacity nearly instantaneously. This is a tremendous advantage for those enterprises, like retailers or tax advisors, that have particularly high demand for IT services during certain times of the year.

- ***Expanded access to computational capabilities previously available only to the very largest companies.*** Because cloud services are accessed remotely, customers get the benefit of the cutting-edge computing resources of their cloud provider – without needing to upgrade their own hardware.

- ***Better collaboration through "anytime, anywhere" access to IT for users located around the world.*** Because cloud applications and data are stored offsite, cloud customers can access their data from any location that has an Internet connection.

- ***New opportunities for innovation as developers move to this new computing paradigm.*** By improving access to computing resources and reducing cost, cloud technologies lower barriers to entry and help developers create new applications and help entrepreneurs start small businesses.

Today, Microsoft cloud technology is helping doctors and patients manage chronic health conditions to improve care and reduce costs; helping NASA engage the public in piecing together images of the surface of Mars; and helping businesses of all sizes better connect with and serve their customers.

Ultimately, these technological developments have involved the shifting of more and more customer data into the online environment, with much of the data being highly sensitive and confidential information. This unprecedented migration of information is valuable for customers because it allows them to increase efficiency and reduce costs, but it also raises an important question: will moving data from my premises to a third party mean that it is no longer as private or secure? This straightforward concern is widely-shared among the public. For example, in a poll commissioned earlier this year by Microsoft, 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.[2]

To allay users' reasonable concerns, we need clear and up-to-date privacy legislation, which will ensure that when a user decides to save a document in the cloud instead of, or in addition to, on his or her local PC, the user will not suffer any decrease in his or her privacy protections.[3]

II. The Need for ECPA Reform

This is not the first time that we have been faced with a public policy issue relating to the protection of privacy in online digital technologies. In 1986, Congress enacted ECPA as a response to new technologies that threatened to upset the balance between the fundamental privacy rights of citizens and the legitimate needs of law enforcement to access information to protect the public. Congress also was motivated by a widely-shared sense of uncertainty as to whether our traditional source of privacy rights, the Fourth Amendment, applies to digital data that is stored online. This constitutional ambiguity extends to the present day: earlier this year, for example, in *City of Ontario v. Quon*,[4] the Supreme Court declined to address whether the Fourth Amendment applies to text messages stored online, noting that courts should exercise caution when considering the constitutional implications of emerging technologies.

At its inception, ECPA was intended to create a balance between the rights of individuals and the legitimate needs of law enforcement with respect to data shared or stored in various types

---

[2] Microsoft Corporation, Cloud Computing Flash Poll – Fact Sheet, *available at*: http://www.microsoft.com/presspass/presskits/cloudpolicy/docs/PollFS.doc

[3] *See* "Building Confidence in the Cloud: A Proposal for Industry and Government Action to Advance Cloud Computing," Microsoft Corporation (Jan. 2010), *available at* http://www.microsoft.com/presspass/presskits/cloudpolicy/docs/CAAProposal.doc

[4] No. 08–1332 (U.S. S.Ct. June 17, 2010)

of electronic and telecommunications services.[5] To achieve this balance, ECPA establishes rules that law enforcement must follow before they can access data stored by service providers. Depending on the type of customer information involved and the type of service being provided, the authorization law enforcement must obtain in order to require disclosure by a third party will range from a simple subpoena to a search warrant based on 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. Today, the basic technological assumptions upon which the Act was based and the nature of protection given to user data stored in the cloud have not kept pace with the unprecedented digitization and storage of online data that cloud computing has enabled. As a result, more and more sensitive personal information has fallen within the reach of law enforcement tools that require a lower standard of proof.

Microsoft comes to this issue as a provider of desktop and server software that has in recent years also moved into the provision of online services to users and organizations. As such, our history gives us a clear perspective on how technological change has impacted the application and effect of ECPA.

Take the example of email. ECPA extends greater privacy protections to email messages stored for less than 180 days than emails stored for more than 180 days.[6] This distinction might

---

[5] Congress's effort to balance these competing interests is reflected in the legislative history of ECPA. *See* H. Rep. No. 99-647, at 19 (1986) (discussing goal of preserving "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement."); S. Rep. No. 99-541, at 5 (expressing the concern that ambiguity over privacy protections online might "unnecessarily discourage potential customers from using innovative communications systems").

[6] Under 18 U.S.C. § 2703(a), a governmental entity may generally require the disclosure of emails in "electronic storage" for 180 days or less only pursuant to a warrant issued on probable cause. In contrast, under 18 U.S.C. § 2703(a) and (b), the government may require the disclosure of the contents of emails that have been in "electronic (continued…)

have made sense in the late 80s and early 90s, when there were few options for users to store their messages online for more than 30 days, but it no longer makes any sense. A decade after the enactment of ECPA, in 1996, Microsoft was offering the first version of Microsoft Exchange – server and desktop software in which a user typically would download email to a local machine for it to be read and stored, after which it would no longer reside on the server. Because email typically was downloaded to a local drive to be read and stored, it was reasonable to conclude that email left with a service provider for more than 180 days was abandoned with little expectation of privacy.

Shortly thereafter, in 1997, we acquired Hotmail, a web-based email service that enabled electronic communications to be stored online, in the "cloud," for longer periods of time. This ability to retain mail online even after it is read by the intended recipient began to call into question the continuing justification of the 180-day distinction. Even then, however, the amount of online storage was quite limited. But since 1997, the amount of online storage available to consumers has progressively increased, to the point where it has become essentially unlimited, with users storing gigabytes and gigabytes of their data online. Today, users regularly store email messages and attachments, including valuable pictures, documents, and data, online for years. And users reasonably expect that this data will be just as private on day 181 as on day 179.

As these and other new technologies have evolved and been embraced by users over the past decade, user expectations of privacy have also evolved alongside them. Put simply, users consider these technologies indispensable and thus are putting more and more data online –

---

storage" for more than 180 days through a menu of options, including a warrant, a subpoena, or a special court order that involves a lower burden of proof than probable cause.

including highly confidential and sensitive information – and are seamlessly moving such data between local and cloud storage. In doing so, these users have no reason to believe – nor should they – that their data is worthy of any less protection in the cloud than when it is stored locally. Many users do not even contemplate a distinction, and, absent adequate privacy protections in the cloud, those that do may be reluctant to embrace cloud services.

For example, technologies such as Microsoft's HealthVault offer individuals and health care providers the ability to store patient records and other health-related information in the cloud. As users begin storing online their medical information, among the most sensitive and private information a person possesses, the concern that a lower standard of privacy applies for data in the cloud could very well become a significant barrier to adoption.

Similarly, Microsoft's Business Productivity Online Suite (BPOS) offering includes hosted email and online document storage for enterprise customers. These businesses routinely deal with highly confidential information including trade secrets, business plans, customer lists, and privileged documents. Enterprise users tell us that they are very concerned about the privacy implications for moving such sensitive data from local storage to remote storage. A significant part of that concern relates to the circumstances under which the government can compel disclosure of their data from third-party providers.

Another example that demonstrates how technology changes can alter people's reasonable expectation of privacy is the addition of online features to traditional desktop software. For instance, features of Microsoft Office 2010 allow users to easily choose between saving a document locally or in the cloud. The seamlessness of this feature makes the distinction between local and online storage less and less salient for users. Increasingly users expect to be able to simply access their documents when they need to – at any time and on any device. We believe it would accordingly come as a surprise to these users that the level of privacy afforded

to their documents differs depending on where the documents happen to be stored. Put differently, their reasonable expectation of privacy no longer hinges on these distinctions – nor should it.

Under ECPA, there is also ambiguity as to when law enforcement can access a user's location information. Microsoft offers Window Phone operating system software for mobile phones and other software that include a function for determining the device's physical location. The ambiguity about the privacy protections afforded location data under ECPA is a source of concern for users, who reasonably see their physical location as a private – and often highly sensitive – piece of information.[7]

In all, the quantity and variety of data stored online is orders of magnitude greater than was envisioned when ECPA was passed in 1986, and this includes some of the most confidential and sensitive business and personal information. There also is an enormous variety of online services and cloud computing offerings – provided by Microsoft and a large number of other companies – that could not have been imagined in 1986. The mismatch between these new computing technologies and ECPA's outmoded distinctions is a source of reasonable concern for all stakeholders with an interest in online privacy, and it is the principal force driving the need for reform.

To restore the balance struck in 1986, we urge Congress to revisit ECPA in light of these technological advancements. We support responsible reforms that will ensure that users do not

---

[7] The status of location data collected through GPS devices also is uncertain under the Fourth Amendment. While some courts have suggested that there is no Fourth Amendment protection against the government using a GPS monitoring device to track an individual's movements, *see United States v. Pineda-Moreno*, 591 F.3d 1212 (9th Cir. 2010), other courts have held that the Fourth Amendment protects against government monitoring for long periods of time on a 24-hour basis using a GPS device that has been attached to their vehicle. *See United States v. Maynard*, No. 08-3030 (D.C. Cir. Aug. 6, 2010).

suffer a decrease in their privacy protections when they move data from their desktop PCs to the cloud. We believe that the principles advanced by the Digital Due Process ("DDP") Coalition[8] will enable citizens to trust that their data will be subject to reasonable privacy protections – akin to the protections they would receive for data on their home computers – while at the same time preserving the ability of law enforcement to collect the information necessary to protect the public. We believe the DDP Coalition principles also will provide greater clarity for all stakeholders. To be clear, while we support the DDP Coalition principles and believe they can accomplish this goal, we view them as a beginning, not the end, of the discussion.

In advocating for these reforms, we are not seeking special privacy protections for the cloud. Nor are we seeking to interfere in any way with the legitimate needs of law enforcement investigators to obtain the data necessary for their investigations. Indeed, we see and understand how important electronic information is for law enforcement, and we are committed to continuing to work closely and cooperatively with federal, state and local law enforcement agencies. Rather, our guiding principle is that policy decisions should be made by Congress, not by unpredictable changes in technology. Responsible reform of ECPA will restore the important balance that Congress struck in 1986 and, in doing so, will give consumers and enterprises the confidence they need to realize the benefits of this exciting new generation of computing technologies.

III. A Comprehensive Approach to Privacy and Security in the Cloud

While reconciling the competing interests of the individual and the state through a reformed ECPA is a worthy and crucial objective, it is equally important to situate ECPA reform in a larger policy context. After all, users also have reasonable expectations that their cloud

---

[8] See Digital Due Process Coalition, Statement of Principles, *available at*: http://digitalducprocess.org.

service provider will keep their data private and secure with respect to entities other than the U.S. government, such as private third parties and foreign governments. To address users' reasonable expectations of privacy and security across the range of these entities, we need a holistic legislative approach. That is why Microsoft supports the enactment of comprehensive legislation that would:

1. ***Improve Privacy and Security by Guaranteeing Transparency***. It should not be enough for service providers simply to claim that their services are private and secure. Customers should be provided with information about why this is the case. To improve transparency, legislation should require that cloud service providers maintain a comprehensive written information security program with safeguards appropriate to the use of their services, provide a summary of that program to potential customers, and disclose their privacy practices to any customer from whom covered personal information is collected.

2. ***Ensure Rigor in Federal Procurement.*** Federal agencies should make their decisions regarding procurement services on the basis of accurate information about cloud service providers' security and privacy practices. To accomplish this goal, Congress should require federal agencies to evaluate and select providers based in part on an assessment of their information security programs.

3. ***Thwart Computer Criminals Who Would Target Cloud Infrastructure.*** Although the cloud is being built with powerful and unprecedented security safeguards, the aggregation of data in cloud data centers presents new and rich targets for hackers and thieves. To combat such criminals, legislation is needed that would enhance criminal enforcement of computer crimes targeting cloud computing data centers and allow cloud service providers to bring suit against violators directly to augment deterrence of such crimes.

4. ***Encourage International Cooperation***. In recent years there has emerged a global thicket of competing and sometimes conflicting laws affecting cloud computing. These laws can place cloud service providers in a Catch-22, where the decision to comply with the lawful demand for data in one jurisdiction can risk violating the data privacy laws of another jurisdiction. Comprehensive cloud privacy and security legislation should encourage the federal government to engage in international efforts to promote consistency in national laws governing privacy, security and government access to cloud data.

At Microsoft, we believe that these issues are interrelated and thus are best addressed in concert. By enacting such legislation, Congress can create a comprehensive regulatory framework which will facilitate the adoption of cloud technologies and spur innovation and economic growth.

IV. Conclusion

Microsoft believes firmly that computing technologies work best when they give users control over their information. It should be up to users to determine what kind of documents to create, where to store them, and with whom to share them. We believe that this is one important reason why the PC revolution unfolded as it did. Consumers felt secure in the knowledge that they could move their most important documents from their desk drawer to their desktop PC and not lose any control over them.

As we experience another transformation in technology – the move from the desktop PCs and on-premises servers to the cloud – we need to ensure that the laws that govern the protection and access to information used by this technology continue to strike an appropriate balance. That is why we support the responsible reform of ECPA to ensure that users have the same privacy rights for their data in the cloud as they do for their on-premises data. Such reform would restore the careful balance that Congress first struck in 1986 when it enacted ECPA.

We also believe it is important to situate ECPA reform in a larger policy context that lays the foundation for users to embrace cloud computing in much the same fashion as they adopted the PC.

Thank you for the opportunity to testify today. Microsoft appreciates this Subcommittee's leadership, and we look forward to working with you on these important issues.

Mr. NADLER. I thank the gentleman.
Mr. Schellhase is now recognized.

TESTIMONY OF DAVID SCHELLHASE, EXECUTIVE VICE PRESIDENT AND GENERAL COUNSEL, SALESFORCE.COM

Mr. SCHELLHASE. Chairman Nadler, Chairman Conyers, Congressman Franks—oh yes, I am sorry—thank you for holding this hearing and inviting me to share my views with you.

Cloud computing is emerging as a powerful engine for economic growth and jobs and it is important that we create a policy framework that supports it. Salesforce.com, my employer, is a leading enterprise cloud computing company that provides Internet-based business applications primarily for helping to automate sales and customer support functions to organizations of all sizes around the world.

Instead of building and maintaining costly I.T. infrastructure our customers simply log onto our Web site and access our cloud services using a unique username and password. Over 82,000 organizations globally, including numerous U.S. Federal Government agencies and businesses in highly regulated industries, trust Salesforce.com to store and process their data.

In my remarks today I will make reference to the enterprise cloud computing model. In doing so I will emphasize two points: First, U.S. public policy should support cloud computing because it is a powerful driver of economic growth and job creation. Second, in order to build confidence in cloud computing the rules for government access to data held in the cloud should be the same as for data held on premise.

Every major analyst firm believes that cloud computing will see explosive growth. Gartner Group estimates that the worldwide market for cloud services will be worth $148 billion by 2014, and a recent Goldman Sachs report called the shift toward cloud computing "unstoppable."

Just as the electric power grid paved the way for the rise of the modern business economy, cloud computing is paving the way for the 21st century digital economy. By unleashing innovation and productivity cloud computing will create jobs not only in the technology industry but also create jobs in sectors as diverse as manufacturing, health care, and government. Cloud computing has already spawned scores of new companies, and as the market for cloud computing accelerates Congress should adopt policies that support the cloud computing model or, at a minimum, that do not discriminate against it.

Government has a very legitimate—has very legitimate reasons to access privately-held data for such purposes as fighting crime and preventing terrorist attacks. In order to generate public confidence in the way that the government obtains this access, however, it is essential that the guidelines for them be applied in a predictable way that is appropriately transparent.

At Salesforce.com we create trust in our cloud computing applications by maintaining robust security practices based on international standards, hosting a public Web site that shows the performance and trust of our system on a daily basis, and contractually agreeing to keep our customers' data confidential with exceptions for due process of law. For many customers these actions are all the evidence they need to determine that they can trust the privacy and security of our data—of our cloud services.

For others, however, especially those outside the United States, these actions are not enough. These customers want something more. They want assurances that the U.S. government will not access their data without appropriate due process.

At Salesforce.com we face this issue on a regular basis, principally from customers who believe that the current regulatory framework permits the U.S. government overly broad access to data stored in the cloud. We need to have clear laws that prove that this belief is unfounded.

As a company, Salesforce.com cannot make representations to its customers that government will not gain access to data. What we can do is point to the legal process that the government must undertake to access data held in the cloud. This is where reform of the Electronic Communications Privacy Act is so crucial.

Because ECPA codifies guidelines for U.S. government access to data it sends a clear signal to other countries about the confidentiality of data held in the cloud. As a result, it is important that Congress update ECPA to clarify that data stored and processed in the cloud on behalf of a customer has the same protections and standards for law enforcement access as data stored locally by that customer.

As Congress contemplates ECPA reform it should embrace the concept of technology neutrality. In practice, technology neutrality that a particular kind of information will receive the same level of protection regardless of the technology platform or business model used to create, communicate, or store it. We are not asking for special treatment for data in the cloud, but rather for equal treatment.

In order to assure technology neutrality in private communications, documents and other private user content stored in or transmitted through the cloud should be subject to the same warrant standard that the Constitution and the Wiretap Act have traditionally provided for privacy of our phone calls or the physical files we store in our homes. In practice, this recommendation would mean that the government must 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.

By making sure that ECPA is technology neutral Congress can send a clear signal to individuals, companies, and governments around the world that they can safely use cloud computing platforms. We believe that doing so will unleash a wave of innovation and productivity that will drive economic growth and create jobs for years to come.

Thank you.

[The prepared statement of Mr. Schellhase follows:]

PREPARED STATEMENT OF DAVID SCHELLHASE

ECPA Reform and the Revolution in Cloud Computing

Testimony of David Schellhase

Executive Vice President and General Counsel

Salesforce.com

Before

The U.S. House of Representatives

Committee on the Judiciary

Subcommittee on the Constitution, Civil Rights, and Civil Liberties

September 23, 2010

Chairman Nadler, Ranking Member Sensenbrenner and Members of the Committee, thank you for holding this hearing on cloud computing and for inviting me to share my views with you. Cloud computing technology is emerging as an engine for economic growth and jobs, and it is important that we create a policy framework that supports it. As the Executive Vice President and General Counsel at Salesforce.com, I am deeply involved in policy discussions about cloud computing, and I applaud the efforts of this Committee to address this issue.

About Salesforce.com

Salesforce.com is a leading enterprise cloud computing company that provides Internet-based solutions to organizations of all sizes in all industries globally. Our main service offerings are applications that allow organizations to input, store, process, and access data to manage their sales and customer services. In addition, we provide an enterprise collaboration tool called Chatter [1]and a development platform called Force.com.[2]

Salesforce.com delivers its services over the Internet through commercially available Web connections and browser software. Before cloud computing, the customers we service today would typically purchase software and hardware from different vendors and

[1] Salesforce.com Chatter enables real-time enterprise collaboration. As both a collaboration application and a platform for building collaborative cloud computing applications, Chatter allows users to connect and share information securely – all in real time.
[2] Force.com is the leading cloud platform for business applications. It gives developers a platform to create rich, collaborative custom cloud applications fast – without buying hardware or installing software.

integrate this technology in their own data centers. Today, instead of building and maintaining costly IT infrastructure, our customers simply log on to the Salesforce.com Website and access their cloud services using a unique username and password. Over 82,000 organizations globally, including governments and businesses in highly regulated industries like financial services, healthcare, insurance and communications trust Salesforce.com with their data. We also have several U.S. federal government customers, including the Department of Justice, the Department of Health and Human Services, the Securities Exchange Commission, and the Department of State.

In my remarks today, I will make reference to the Salesforce.com enterprise cloud computing model, not the consumer cloud computing model that companies like Amazon and eBay have made popular. In doing so, I will emphasize two points:

1. **US public policy should support cloud computing because it is a powerful driver of economic growth and jobs.**
2. **In order to build public confidence in cloud computing, the rules for government access to data held in the cloud should be the same as for data held on-premise.**

Cloud Computing is a Driver of Economic Growth

Cloud computing has already been embraced by consumers and successfully implemented by organizations of all sizes around the world. Every major analyst firm

believes that cloud computing will expand its share of the overall IT market. According to Gartner, the worldwide market for cloud services will be worth $148.8 billion by 2014.[3] According to Saugatuck Technology, an average of 45 percent of all new business and IT spending will go to cloud services within the next five years. [4] According to a recent Goldman Sachs report[5] the shift toward cloud computing is "unstoppable" and has likely been accelerated by the macroeconomic downturn that has forced businesses to look for lower-cost solutions.

A good way to explain why enterprise cloud computing is gaining popularity is to compare it to a high-rise office building that houses many different businesses under one roof. Just as a high-rise allows tenants to lease secure, individual offices in the same building while sharing core services such as plumbing and electricity, multi-tenant enterprise cloud computing allows organizations to use individualized software applications while sharing core computing services such as database and security. For the tenants, it's cheaper, more efficient, and easier to scale up than are the alternatives. By eliminating the need for costly and wastefully duplicative infrastructure, multi-tenant cloud computing frees users to focus on their core business, not their IT.

In a multi-tenant cloud, data and applications are separated logically within the hardware and software, so different users can view only the information and cloud services that

---

[3] Gartner, Inc., Forecast: Public Cloud Services, Worldwide and Regions, Industry Sectors, 2009-2014, June 2, 2010
[4] Saugatuck Technology, Ageing IT Infrastructure: A Boon for Cloud Adoption?, March 12, 2010.
[5] Goldman Sachs SaaS Survey, February 2010.

pertain to them. In this respect, multi-tenant cloud computing is like online banking – it allows large numbers of individuals to use their accounts at the same time while keeping their information private through the logical (not physical) separation of data.

In order to appreciate the power of multi-tenant cloud computing, it is useful to contrast it to traditional, single-tenant computing applications. Multi-tenant applications can satisfy the needs of numerous organizations with the hardware resources and staff needed to manage one large computing stack. By contrast, single-tenant applications require a dedicated set of resources for each organization. It is largely for this reason that the Application Service Provider (ASP) single-tenant computing model of the late 1990s failed. In the ASP model, the setup, maintenance and upgrades of computer applications were outsourced to a third-party service provider, just like they are with cloud computing. The difference was that the ASP had to maintain a separate infrastructure stack for each customer. As more and more customers were added, the sheer scale, cost and complexity of maintaining the aggregate computing infrastructure became unsustainable.

With multi-tenant cloud computing, the software applications are provided as a service to multiple customers on a single, large infrastructure stack. The configurations of each user are stored as metadata that describes the base functionality of their application and corresponds to their data and customizations. This metadata is then interpreted by the platform's runtime engine. In a robust multi-tenant, metadata cloud architecture there is a clear separation of the compiled runtime engine (kernel) and the application data. As a

result, the kernel can be upgraded without disrupting customer's applications or data, thus allowing for continuous improvements in performance.

With its multi-tenant architecture, Salesforce.com is able to run approximately 230,000 applications for its more than 82,000 customers on just a few thousand servers. No other computing model delivers that kind of efficiency. A single-tenant computing model (sometimes referred to as a "private cloud") would require a minimum of 2 servers per application (one database server and one application server), plus additional servers for redundancy and disaster recovery. Consequently, a single-tenant computing model could require several hundred thousand servers to manage the computing needs of the customer base that Salesforce.com manages with just a few thousand servers.

Nicholas Carr, former executive editor of the *Harvard Business Review* and one of the most influential thinkers in the IT industry, has written a best-selling book validating the concept of multi-tenant cloud computing. Carr believes that ''utility-supplied'' computing will have economic and social impacts as profound as the ones that took place a hundred years ago, when companies ''stopped generating their own power with steam engines and dynamos and plugged into the newly built electric grid.''[6] Just as the electric grid made it possible to deliver electrical services to large numbers of users remotely, cloud computing makes it possible to deliver computing services to large numbers of users remotely. Moreover, just as electric utilities led to a surge of new businesses and jobs, so will cloud computing. Thus, the jobs that cloud computing generates are measured not only by the jobs created in the cloud computing industry itself, but also by

[6] Nicholas Carr, The Big Switch: Rewiring the World, from Edison to Google, New York: Norton, 2008.

the additional jobs that cloud computing customers can generate by being freed of the burden of maintaining a costly internal IT infrastructure.

Multi-tenant enterprise cloud computing is cost-effective, fast, easy-to-use, flexible and available anywhere. It is also a powerful driver of innovation. This combination of benefits allows organizations that use cloud computing to dramatically boost their performance.

Cost-Effective

Because enterprise cloud computing customers do not have to invest in costly IT infrastructure, they enjoy significant upfront savings. And because they pay on a per subscriber basis that includes system upgrades, costs are more predictable.

Fast

Because customers do not have to spend time procuring, installing or maintaining servers and networking equipment, cloud applications can be implemented quickly (from a few days to a few months) and deployed simultaneously to thousands of users in different locations.

Easy to Use

Because Salesforce.com has modeled its service after consumer Web applications like Amazon and Google, interfaces are intuitive and easy to use, leading to high user adoption and customer satisfaction.

Flexible

Because enterprise cloud computing is built on Internet scale platforms, it provides flexibility that traditional computing cannot. For example, it took only three weeks for the 2008 Presidential Transition Team to launch its Change.gov application on the Salesforce.com platform, and during the week that the application was live, it registered 40 million hits and handled 145 hits per second at its peak.

Available Anytime, Anywhere

Because enterprise cloud applications are accessed over the Internet and housed in large data centers that run 24 hours a day, users can securely access real-time data anytime and from anywhere with an Internet browser.

Continuous innovation

Because Salesforce.com implements all upgrades on its platform automatically, our customers benefit from new features immediately and do not have to worry about legacy software. Because Salesforce.com lets developers build, host and support their applications on our platform, they can bring innovative ideas to life quickly and share them widely.

Together, these benefits constitute a powerful engine for economic growth. Cloud computing has already spawned scores of new companies and the jobs that go with them.

IDC estimates that there are more than 1,000 worldwide software-as-a-service providers alone. In the coming decade, thanks to the proliferation of cloud services, low-cost bandwidth, and inexpensive access devices like smart-phones, the market for cloud computing will accelerate. In order to maximize the benefits to the American economy, Congress should adopt policies that support the cloud computing model, or at a minimum, do not discriminate against it.

The Rules for Government Access to Data in the Cloud should be the same as for Data On-premise.

Government has legitimate reasons to access privately-held data. It needs to access data in order to fight crime and prevent terrorist attacks. The legitimacy of these activities is widely accepted. In order to generate public confidence in the way that government manages these operations, it is essential that the guidelines for them be applied in a predictable way that is appropriately transparent.

At Salesforce.com, we endeavor to promote trust in our enterprise cloud computing solution in several ways:

- We maintain robust security practices based on international standards like ISO 27001.[7]
- We publicly post our privacy policies.
- We host a public website, https://trust.salesforce.com, which shows the performance of our system on a daily basis.
- We list customer success stories from around the world.
- We track and share information about customer satisfaction.
- We contractually agree to keep our customers' data confidential with exceptions for due process of law.

For many potential customers, these actions are all the evidence they need to determine that they can trust the privacy and security of our cloud services. For others, however, especially those outside the United States, these actions are not enough. These customers want something more -- they want assurances that the U.S. government will not access their data without deliberate due process. As the demand for cloud computing services has grown, so have these concerns about undue government access. At Salesforce.com, we face this issue on a regular basis, principally from customers who have often expressed their belief that the current regulatory framework permits the U.S. government overly broad access to data stored in the cloud. We need to have clear laws that prove this belief incorrect.

[7] The International Organization for Standardization (ISO) is the world's largest developer and publisher of international standards.

As part of the private sector, Salesforce.com cannot make representations to its customers that government will not gain access to data. What we can do is point to and explain the legal process that government must undertake to access data held in the cloud. This is why reform of the Electronic Communications Privacy Act is so critical. Because ECPA codifies guidelines for US government access to data, it sends a signal to other countries about the confidentiality of information held in the cloud. As a result, it is urgent that Congress update ECPA **to clarify that data stored and processed in the cloud on behalf of a customer has the same protections and standards for law enforcement access as data stored locally by that customer.**

ECPA has not been significantly revised since it was enacted in 1986 – well before the emergence of cloud computing. Today, ECPA is a patchwork of confusing standards that have been interpreted inconsistently by the courts, creating uncertainty for service providers and law enforcement agencies alike. 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 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.

As Congress contemplates ECPA reform, it should balance the law enforcement interests of government, the privacy interests of users, and the public confidence interests of business. In attempting to balance these interests, Congress should embrace the concept of technology neutrality. In practice, technology neutrality means that a particular kind of information (for example, the content of private documents and communications) will receive the same level of protection regardless of the technology, platform or business model used to create, communicate or store it. We're not asking for special treatment for data stored in the cloud, but rather for equal treatment.

Salesforce.com is part of the Digital Due Process Coalition whose goal is to update ECPA to keep pace with changes in technology. The Coalition did not seek to answer all questions or concerns about ECPA, but it has agreed on four principles that provide a framework for opening a public dialogue on the issue. The overarching goal of the Coalition is as follows:

> *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.*

The Coalition principle that is the most relevant to cloud computing reads as follows:

> *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 or stored data that are not readily accessible to the public only with a search warrant 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.*

What this principle would mean in practice is that the government must 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 would subject private communications, documents and other private user content stored in or transmitted through the Internet "cloud" to 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, digital 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.

Conclusion

In the past decade, 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, jobs, education, democratic participation and social engagement. In order to create the public confidence necessary to fuel continued innovation and economic growth, Congress should update ECPA in ways that preserve law enforcement tools and give companies the clarity they deserve. Congress should extend the traditional warrant standard to our personal communications, private commercial documents and highly sensitive information stored and processed in the cloud. By making sure that ECPA is technology-neutral, Congress can send a clear signal to individuals, companies and governments around the world that they can safely use cloud computing platforms. Doing so will unleash a wave of innovation and productivity that will drive economic growth and create jobs for years to come.

Mr. NADLER. Thank you.

I will now recognize Mr. Robinson.

TESTIMONY OF PERRY ROBINSON, ASSOCIATE GENERAL COUNSEL, RACKSPACE HOSTING

Mr. ROBINSON. Thank you, Mr. Chairman, Members of the Committee. Thank you for taking the time to address this important matter.

I am here on behalf of Rackspace Hosting, and unlike many of the other panelists, which are household names—is that a little bit better?—which are household names, Rackspace is a smaller organization. Provide just a little bit of background: We are a company that is based out of San Antonio, Texas. We were founded in 1998 by four college students.

Over the time we have grown. We have now got about 3,000 employees. We employ people in San Antonio, Texas; Austin; Chicago, Illinois; Herndon, Virginia. And we have had this growth in part due to the growth of the cloud. Rackspace is invested heavily in cloud technology and offers cloud servers, cloud sites, and cloud files to its customers. Now, I provide this information as background to the context in which ECPA applies to a company such as ours, which is an emerging organization.

So I would also like to briefly explain some examples of how Rackspace provides cloud computing technology to its customers. Cloud technology can be somewhat challenging, I think, to understand at first.

The concept at a high level, though, can also be very simple. In fact, for many consumers they are not aware of the times at which they are actually using cloud technology.

To oversimplify the concept a bit, cloud servers is kind of like a motor pool, right, in which a vehicle is provided at just the right time for your use. Its function is the same as a physical vehicle but it has essentially been virtualized through computing code.

The fact that this virtual instance is virtual and not physical in nature, though, doesn't change the experience of the consumer itself. And so the end user of this technology oftentimes has the same understanding of the rights and implications of this use of technology as they would any other traditional form of communication.

Cloud storage, on the other hand, makes use of file technology to provide storage which is provided through a connection to the Internet. Many applications, or apps, on mobile devices and telephones make use of such cloud storage. An example of such storage might be the storage of documents which are created on a mobile device or, as Professor Felten was saying, the use of an online calendar.

For many of its customers Rackspace provides the base technology on which her customers are able to develop the use of cloud servers or cloud storage for the development of their businesses. Our customers are often businesses who are, themselves, providing services to an end user. Now, the complication here is that as you move down the chain you have a process which goes from the provider of the cloud services down to an end user and there is—and that created a gap, sometimes, in which, again, the end user

doesn't always have an absolute understanding of how the technology is actually provided to them.

In each case there are expectations by these users that their use of this technology—of cloud servers, of cloud files—is subject to control of the end user itself and that the content will not be accessed by third parties or others unless permission has been granted. This privacy expectation is a fundamental aspect of the acceptance of cloud technology.

Rackspace believes that ECPA has fallen behind these advances in technology. To be clear, Rackspace does not believe that ECPA is flawed in its intent and does not seek to change the balance of the individual interests and the privacy of their electronic communication with the needs of law enforcement.

However, Rackspace does see ECPA as having fundamentally failed to maintain pace with changes in technology. As a result, there is a great deal of confusion regarding the level of protection afforded to end users which is stored on or accessed through the cloud.

These concerns translate to hesitancy regarding the adoption of cloud technology despite the benefits, the flexibility, and cost savings that it provides. They have a financial impact on the growth of businesses such as Rackspace, Rackspace's other customers, and quite frankly, they have an impact on, potentially, the economy itself.

Rackspace believes now is the time to update ECPA and to bring clarity and predictability to the law so that people will know what protections are afforded to their data and their use of their technology, thereby allowing the sector to grow and create jobs and help drive the economy forward.

Thank you for your time.

[The prepared statement of Mr. Robinson follows:]

PREPARED STATEMENT OF PERRY ROBINSON

Prepared Statement of Perry Robinson

Statement of Perry Robinson
Associate General Counsel
Rackspace Hosting

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

Hearing on ECPA Reform and the Revolution in Cloud Computing

September 23, 2010

Chairman Nadler, Ranking Member Sensenbrenner, and honorable Members of the Committee, my name is Perry Robinson, and I am Associate General Counsel at Rackspace Hosting, a technology company that delivers hosting services to businesses of all sizes and all kinds around the world.

My responsibilities at Rackspace include directing a team of attorneys and legal professionals regarding legal and contractual matters relating to the provision of services to our customers. As part of these responsibilities I oversee Rackspace's program for compliance with state and federal law enforcement agency requests, warrants, and subpoenas; state and federal regulatory requests; and other court orders. I am also a Certified Information Privacy Professional (CIPP) and member of the International Association of Privacy Professionals.

We at Rackspace would like to thank you for the opportunity to share Rackspace's views on the reform of the Electronic Communications Privacy Act of 1986 (ECPA). This initiative is an important one, not only because of the potential impact this initiative can have on the privacy of individuals and the efforts of law enforcement agencies, but also on the economic development and growth of the technology sector in the United States and growing businesses such as Rackspace.

Rackspace Hosting is a company that has specialized in providing dedicated and cloud hosting services as well as paid email service to its customers with products such a Rackspace Managed Hosting, The Rackspace Cloud™ and Rackspace Email & Apps. Rackspace began as the idea of few college students at a small liberal arts university in San Antonio, and since its inception in 1998, Rackspace has built a service oriented IT business by focusing on the hosting needs of its customers and their desire for customer service by providing what Rackspace calls Fanatical Support. Over the last dozen years, Rackspace has transformed from that small college based business to a leading provider of hosting services with more than 99,000 customers including over 80,000 cloud computing customers. Even during these economically challenging times Rackspace has managed to grow, creating employment for thousands of people in San Antonio, Texas; Dallas, Texas; Herndon, Virginia; and Chicago, Illinois.

WHAT IS THE CLOUD?

You may have heard the term cloud computing or 'the Cloud,' but there are so many definitions flying around that you would not be alone if you struggled to

define it. Simply put, cloud computing is a set of pooled computing resources and services delivered over the Internet. Cloud computing should not be confused with grid computing, utility computing, or autonomic computing as it involves the interaction of several virtualized computing resources. As an example, Rackspace's Cloud Servers™ connect and share information based on the level of website traffic across the entire network. Cloud computing is often provided "as a service" over the Internet, typically in the form of infrastructure as a service (IaaS), platform as a service (PaaS), or software as a service (SaaS). Cloud computing delivers flexible applications, web services, and IT infrastructure as a service, over the Internet which allows users to create, store, access and use data from anywhere in the world using an ever growing number of computing and electronic devices.

The availability of cloud computing technology enables the growth of new businesses in which many of the traditional costs are reduced, if not eliminated. Cloud customers don't have to raise the capital to purchase, manage, maintain, and scale the physical infrastructure required to handle drastic fluctuations in the number of users accessing their systems. Rackspace's customers have clearly expressed their desire to make use of these advantages through the adoption of cloud technology, and service providers like Rackspace have invested heavily in the technology that will permit them to do so.

CLOUD COMPUTING TECHNOLOGY AND THE ECPA

When the ECPA became law nearly a quarter century ago, much of the technology driving Rackspace's customer's businesses did not exist. Not only has

computing technology changed and advanced over the past two-plus decades, the consumption and adoption of this technology has changed as well. In fact, it is this consumption and adoption of computing resources that has driven Rackspace's own growth. Rackspace believes that we are in the midst of yet another revolution in computing and technology today as cloud computing comes to the forefront.

While this revolution has already begun, the way that cloud computing technology works, and more importantly, when it is being used, remains murky for many Americans. For example, how many Americans are aware that their free email service is provided through cloud computing? How many are aware that the legal protections regarding their emails can vary because the email service is provided using cloud computing technology? Cloud computing technologies may very well be common place, but many Americans are unaware of the ways in which their data may be accessed under the ECPA when stored with a cloud service provider.

RACKSPACE SUPPORTS ECPA REFORM

Over the past months, you have been presented with the testimony of many learned scholars and professionals regarding the need to update the ECPA and the specific areas where discrepancies or difficulties lie. You have heard repeatedly about confusion in the courts regarding the meaning and intent of the ECPA, and among law enforcement and service providers like Rackspace as well. While there have been differences of opinion as to precisely how the ECPA should be updated, the need for the update is near unanimous. Rackspace too sees the need to reform and update the ECPA.

To be clear, Rackspace does not believe that the ECPA is flawed in its intent, and does not seek to change the need to balance individual interests in the privacy of their electronic communications with the needs of law enforcement, however Rackspace does see the ECPA as having fundamentally failed to maintain pace with changes in technology. This failure to keep pace has created challenges in which the legal protections afforded to a person with regard to a particular piece of information change not based on the nature of the data itself, but on the means of storage including storage with a cloud service provider.

While the way that people create, store, access and use data is changing, expectations regarding privacy have not changed. As a company that has literally based its business on customer service and customer experiences, Rackspace is experiencing challenges in its ability to communicate the applicability of the ECPA to the growing desire by consumers to access the advantages of technology like cloud computing.

For Rackspace, these challenges also translate into economic costs. First, there is the actual cost of providing staff to address law enforcement requests for customer data pursuant to the ECPA. These costs are not limited to the processing of a subpoena or other order, rather, they often extend to legal costs relating to the opinion of counsel. These costs are often times disproportionate to the fees that a service provider such as Rackspace may earn in hosting the data.

Secondly, there is the cost of lost business from abroad. As new laws regarding privacy and data protection emerge all over the world, new and

additional requirements for technology providers and users are also created. Our customers abroad want to do business in the United States, but are often faced with questions about how the ECPA may apply to data stored by their end users. These customers are seeking electronic data privacy laws that are intelligible and predictable so that they can meet regulatory requirements and the expectations of their own customers. The current state of the law as it relates to the ECPA puts American businesses like Rackspace at a significant disadvantage with companies based abroad. Without such clarity, American businesses like Rackspace face challenges in their growth within the United States, ultimately impacting their ability to contribute to the growth of the US economy.

Finally, given the demands of consumers to know how laws that apply to the protection of their electronic data will be applied by law enforcement and the courts, the current lack of clarity in the ECPA has to a degree inhibited the growth and adoption of this technology as a whole.

CONCLUSION

Rackspace strives to balance the understandable demand for privacy that comes from our customers with the equally understandable need of law enforcement to conduct investigations and ensure public safety. Even without other challenges, this balance is not always easy to affect. When one adds in the confusion created by the ECPA's failure to keep pace with technology, and this balance is nearly impossible to maintain.

Whatever changes are made to the ECPA, it is critical that any reform of the ECPA be made "technology neutral" so that future advances in technology do not again result in a statute which has become outdated in light of the technology of the day.

I thank you for the opportunity to share this information with you on behalf of Rackspace, and thank you for your efforts and time in addressing this matter.

Mr. NADLER. Thank you.
And we will now hear from—I will now recognize Mr. Misener.

TESTIMONY OF PAUL MISENER, VICE PRESIDENT FOR GLOBAL PUBLIC POLICY, AMAZON.COM

Mr. MISENER. Thank you very much, Mr. Chairman, and Mr. Franks, and Chairman Conyers, and Members of the Subcommittee. My name is Paul Misener, and I am Amazon.com's vice president for global public policy. On behalf of our company and our millions of customers, thank you very much for inviting me to testify on this important hearing.

Amazon.com Web site began in 1995 as a place to buy books. Since then we have strived to be earth's most customer-centric company where people can find and discover virtually anything that they may want to buy online. Now Amazon Web Services provides a family of cloud computing functions to small and large businesses, government agencies, academic institutions, and other users.

Cloud computing, as others have described for the Subcommittee, is a means of providing, through the Internet, computing functions similar to what a desktop or laptop computing can provide but far more efficiently and reliably, and at much greater scales and speeds. For example, desktop PCs can store files like memos, spreadsheets, digital photos, and music. So can cloud computing services, only much more efficiently and reliably.

A desktop computer's hard drive can crash, for instance, potentially deleting files. Cloud computing storage done well, however, is redundant, and thus files are far more durable and the chance of unintentionally deleting them is virtually nil.

Amazon offers data storage as Amazon Simple Storage Service, or S3. This service can be used to store and retrieve any amount of data at any time from anywhere on the Web. S3 gives users access to the same highly scalable, reliable, secure, fast, inexpensive infrastructure that Amazon uses to run its own global network of Web sites.

The service aims to maximize benefits of scale and pass those benefits to users. In one example a company called ElephantDrive uses Amazon S3 storage to pride consumers an inexpensive way to make backup copies of digital files.

Likewise, desktop PCs can perform calculations on data. Although many of us never perform calculations much more complicated than with spreadsheets, small and large businesses, researchers, and government agencies often need to perform complicated and data-intensive calculations.

Desktop PCs are often not up to the task, and even dedicated local workhorse computers often can't deliver satisfactory results or are a cost-prohibitive capital investment. Cloud computing, on the other hand, can provide virtually unlimited computation capacity that may be rented as needed rather than obtained through a large, wasteful, up-front capital expenditure that requires expert setup and maintenance and rapidly becomes obsolete.

Amazon also offers a service known as Amazon Elastic Compute Cloud, or EC2, that is designed to make Web-scale computing easier. Just as S3 enables storage in the cloud, Amazon EC2 enables compute in the cloud.

The EC2 Web interface allows users to obtain and configure capacity and control computing resources. Users may quickly scale up

capacity—and then down—as their computing requirements change, and they pay only for the capacity that they actually use. In one case an engineer at The Washington Post used the equivalent of over 1,400 server hours on EC2 to convert over 17,000 pages of First Lady Hillary Rodham Clinton's newly-released documents into a Web-friendly format within just 9 hours and for less than $150.

The benefits of these and other cloud computing services to businesses large and small, government agencies, to researchers, and other organizations are manifest. The power of expensive and complicated computer hardware is available immediately on a pay-as-you-go basis. No longer must an enterprise expend capital up front and endure delays. And the computing capacity is completely elastic, scaling up in time of high demand and down as appropriate.

Bottom line, with cloud computing enterprises can focus their engineering resources on their own specialties. No longer must they manage the difficult tasks of building and maintaining computer infrastructure.

Accordingly, we believe that it is in the public interest to ensure that there are no inappropriate legal impediments to cloud computing and that applicable law, including ECPA, is clear and current. We appreciate the Subcommittee's interest in this matter and the investigation of whether and how ECPA should be modified.

Amazon is a member of the Digital Due Process coalition, which has proposed clarifications of ECPA in four areas, covering requests for: one, the content of electronic communications; two, location information; three, real-time transactional data about communications; and four, broad information requests about broad categories of users. Although we are aware, for example, that the standards applied to location information may need clarification our experience primarily relates to requests for the content of communications, as a provider of remote computing service.

With respect to the content of electronic communications we believe that ECPA requires law enforcement authorities to obtain a search warrant to compel disclosure. We do not release information without valid process and have not disclosed content without a search warrant.

In order to protect the privacy of communications we certainly agree with our fellow members of the Digital Due Process coalition that this is how the law should operate: compelled disclosure of content should require a search warrant, just as obtaining content out of a person's desk drawer would. If there is any significant ambiguity in ECPA, such as with respect to the age of a communication, we would support legislation to clarify that compelled disclosure of content may only come as a result of a search warrant, regardless of the age of a communication.

Thank you again for the opportunity to testify on the important topic of cloud computing services. Amazon believes that these new services have important societal benefits, and if laws such as ECPA should be clarified to address cloud computing we support the effort.

[The prepared statement of Mr. Misener follows:]

PREPARED STATEMENT OF PAUL MISENER

Statement of

Paul Misener
Vice President for Global Public Policy, Amazon.com

At the Hearing

"ECPA Reform and the Revolution in Cloud Computing"

Before the

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

September 23, 2010

Good morning, Chairman Nadler, Ranking Member Sensenbrenner, and members of the Subcommittee, my name is Paul Misener, and I am Amazon.com's Vice President for Global Public Policy. On behalf of my company and our millions of customers, thank you very much for inviting me to testify at this important hearing on cloud computing.

The Amazon.com website began in 1995 as a place to buy books. Since then we have strived to be Earth's most customer-centric company, where people can find and discover virtually anything they want to buy online, and now Amazon Web Services provides a family of cloud computing functions to small and large businesses, government agencies, academic institutions, and other users.

Cloud computing, as others have described for the Subcommittee, is a means of providing, through the Internet, computing functions similar to what a desktop or laptop

computer can provide, but far more efficiently and reliably, and at much greater scales and speeds.

For example, desktop PCs can store files, like memos, spreadsheets, digital photos, and music. So can cloud computing services, only much more efficiently and reliably. A desktop computer's hard disk drive can "crash," for instance, potentially deleting files. Cloud computing storage done well, however, is redundant and thus files are far more durable and the chance of unintentionally deleting them is virtually nil.

Amazon offers data storage as Amazon Simple Storage Service, or "S3." This service can be used to store and retrieve any amount of data, at any time, from anywhere on the web. S3 gives users access to the same highly scalable, reliable, secure, fast, inexpensive infrastructure that Amazon uses to run its own global network of web sites. The service aims to maximize benefits of scale and to pass those benefits to users. In one example, a company called ElephantDrive uses Amazon S3 storage to provide consumers an inexpensive way to make backup copies of digital files.

Likewise, desktop PCs can perform calculations on data. Although many of us never perform calculations much more complicated than with spreadsheets, small and large businesses, researchers, and government agencies often need to perform complicated and data-intensive calculations. Desktop PCs are often not up to the task, and even dedicated local workhorse computers often can't deliver satisfactory results or are cost-prohibitive capital investments. Cloud computing, on the other hand, can

provide virtually unlimited computation capacity that may be rented as needed, rather than obtained through a large, wasteful up-front capital expenditure that requires expert set-up and maintenance and rapidly becomes obsolete.

Amazon also offers a service known as Amazon Elastic Compute Cloud, or "EC2," that is designed to make web-scale computing easier. Just as S3 enables storage in the cloud, Amazon EC2 enables "compute" in the cloud. The EC2 web interface allows users to obtain and configure capacity and control computing resources. Users may quickly scale capacity, both up and down, as their computing requirements change, and they pay only for capacity that they actually use. In one case, an engineer at *The Washington Post* used the equivalent of over 1400 server hours on Amazon EC2 to convert over 17,000 pages of First Lady Hillary Rodham Clinton's newly-released documents into a web-friendly format – within just nine hours and for less than $150.

The benefits of these and other cloud computing services – to businesses large and small, to government agencies, to researchers, and other organizations – are manifest. The power of expensive and complicated computer hardware is available immediately, on a pay-as-you-go basis. No longer must an enterprise expend capital up front and endure delays. And the computing capacity is completely elastic, scaling up in time of high demand and down as appropriate. Bottom line, with cloud computing, enterprises can focus their engineering resources on their own specialties. No longer must enterprises manage the difficult tasks of building and maintaining computing infrastructure.

Accordingly, we believe it in the public interest to ensure that there are no inappropriate legal impediments to cloud computing and that applicable law, including the Electronic Communications Privacy Act (or "ECPA"), is clear and current. We appreciate the Subcommittee's interest in this matter and its investigation of whether and how ECPA should be modified.

Amazon.com is a member of Digital Due Process, a coalition of companies, public interest groups, scholars, and others that was formed "[t]o 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." Amazon also supports several other members of this group, including the Center for Democracy and Technology and the American Booksellers Foundation for Free Expression.

The Digital Due Process coalition has proposed clarifications of ECPA in four areas, covering requests for (1) the content of electronic communications; (2) location information; (3) real-time transactional data about communications; and (4) bulk information about broad categories of users. Although we are aware, for example, that the standards applied to location information may need clarification, our experience primarily relates to requests for the content of communications.

With respect to the content of electronic communications, we believe that ECPA requires law enforcement authorities to obtain a search warrant to compel disclosure. We do not release information without valid process and have not disclosed content without a search warrant. In order to protect the privacy of communications, we certainly agree with our fellow members of the Digital Due Process coalition that this is how the law *should* operate: compelled disclosure of content should require a search warrant, just as obtaining content out of a person's desk drawer would. If there is any significant ambiguity in ECPA, such as with respect to the age of a communication, we would support legislation to clarify that compelled disclosure of content may only come as a result of a search warrant, regardless of the age of a communication.

Thank you again for the opportunity to testify on the important topic of cloud computing services. Amazon believes that these new services have important societal benefits, and if laws such as ECPA should be clarified to address cloud computing, we support the effort.

* * * * * * *

Mr. NADLER. Thank you very much.

We will now begin the questioning by—I will recognize myself for the 5 minutes.

Professor Felten, in your testimony you described the many ways you use cloud computing technology and services in your professional and personal life. When you think about your and society's digital life now as compared to 1986 do you think that ECPA's 1986 concept of electronic communications service and remote communications service accurately reflect network usage today, and if not why not?

Mr. FELTEN. I think not. In 1986 it made more sense, in terms of people's use of these services, to separate communication and computing into separate products and separate mental categories, but these days these computation, storage, and communication are really integrated together to provide a unified product that meets some need of the end user for managing a calendar, or document collaboration, or whatever it is that the user is wanting. Users often don't think about and often don't know what is happening behind the scenes to make all this work, and so it is a line that is not visible to a lot of the decision-makers, and it makes a lot less sense than it did then.

Mr. NADLER. Thank you. And you also, in your testimony, discussed the fact that it may be difficult for a user to tell whether or not his or her data is stored in the cloud because cloud services can offer nearly the same user experience as local servers. And as someone who uses a computer all the time and never heard the phrase "cloud computing" until a few weeks ago I certainly never think about—or certainly never thought about—whether it is in the cloud or not.

Elaborate on this concept, and how might a user be unaware or unsure of whether or not he is working or operating in the cloud, and why should it make a difference to him?

Mr. FELTEN. Well, at one level it should not make a difference to the user as long as the job that they want done is being done well. It may prove to make a difference to the user if there is a legal line that gets drawn.

But increasingly what users are after is the experience of solving their problem, doing their job without having——

Mr. NADLER. And they don't care how it is done. They just care about the result; they don't care how the problem is solved.

Mr. FELTEN. Absolutely.

Mr. NADLER. Thank you.

Mr. Salgado and perhaps Mr. Hintze, my understanding is the Stored Communications Act, and specifically the electronic communications service and remote communications services distinctions can be difficult to apply to many of today cloud-based services, as Professor Felten just said. And of course, under the law ECS provides greater privacy protection than RCS.

What position do you generally take regarding classifying services or information as either ECS or RCS and the legal process you require before disclosing information when you get law enforcement requests for the following: Web mail search—on the one hand, Web mail search, word processing, online photo video storage services, and on the other, names or I.P. addresses of users who search for

a specific phrase? And in answering the question, please indicate whether you must make creative arguments or take an aggressive view of the law in order to provide great privacy protections to your customers—in order to provide the privacy protections you thing they require.

Mr. Salgado first?

Mr. SALGADO. Thank you, Mr. Chairman. The question is complicated because of how the ECPA is written, so I apologize at the beginning for probably not being able to address each one of those categories, but it is the very fact of the complexity of ECPA that makes that difficult to answer.

In in ideal world I would like to be able to tell you, this is the type of legal process we require for all those types of information and it is a result of a—it is the result of a thoughtful balance and a consideration of the equities of law enforcement and the interests of the users and the providers. That is not the situation and so the result is, as you list these different products each one of those requires a separate legal analysis, oftentimes requiring consulting with outside counsel, pulling out the statute again, rereading the statute to figure out what type of legal process is required for what types of data.

The distinctions between RCS and material and ECS material are often arbitrary, and even within the category of ECS material—electronic stored material—the definition is so tiered and complex there is nothing intuitive about it. It often turns on whether the communication is, using the terms of the statute, in electronic storage. And I think a lot of people, if you ask them, "What does it mean to be in electronic storage?" would answer, "It means to be stored electronically," and they would be wrong. And in fact, they would have to look at the statute to understand that that term is actually a very complex, tiered test to figure out whether something is in electronic storage for the purposes of the statute.

This is where the 180-day rule comes in. That is the part of the definition of electronic storage. So the question you ask is a complex one because the statute doesn't make it an easy answer.

I think the Digital Due Process coalition members believe the answer to that should be, it requires a search warrant. It should require a search warrant.

Mr. NADLER. And Mr. Heintz, would you comment on the same question? In particular, indicate whether your experience has necessitated the use of what one might call creative arguments or an aggressive view of the law in order to do your job properly.

Mr. HINTZE. Certainly. I would be happy to. I would point out that, as Mr. Salgado's experience as both a prosecutor and in business having trouble answering these questions, you know, I think that is indicative of the fact that all of us do and these are very complicated matters.

You know, the various types of data that may become an issue here—of those probably the ones that ECPA speaks to most clearly would be e-mail, because that was one of those things that was contemplated at the time that ECPA was drafted. But as we have heard, the way e-mail is used has changed dramatically since 1986 and a lot of those distinctions make—no longer make sense, although I think it is quite clear that e-mail is an ECS under ECPA

and the content of a message and the subject line would be considered content and protected by the warrant statute standard up to 180 days or up to when it has been opened, except for in the 9th Circuit where it is—so crystal clear, right?

Other services are even more difficult to discern and what the various levels of protection might be depending on the nature of the service, the nature of the data, the timeframe under which it has been stored electronically, what circuit you happen to reside in.

Mr. NADLER. And all this is carefully considered in the privacy expectations by the customer, right?

Mr. HINTZE. Yes, absolutely.

You know, I think also, you know, some of these questions are theoretical. You know, the bulk of the requests we get from law enforcement are for traditional communications, e-mail. Some of these things we just simply haven't gotten requests.

But you look at new services like search that both Google and Microsoft provide, and the question is how that applies under these definitions. I mean, looking at the definitions you would have no idea. There are arguments that could be made in different ways.

I mean, we think probably the best interpretation of search under ECPA is that the query itself would be content, yes, but you know, trying to find that and trying to discern that in the statute is very difficult. That is why we—one of the reasons we support the Digital Due Process coalition principles is that it makes those distinctions. While it doesn't touch the definitions, per se, it says that all content, whether the content of a search query or the content of an e-mail, the content of your documents would be protected by the warrant standard for probable cause.

Mr. NADLER. Thank you.

Let me ask Mr. Schellhase and Mr. Robinson, both of your firms have indicated in your written testimony that you have customers who are concerned that the U.S. government has overly-broad access to their data that is stored in the cloud. What you appear to be saying is that overly-broad U.S. government access to data is a consideration for some customers in determining whether they should put their information in the cloud.

How does such a concern affect your business model? How do you address this concern with your customers? What aspects of ECPA reform could address this issue specifically?

Let me add one other thing: Why should we protect people who want to keep secrets from the government? Isn't that for no good purposes?

Mr. SCHELLHASE. I will answer first, Mr. Chairman. I think in part what we fight largely is a perception problem, right? And there is a perception on the part of many of our European customers and prospects that the U.S. government has undue access to data——

Mr. NADLER. More from European than from the American customers?

Mr. SCHELLHASE. Yes. Much more from European customers.

But nevertheless I think, you know, the defense that we fall back on, as I mentioned in my testimony, is we provide contractual assurances but we also look to the U.S. to have appropriate due process around accessing data, and so that—you know, so any consist-

ency and reinforcement of consistency in the law benefits us when we sell to customers who have this perception.

Mr. ROBINSON. Yes, a similar situation on Rackspace's side. A good deal of my time is spent each week explaining to customers, both from the United States and customers in Europe and Canada, Australia, basically all over the world, exactly what circumstances in which their data may be accessed, right? And what becomes difficult is with the current state of the law, with ECPA that answer is not easy, right? And so it makes it a very challenging discussion.

The answer, quite frankly, is if we are required by law to provide your information over we will have to do that. They say, "Okay, in what circumstance?"

Well, that is a very long conversation. Where would you like to start? You get into the specifics of how ECPA applies and, you know, as some of the other panelists have mentioned you have to start at times, you know, going back to the statute, considering, you know, bringing in outside counsel especially.

This makes it challenging to do business, and quite frankly it has an impact on our ability for our product.

Mr. NADLER. Thank you very much.

My time is expired. I now recognize the gentleman from Arizona.

Mr. FRANKS. Well, thank you, Mr. Chairman. It seems like this is a pretty important subject.

It occurs to me that even programs and whole systems essentially could eventually be completely operated in the cloud and all of the programs could be updated from there, even operating systems where you only have an Internet operating system intervening between the customer and the cloud. And it is a pretty impressive technology and so it does seem to be a very, very important trend.

And I guess I will start out by asking you, Mr. Hintze—and I am assuming it is Hintze and not Hintze, correct?

Okay, Mr. Hintze, you state that in a poll conducted by Microsoft earlier this year that 90 percent of the general population and senior business leaders say that they are concerned about the security and privacy of data as it relates to cloud storage, and I guess my question is, does this number specifically relate to concern about a government intruder or is this number broader to include criminals and other individuals seeking to hack into the cloud, and is that a significant issue?

Mr. HINTZE. It certainly is a significant issue, and that number encompasses both. People are concerned about the impact on their privacy and security of their data as they put it in the cloud. Whether that is from the government, whether it is from the service provider itself, or whether it is from nefarious actors outside of the service provider who are trying to get into it.

That is one of the reasons that we support a broad approach to addressing these privacy issues and security issues in the cloud. In addition to privacy vis-a-vis the government we think that there is a role for Congress in ensuring privacy vis-a-vis service providers' own practices, which support broad privacy legislation affecting the private sector.

We think that law enforcement should be given tools to go after the hackers who are trying to get into the cloud. We think there

is a role for giving service providers a private right of action to go after those malicious actors as well, and other similar enhancements of security online.

And then, as I mentioned in my oral testimony, these issues are not simply U.S.-focused as well, and we think that as cloud infrastructures grow and data crosses borders we are seeing increasing challenges with respect to the laws of a foreign government that create conflict of laws issues, distinctions between law enforcement and privacy, and data retention and privacy, and we think there is a role for Congress to encourage the Federal Government to engage on a bilateral and multilateral basis to address some of those.

Mr. FRANKS. Well, it takes me in a little different direction where I was going, but let me go ahead and ask this based on some of your comments: While the cloud would be subject to the jurisdiction of the United States, you know—or I guess that is if the cloud resides in the United States—wouldn't a U.S.-based cloud with heightened access requirements for law enforcement be potentially a haven for laundered or data hiding, or would this be especially attractive to foreign customers as a result? In other words, does it represent any sort of a vulnerability for data to be stored in a cloud here in the United States and sort of hidden away based on some nefarious or malevolent purpose?

Mr. HINTZE. As we have heard from other panelists today, today the concern is that the standards around government access to data may be lower than in other places, so there is a concern from foreign customers particularly about doing business with U.S. providers, which makes it challenging for us to sell our products and services to customers outside the United States.

With the Digital Due Process coalition proposals we think that will bring more clarity and bring the statute back into balance and line with where the judgments were made between the interests of privacy and law enforcement back when they were in 1996. We view it as a fairly modest proposal, not one that would create such high barriers that the United States would be looked at as some kind of data haven that Switzerland——

Mr. FRANKS. I understand.

Mr. HINTZE [continuing]. Computing.

Mr. FRANKS. Well, Professor Felten, you state that even those few who don't know or don't even use the Internet or don't have cell phones will still leave an extensive electronic trail online, including their health records and financial records, you know, and I guess I would ask you to elaborate both on the cell records that we leave, our health care records, all of the records that we leave just as a matter of doing everyday activities.

Are those things left in the cloud somewhere? Is there a way to ever completely erase them? And in terms of the actual practice—and I don't want to make this too complicated—of law enforcement, does law enforcement on a routine basis ask for that data that is just kind of somewhere out there floating without a clear reference point?

Mr. FELTEN. Well, as to what data there is and where it might be stored, I as a consumer have little idea. Most businesses keep extensive records of the interactions they have with their customers. That is true in a lot of areas such as health care as well.

Cell phone companies have records which they keep for some length of time about the location and movement and calls, and so on. And in today's world where computer storage is so cheap the default, in a lot of cases, is to keep everything in the hopes that there might be a business use for it.

And so I think it is very difficult for consumers to really know exactly what exists, but as more things go online and as areas like health care move toward electronic records and toward networking you are going to see more and more of the characteristics of the cloud emerging there as well.

Mr. FRANKS. But do you think—and I throw this last question out, Mr. Chairman, to anyone to—do you think that there is a vulnerability in general for the myriad amounts of information that represent text messages, and pictures, and things that people send all the time? Is that something that is regularly or even irregularly accessed by either law enforcement or hackers, or just in general?

I mean, how safe is our information out there right now? Is it something where a lot of it is compromised?

Mr. FELTEN. Certainly there are compromises and it is something that we should be concerned about. There are a lot of different types of data and they can be mosaicked together to get a lot of information about what people are doing, and especially to track down people who might have special concerns about being victims of crimes. I think it is an issue that is important even beyond the scope of ECPA.

Mr. FRANKS. Mr. Chairman, it is an important issue and I yield back.

Thank you all.

Mr. NADLER. Thank you.

I would like to follow up one thing Mr. Hintze said. You mentioned private right of action by victims of hackers?

Mr. HINTZE. Among the things we have supported would be a private right of action for cloud service providers to go after——

Mr. NADLER. Cloud service providers. Does the victim already have that private right, does he not?

Mr. HINTZE. I think under some cases that might be the case. We do think that the service providers have the resources and the incentives to really go after the hackers——

Mr. NADLER. And they don't have that private right of action?

Mr. HINTZE [continuing]. Private right of action today under the Computer Fraud and Abuse Act.

Mr. NADLER. Thank you very much. I want to thank this panel for their expert testimony, and thank you.

And let's seat the second panel. We are going to have a series of votes in a few minutes but we can get some of this done before that series of votes.

And again, thank you to the members of the first panel.

We will now proceed with our second panel. I would ask the witnesses to take their places. In the interest of time I will introduce the witnesses while they are taking their seats, although I see they have already done that.

Kevin Werbach is an associate professor of legal studies at the Wharton School, University of Pennsylvania. Professor Werbach co-led the review of the Federal Communications Commission for the

Obama administration's presidential transition team and was an advisor in broadband issues to the FCC and the National Telecommunications and Information Administration.

Earlier in his career he served as counsel for new technology policy for the FCC during the Clinton administration. Professor Werbach received his J.D. from Harvard University and his B.A. from University of California at Berkeley.

Fred Cate is the distinguished professor and C. Ben Dutton professor of law, adjunct professor of informatics and computing, and director of the Center for Applied Cybersecurity Research at Indiana University.

I won't ask you today, but sometime you will tell me what informatics is.

Professor Cate served as a member of the National Academy of Science's committee on technical and privacy dimensions of information for terrorism prevention, counsel to the Department of Defense technology and privacy advisory committee, and as a member of the Federal Trade Commission's advisory committee on online access and security. He earned his undergraduate and law degree from Stanford University.

Senior Investigator Thomas H. Hurbanek—and I hope I got that right—is a 24-year veteran of the New York State Police. He has been assigned to the state police computer crime unit since 1997, working on investigations and forensic cases involving computers and technology. His current assignment involves supervising the cybercrime and critical infrastructure response section of the computer crime unit, working jointly with Federal and state agency partners to respond to incidents impacting New York's computing infrastructure.

Kurt Schmid has been a law enforcement official for 40 years and currently serves as the executive director of the Chicago High Intensity Drug Trafficking Area, or HIDTA, program. Previous to this assignment Mr. Schmid served as senior law enforcement advisor for the Counterdrug Technology Assessment Center and the national director of the HIDTA program in the White House Office of National Drug Control policy in Washington for 10 years.

Marc Zwillinger is a founding partner of Zwillinger Genetski, LLP, where for 10 years his practice has focused on issues related to Electronic Communications Privacy Act, the Wiretap and Communications Act, surveillance law and privacy. Previously Mr. Zwillinger ran the privacy and security practice groups at Sonnenaschein Nath & Rosenthal and at Kirkland & Ellis.

Prior to that he served 3 years as a trial attorney in the computer crime and intellectual property section of the criminal division of the Department of Justice. Mr. Zwillinger earned his J.D. magna cum laude from Harvard Law School.

I am pleased to welcome all of you. Your written statements will be made part of the record in their entirety. I would ask each of you to summarize your testimony in 5 minutes or less, and I presume you heard what I said about the lights earlier and what they mean.

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

If you would please stand and raise your right hands to take the oath?

Let the record reflect that the witnesses answered in the affirmative, and you may be seated.

Well, we can start the testimony. We will see how far we get before we are called to votes.

So I will recognize Professor Werbach to begin.

TESTIMONY OF KEVIN WERBACH, PROFESSOR, THE WHARTON SCHOOL, UNIVERSITY OF PENNSYLVANIA

Mr. WERBACH. Thank you, Mr. Chairman, Congressman Franks, and Members of the Committee.

On the prior panel you heard from a number of cloud computing vendors. As a business school professor who studies emerging technologies I would like to give you a broader picture of the business changes that the Internet has fostered in recent years. Reform of ECPA should be considered against the backdrop of these trends.

Cloud computing is not just a set of popular services like Web mail or even a market segment; it is all around us. The quarter-century from the birth of the personal computer industry until 2000 marked the progress towards, in the words of Microsoft's original mission statement, "a computer on every desk and in every home."

Today the model is no longer one computer per person but many devices for each user in different locations offering different form factors and functionality. This multi-device era is necessarily a connected era because devices draw upon the network to offer services, and it is necessarily a cloud computing era.

When users access their data from many devices that data must be stored remotely or synchronized through the network. In particular, the growth of mobile smartphones, like the iPhone and Android devices, and newer classes like netbooks, tablets such as the iPad, and set-top boxes eliminate the traditional assumption that a personal computer is the sole repository of a user's information and application. As these devices proliferate file-hosting and software as a service will become integral parts of the computing experience rather than options.

The Internet is no longer a nascent technology. There are over 2 billion people around the world online. In 1986, when ECPA was passed, there were no Web sites; in 1996 there were roughly 100,000; today there are over 100 million.

Facebook was just founded in 2004. It now has half a billion members worldwide. I could give many other examples.

As the external usage of the network has changed the internal components have evolved as well. Google probably has more Web-connected servers than the entire Internet did 15 years ago, all linked into a colossal virtual super-computer.

Many other providers are building their own cloud data centers. All others tap into public clouds from companies like Amazon.com.

Increasing bandwidth and storage are making the cloud architecture increasingly pervasive. These cloud-based services are online intermediaries. The Internet creates and depends upon a large number of such intermediaries, including search engines,

ecommerce marketplaces, social networks, content hosting tools, collaboration services, payment processors, and more.

These intermediaries create value for users and sometimes become application platforms of their own. However, they also necessarily raise important privacy and security issues. By their very nature cloud computing intermediaries require users to give up physical control over their data. This distributed processing can be transparent to the end user who may not realize that her data is sitting in a pool of servers far away.

In several statutes Congress effectively made a deal with online intermediaries. They avoid intermediary liability in return for commitment not to meddle with their users' data and to establish orderly procedures for access when sought for legitimate purposes, such as law enforcement. This structure underlies the safe harbors of Section 230 of the Telecommunications Act of 1996 and Section 512 of the Digital Millennium Copyright Act.

This safe harbor approach provides confidence for all parties. A user has the confidence his or her information won't be accessed inappropriately; the service provider has confidence it won't accrue legal liability for the actions of its users; and law enforcement and other outside parties such as copyright holders have the confidence that service providers will provide them with access to necessary information subject to an appropriate process.

All that, however, depends on clear definitions. If user data stored in the cloud is not subject to appropriate protections from unauthorized access, both private and governmental, trust in could computing could be undermined.

A loss of trust in the Internet would impact far more than the companies providing cloud-based services. If users lose their trust in online intermediaries some will use encryption to make data less visible, some will keep more data locally even when the cloud architecture provides clear benefits, and some will simply engage in less activity online. These actions will be based on incomplete information and confusion.

In other words, a drop in trust in online intermediaries will inevitably add greater friction to the Internet economy. The health of the Internet should be a national priority. American businesses and consumers have benefited enormously from the growth of our Internet economy during the past 2 decades and cloud computing represents the next evolution of that economy.

Already, there are few Americans who do not have some of their data stored on remote servers by these online intermediaries. Congress must consider how to ensure that our legislative and regulatory regimes do not undermine the benefits the Internet provides.

Thank you.

[The prepared statement of Mr. Werbach follows:]

PREPARED STATEMENT OF KEVIN WERBACH

Written statement of

Kevin Werbach

Associate Professor of Legal Studies & Business Ethics,

The Wharton School, University of Pennsylvania

Hearing on ECPA Reform and the Revolution in Cloud Computing

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

September 23, 2010

Hearing on ECPA Reform and the Revolution in Cloud Computing
September 23, 2010

Written Statement of Kevin Werbach

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

Thank you for holding this hearing on the important issues around privacy and cloud computing, and for inviting me to testify. I am an associate professor of Legal Studies at the Wharton School of the University of Pennsylvania, and the founder of Supernova Group, an independent technology consulting firm. As FCC Counsel for New Technology Policy in the Clinton Administration, and as a member of the Presidential Transition Team for the Obama Administration, I saw how government actions can positively or negatively influence technological development. In my work as a scholar, I examine how policies supporting open, interconnected networks promote benefits such as innovation, investment, job creation, free expression, and U.S. global competitiveness.

In considering reform of the Electronic Communications Privacy Act (ECPA) in the age of cloud computing, this committee and the Congress have an opportunity to update our legal regime to reflect major changes in the technological environment over the past two decades. My testimony highlights these developments. In particular, I will highlight four major changes since the passage of ECPA in 1986:

- The move from personal computing to connected computing.
- The evolution of the Internet to a ubiquitous global platform for information, communications, and commerce.
- The emergence of cloud computing, and the business drivers of its growth.
- The importance of online intermediaries to trust in the Internet ecosystem.

Reform of ECPA should be considered against the backdrop of these broader trends. In each case, legislation and other government decisions have influenced the business environment, and will continue to do so.

From PCs to Connected Devices

The quarter-century from the birth of the personal computer industry until 2000 marked the successful progress toward, in the words of Microsoft's original mission statement, "a computer on

every desk and in every home." The second stage of the information age involves the transformation of those personal computers into connected devices. The model is no longer one computer per person, but many, in different locations, offering different form factors and functionality. Apple, for example, sells the MacBook, the iPhone, the iPad, and the Apple TV, all of which are powerful personal computing devices. Users are not expected to choose among them, but to use each in different situations, as well as to access connected services from other devices at work or elsewhere.

The explosion of mobile devices accentuates this trend. Fifteen years ago, mobile phones were a luxury enjoyed by a small percentage of Americans. Today they are ubiquitous. Those phones have also steadily increased in functionality, becoming powerful handheld computers. With continuing advances in computing capacity and improvements in mobile networks, this trend will only continue. Major wireless network operators are beginning to roll out fourth generation (4G) mobile networks, offering substantially greater data capacity. In addition, an increasing number of phones support local wireless connections through WiFi or other technologies.

The iPhone did not exist in 2006. Within five years, every mobile phone sold in the US will likely be what is today considered a high-end smartphone: a device capable of accessing Internet-based services and running applications. These phones will increasingly integrate cameras, location detection, accelerometers, touch screens, and other features. And they will support large application ecosystems, much as Microsoft's Windows laid the foundation for a vast personal computer industry. There are already over 250,000 iPhone apps, and a growing number on competing platforms such as Android and Blackberry.

The multi-device era is necessarily a connected era, because the devices draw upon the network to allow themselves to offer smaller form factors and lower prices. And it is necessarily a cloud computing era. When users access their data from many devices, that data must be stored remotely in the network or synchronized across the devices through the network. In particular, the growth of mobile smartphones and the newer classes of netbooks and tablets eliminates the traditional assumption that a personal computer is the repository of all a user's information and applications. File hosting and "software as a service" will become integral parts of the computing experience, rather than options.

The combination of a pervasive Internet, widespread adoption of mobile devices, and rapid growth of cloud computing generate business activity that is already significant and increasingly massive. Moreover, there are few Americans who will not have some of their personal data stored on remote servers by online intermediaries. Government action to promote trust in electronic

commerce and legislation creating safe harbors for digital intermediaries played an important role in the growth of the Internet ecosystem over the past fifteen years. There can be little doubt that the Internet has been a major boon to innovation, investment, freedom, and other national goals. Congress must now consider how to ensure that outdated legislative and regulatory regimes do not undermine those benefits in the coming years.

The Evolution of the Internet

The Internet today is both an essential business tool and an integral part of daily life for the vast majority of Americans. Many of us still talk about the Internet as a nascent technology. In reality, it has been roughly fifteen years since the Internet and electronic commerce first reached the commercial mass market, following more than twenty years of gestation as a research network. Though it is still developing, the Internet is now a major, well-established platform for communications, entertainment, information, and commerce.

Every day, hundreds of millions of Americans use the Internet to check the weather, book travel reservations, look up recipes, buy gifts, read the news, chat with friends, check their bank accounts, reserve movie tickets, research medical information, share photos, track sports scores, look for jobs, look for dates, watch television shows, watch short videos, play games… and countless other common activities. Online chatter and social networks drive success of every major entertainment category, online information sources are having a dramatic effect on the media, online resources and fund-raising are decisive elements of major political campaigns, and online transactions represent an ever-growing share of virtually every form of commercial activity.

Over 240 million Americans, nearly 80% of the population, are now Internet users, according to Nielsen. Millions more have access to the Internet at work. And with over 285 million US mobile phone subscribers and widespread deployment of WiFi wireless hotspots, a majority of American adults already access the Internet through wireless connections, according to the Pew Research Center. That latter number is growing especially rapidly. Globally, there are two billion people online, and over five billion mobile phones in use, an increasing percentage of which offer Internet connectivity. The Internet is the mass medium of the 21st Century.

Even more significant than the size of the Internet today is how Internet usage has changed. In 1995, accessing the Internet meant initiating a dial-up connection through a modem attached to a personal computer, at speeds that required several seconds to download a single image file. Today, the vast majority of American Internet users have broadband access, an "always on"

service roughly 100 times as fast.[1] Software and hardware have evolved to offer a smoother, richer, more sophisticated Internet experience. Personal computers and even packaged software applications now build in automatic updating and other communications functions, taking for granted an Internet connection as an integral part of the experience.

In 1996, when Congress passed the Communications Decency Act, there were approximately 100,000 websites in existence; today there are well over 100 million. In 1998, when Congress passed the Digital Millennium Copyright Act and the Internet Tax Freedom Act, Google had not yet been founded. In fact, virtually none of the top 100 sites on the Web today were in existence at that time.[2] Facebook, the most popular site on the Web today, was only launched in 2004. Today it has over half a billion users worldwide. I could cite many other examples. The point is that the Internet of 2010 is not the Internet fifteen or ten or even five years ago. And the Internet of 2015 or 2020 will diverge even further from the past.

Rise of the Cloud

As the external usage of the network has changed, the internal components have evolved as well. Cloud computing is an approach that places application processing and storage in network based data centers rather than solely in end-user devices such as personal computers. There are many definitions of cloud computing, but experts agree on one thing: this shift to network-based functionality will have massive business impacts. As John Hagel and John Seely Brown of Deloitte's Center for the Edge recently stated, "Cloud computing has the potential to generate a series of disruptions that will ripple out from the tech industry and ultimately transform many industries around the world."[3]

Fifteen years ago, many websites resided on a single server computer. Even very popular sites might only have a handful of servers fed by "load balancing" software at a single location. Today, the leading Internet companies build massive, multi-billion dollar data centers the size of several football fields, each housing thousands of networked computers. A major service provider such as Google has more web-connected servers than the

---

[1] A February 2010 FCC survey found that 78% of American adults are Internet users and 65% have home broadband access. *See* Broadband Use and Adoption in America, John B. Horrigan, OBI Working Paper No. 1, at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-296442A1.pdf.

2 *See* The 1000 Most-Visited Sites on the Web, *at* http://www.google.com/adplanner/static/top1000/.

[3] John Hagel III and John Seely Brown, Cloud Computing's Stormy Future, HBR Blog, September 14, 2010, *at* http://blogs.hbr.org/bigshift/2010/09/cloud-computings-stormy-future.html.

entire Internet fifteen years ago, all linked into a colossal virtual supercomputer. And Google is at the leading edge of a huge trend. Smaller providers such as Twitter are building their own data centers, while others tap into "public clouds" offered by companies such as Amazon.com.

The rise of smart connected mobile devices further feeds this trend. Due to their small size, mobile phones do not have the same storage capacity as personal computers. Even when used for services such as email or document review, they are almost never a user's sole computing device. Rather, provide a mobile "window" into the user's data. As a result of these two factors, virtually any application involving significant amounts of user data on mobile devices will incorporate remote storage and a cloud computing architecture. This is equally true for mobile access to a consumer service such as iTunes for music or Yelp for local restaurant information, as for business applications such as Salesforce.com or Google Docs.

The momentum toward cloud computing is strong. A solid majority of experts participating in a recent Pew Foundation Future of the Internet Survey expected that in a decade, most people will access software applications and share information through remote servers rather than desktop applications.[4] Cloud computing involves much more than a few high-profile applications such as GMail and Salesforce.com. Startup companies increasingly rely on public clouds provided by vendors such as Amazon.com in lieu of building and maintaining their own server infrastructure. At the other end of the spectrum, large online service providers as well as enterprises with their own existing data center infrastructure are all potential or actual cloud computing providers.

The business case for cloud computing is based on three core benefits.

First, there are significant economies of scale in delivering application functionality through large remote data centers. Service providers can operate, configure, and update a centrally-managed collection of resources more efficiently than individual users responsible for their own personal computers. Backup, business continuity, security, and other utility functions are significantly more efficient if deployed across a large virtualized cloud of computers. The cost is shared across all the customers, and the cloud provider can develop expertise beyond that of individual companies.

---

[4] Janna Quitney Anderson and Lee Rainie, The Future of Cloud Computing, Pew Internet and American Life Project, June 11, 2010, *at* http://pewresearch.org/pubs/1623/future-cloud-computing-technology-experts.

Second, because it allows many users to share large utility computing clusters, cloud computing is a better solution when demand fluctuates. Consider a startup launching a new web-based service. It has to ensure that it has enough processing and storage capacity to meet user demand. If the company must provision servers itself, there may be a substantial cost and delay to increase capacity when it under-estimates demand. And if the company over-estimates demand, it will spend unnecessary resources provisioning servers that it doesn't use. In one case, the service may crash, and in the other, the company wastes money. Neither is an attractive outcome. Moreover, demand forecasting is a constant exercise. What if the company runs a special promotion that causes a short-term spike in usage? Or what if it offers an enterprise service that is lightly used on the weekends? There is no way for any individual company to match supply and demand efficiently.

In a cloud computing environment, on the other hand, companies share virtual capacity in massive clouds. The scale of the cloud platforms makes capacity a commodity for the provider, so overprovisioning is not the same difficulty as for individual companies. The cloud provider can also deploy virtualization software and other technical mechanisms to more efficiently utilize its capacity. Aggregation of demand across different services with different requirements naturally tends to smooth out spikes. Especially in a fast-changing environment, the cloud approach therefore provides a more efficient and higher performing solution than companies could provide through local self-provisioning.

Third, cloud computing allows the service provider to capture and aggregate large volumes of user data. This information can help the service provider improve its service, or it can open up new business opportunities. Gmail, which generates revenue through targeted advertisements, is a good example. Google does not need to charge for its email service, even though the gigabytes of storage it provides to users are not costless to provision. Instead, Google monetizes Gmail by algorithmically matching message text to targeted advertisements. Only because Google can aggregate large numbers of ads and large volumes of email text in the same computing environment as its analytical software can it make this model work.

From a pricing standpoint, cloud computing overcomes many of the problems with traditional software business models. It produces recurring revenue streams, which are often more attractive than one-time payments. It allows customers to "pay as you go", without substantial up-front costs, and to scale up or down their financial commitments as needed. For businesses, cloud computing represents a shift from computing services as a set of capital expenditures - servers, bandwidth, software

licenses, software maintenance, IT staff, etc. - into a payment analogous to other utilities such as electricity and water.

Cloud Providers as Intermediaries

In the early days of e-commerce, there was much enthusiasm for the concept of disintermediation. Rather than operate through a middleman such as a retail store or an insurance agent, a supplier of products or services could use the Internet to interact directly with its customers, cutting costs and improving efficiency along the way. To some extent this has been the case, but the disintermediation story is incomplete. The Internet in fact creates and depends upon a new set of digital intermediaries. The oceanic quantity of information available online overwhelms the ability of any user to find the most relevant, highest quality resources on their own. Online intermediaries can perform these functions and add additional value in the process.

Search engines were the first prominent online intermediaries. Users can connect to any website directly, but it takes the incredibly sophisticated analytics and massive computing power of sites such as Google and Bing to sift in real time through billions of pages and show the user where to find what they were looking for. E-commerce sites such as eBay and Amazon.com also function as intermediaries, not only processing transactions, but offering features such as ratings, recommendations, wish lists, and other functions beyond the capability of any physical world retailer. Facebook knits together social networks and provides hosting for billions of messages, photos, videos, links, and other materials. Paypal offers payment processing functionality so that virtually any online business can access payments efficiently from users around the world.

The companies in these examples have gone even further by establishing application programming interfaces (APIs) to allow other providers to plug into their platforms. Consider a company such as Zynga, a developer of social games. It operates largely on top of Facebook, rather than as a standalone website. By leveraging Facebook's massive user base, development tools, and social networking tools, Zynga quickly developed a string of massively successful games. It reportedly will generate $500 million in revenue this year, its most recent venture capital funding valued the company at well over $1 billion, and it is on track for an initial public offering. Zynga is an intermediary for tens of millions of players, but it is an intermediary that itself connects to other intermediaries such as Facebook and PayPal. The relationships between those providers necessarily involve sharing of user data.

Online intermediaries therefore necessarily raise important privacy and security questions. The growth of cloud computing will bring these issues to the forefront. By its very nature,

cloud computing requires users to give up physical control of their data, and allow it to reside on the remote infrastructure of an intermediary provider. This applies to both the identity information about who the user is and where information is being transported, as well as the content of that information. While there are technical mechanisms to secure that data, it is the service provider, not the user, that must implement them. Users in many cases will not even realize that their data is sitting on remote servers and subject to inspection or distribution. Cloud computing makes distributed processing transparent to the end-user, so a user may have no indication that her data is no longer sitting on her PC, but on a rack of servers far away.

A smooth transition to cloud computing requires users to continue feeling a sense of trust online. In the early days of e-commerce, users hesitated to give their credit cards to websites. The idea of typing this information into a machine seemed scary. Concerns about fraud held back the growth of e-commerce. It was only through a combination of technical measures to secure information, adoption of best practices in part through government prodding, and gradual development of user confidence that this hurdle was overcome. Every time an ordinary American ordered a book on Amazon.com or bought a collectible on eBay and got what they paid for, their trust in the Internet increased a little bit. Even more important, that American's friends and family saw the same thing. The gradual accumulation of positive experiences, and the relative paucity of negative experiences, brought the Internet to its current point of mainstream acceptance.

If circumstances change, this trust could unravel. At the margin, users will choose to engage more or less actively online based on their own experiences and those of their friends and families. Already, the large amount of personal information regularly shared on social networks has produced sharp concerns in many quarters. Though it is fashionable to assert that today's young people are unconcerned about privacy, research shows that in many ways they feel even more strongly about the need to control their personal information than their elders.[5]

Users care about protection of their data, and will change their behavior if they feel the protections are insufficient. Some users will switch to more secure providers, some will use encryption to make their data less visible, some will keep more data locally even when the cloud architecture provides clear

---

[5] *See* danah boyd and Eszter Hargittai, Facebook Privacy Settings: Who Cares?, First Monday, August 2010, *at* http://www.danah.org/papers/2010/FM-FacebookPrivacySettings.pdf; Mary Madden and Aaron Smith, Reputation Management and Social Media, Pew Internet and American Life Project, May 2010, *at* http://www.pewinternet.org/Reports/2010/Reputation-Management.aspx.

benefits, and some will simply engage in less activity online. All of these actions will be based on incomplete information and colored by confusion or inaccurate rumors. In other words, a drop in trust in online intermediaries will have unpredictable results, but will inevitably add greater friction to the Internet economy. That friction will be a drag on the continued growth of online activity, and all the benefits it brings.

One important reason for the level of confidence about Internet privacy is an implicit deal embedded in several key Internet-related statutes. The essence of this deal is that service providers avoid intermediary liability in return for a commitment not to meddle with user information, and to establish orderly procedures for access when sought for legitimate purposes such as law enforcement and stopping copyright infringement. This structure underlies the safe harbors in Section 230 of the Telecommunications Act of 1996, as well as Section 512 of the Digital Millennium Copyright Act. It represents an extension of the common carriage mechanism that historically applied to telephone companies, and data privacy restrictions that Congress imposed on cable television providers.

The safe harbor approach is valuable because it provides confidence for all the potential parties. A user has confidence that if she makes information available to an online service provider, that information won't be accessed inappropriately. The service provider has confidence that it won't accrue legal liability for the actions of its users. Given the enormous scale and velocity of online information flows, any regime requiring online providers to monitor or approve user activity beforehand is likely to be infeasible. Investors will hesitate to fund business models when massive liability could undermine a profitable business. Finally, law enforcement and other outside parties such as copyright holders have the confidence that service providers will provide them access to necessary information, subject to an appropriate process.

If user data stored in the cloud is not subject to appropriate protections from unauthorized access, trust in cloud computing could be undermined. This is true whether the access is by private or governmental actors. The fallout from a loss of trust in the Internet would be felt not only by companies that provide cloud-based services, but by the much larger community of businesses they connect to, and by users themselves. In considering ECPA reform, this committee should consider not only the appropriate balance between the needs of law enforcement and protection of civil liberties, but also the effects of its decisions on the health of the Internet ecosystem.

Conclusion

The health of the Internet should be a national priority. Most of the greatest Internet startup success stories are based

here in the U.S., and American businesses and consumers have benefitted immensely from the growth of our Internet economy during the past two decades. Cloud computing represents a new stage in the evolution of that economy. U.S. Internet leadership stems in part from our success in implementing "a predictable, minimalist, consistent and simple legal environment," in the words of the 1997 *Framework for Global Electronic Commerce*. However, the solutions of the past may not be the best ones for the present or the future. Keeping old rules in place may actually create inconsistency and uncertainty. It is incumbent upon Congress and the other arms of the Federal Government to consider how to achieve legitimate public policy objectives consistent with the fast-changing technological environment.

Mr. NADLER. Thank you.

We will now hear from our second witness. Professor Cate is recognized.

TESTIMONY OF FRED H. CATE, PROFESSOR, DIRECTOR, CENTER FOR APPLIED CYBERSECURITY RESEARCH, INDIANA UNIVERSITY

Mr. CATE. Thank you very much, Mr. Chairman, Mr. Franks.

I have been asked to present a brief overview of the Stored Communications Act, and although I would rather describe almost anything else I will nevertheless take the next few minutes to do so. But before doing so I would like to say first, Mr. Chairman, how much I appreciate your holding these hearings today and the series of hearings that you have been holding about Electronic Communications Privacy Act reform. It is a critical issue and worthy of the attention that you and this Committee have been devoting to it.

The primary constitutional limit on the government's ability to obtain personal information about individuals is the Fourth Amendment. However, under the Supreme Court's Third Party Doctrine records disclosed to or held by a third party receive no constitutional protection. Searches of these records need not be reasonable and no judicial oversight is involved.

Congress responded to the Court's Third Parry Doctrine decisions by enacting a variety of laws to put in place statutory protections where constitutional protections were missing. One of those was the Stored Communications Act, which deals, of course, as you know, with communications and other records in electronic storage such as e-mail and voicemail.

The 1986 Senate report on the Stored Communications Act explains that computer users at that time generally used network services in two ways. First, they used networks to send and receive e-mail.

Second, they used network services to remotely store and process data—in other words, to do things which they could not do on a local computer. Both of these sets of uses would receive no constitutional protection so Congress enacted statutory protection.

And the Stored Communications Act divides stored electronic communications into two categories responding to these two predominant uses in 1986. An electronic communication service is defined by the statute as the temporary, intermediate storage of a wire or electronic communications incidental to the electronic transmission thereof, as well as storage for certain backup protections. A remote computing service is the provision to the public of computer storage or processing services by means of an electronic communication system.

Now, records within an electronic communication service, an ECS, are further divides into subcategories based on the duration of storage. So government demands for records that are held as part of an ECS that have been stored for 180 days or less require a traditional warrant issued by a competent court.

To obtain material within an ECS that has been stored for more than 180 days or to obtain material stored as part of an RCS, or remote communication service, the government has three options. It can use a warrant; it can use a subpoena, which has no involve-

ment of a court; or it can use a court order based on specific and articulable facts, sometimes called a 2703D order, or a D order, for short.

If the government chooses not to provide notice to the individual then a warrant is required. If it does provide contemporaneous, or in some cases delayed, notice then it may use a subpoena or a D order, at its election. Under either category of service, an ECS or an RCS, a service provider may voluntarily provide the records to the government certain to—subject to certain limitations.

Now, complicating this already somewhat complicated picture is the fact that the Department of Justice believes, and most courts who have considered the issue to date have agreed, that the warrant requirement for records stored 180 or less only applies to unopened e-mail. If you have opened the e-mail it is automatically kicked into the more-than-180-days rule, which would allow access without the involvement of a court.

Information about a customer's account, as opposed to the content of a customer's communication, may be obtained under a much lower standard, either, again, with a warrant, a 2703D order, or, in the case of telemarketing fraud, merely upon formal written request—it takes no judicial authorization at all. And even more basic information, what the statute refers to as "basic subscriber information," such as name and address and length of service and type of service and means of payment, can be obtained with an administrative subpoena, a grand jury subpoena, or a trial subpoena—again, no involvement of a court; these can be issued by the law enforcement agency itself.

This quite complicated set of arrangements is actually described in a chart in my prepared testimony. It is rare that I would ever refer you to a chart, but this is one instance in which the Committee might find it of some use.

So let me conclude by noting, as I think you have heard already, the Stored Communications Act has been the subject of considerable criticism, and that criticism might be divided into a number of categories. I would encourage you to distinguish between two, however: those which related to the—what we might think of as the ambiguity or the drafting of the statute itself, and those—which I think have been highlighted this morning—those caused by the transformation in the technology, transformation which has actually rewritten the statute without any action by Congress or by this Committee.

Thank you very much.

[The prepared statement of Mr. Cate follows:]

PREPARED STATEMENT OF FRED H. CATE

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

Hearing on

ECPA REFORM AND THE REVOLUTION IN CLOUD COMPUTING

Washington, DC
September 23, 2010

Statement of Fred H. Cate
Distinguished Professor and C. Ben Dutton Professor of Law
Director, Center for Applied Cybersecurity Research
Indiana University

Chairman Nadler, Representative Sensenbrenner, and Members of the Subcommittee,

My name is Fred Cate, and I am a Distinguished Professor and C. Ben Dutton Professor of Law at the Indiana University Maurer School of Law, and the director of Indiana University's Center for Applied Cybersecurity Research, a National Center of Academic Excellence in Information Assurance Education and in Information Assurance Research.

For the past 20 years I have had the privilege of researching and teaching about a variety of privacy, security, and other information law and policy issues. I served as a member of the National Academy of Sciences Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, reporter for the American Law Institute's project on Principles of the Law on Government Access to and Use of Personal Digital Information, and counsel to the Department of Defense Technology and Privacy Advisory Committee.

In addition to my academic appointment, I am also a senior policy advisor to the Centre for Information Policy Leadership at Hunton & Williams LLP, a member of Microsoft's Trustworthy Computing Academic Advisory Board, a member of Intel's Privacy and Security External Advisory Board, editor of the Privacy Department of the IEEE's (Institute of Electrical and Electronic Engineers) *Security & Privacy*, and one of the founding editors of the Oxford University Press journal, *International Data Privacy Law*, among other activities.

I am testifying today on my own behalf; the views I express should not be attributed to any organization with which I am affiliated.

Chairman Nadler, I want to begin by thanking for your leadership in holding this important series of hearings of Electronic Communications Privacy Act reform, and for inviting me to participate in today's hearing on Title II of that Act, the Stored Communications Act (SCA),[1] and how it affects, and is affected by, the rise of cloud computing.

---

[1] Pub. L. No. 99-508, Title II, § 201, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2701-2711).

I have been asked to present a brief overview of the SCA and how it interacts with cloud computing, and I am delighted to do so. I will begin with a brief survey of the constitutional background to the statute.

The Fourth Amendment and the "Third Party" Doctrine

The primary constitutional limit on the government's ability to obtain personal information about individuals is the Fourth Amendment, which reflects the Framers' hostility to "general searches"—searches not based on specific suspicion.[2]

The Fourth Amendment does not purport to keep the government from conducting searches or seizing personal information. As interpreted by the Supreme Court, it requires that the government generally conduct searches with a warrant issued by a court.[3] For a court to issue a warrant, the government must show "probable cause" that a crime has been or is likely to be committed and that the information sought is germane to that crime.[4] The Supreme Court also generally requires that the government provide the subject of a search with contemporaneous notice of the search.[5]

The Court has repeatedly found that the Fourth Amendment (and its requirement for a warrant) only apply to searches of material or places in which there is a "reasonable expectation of privacy." In his 1967 concurrence in *Katz v. United States*, Justice Harlan wrote that reasonableness was defined by both the individual's "actual," subjective expectation of privacy and by an objective expectation that was "one that society was prepared to recognize as 'reasonable.'"[6] The Court adopted that test for determining what was "private" within the meaning of the Fourth Amendment in 1968 and continues to apply it today.[7]

The Court wrote in *Katz* that "what a person knowingly exposes to the public . . . is not the subject of Fourth Amendment protection."[8] While in the context in which this was originally used, this language is perfectly understandable, the Court's subsequent interpretations of this passage have created a significant exception to the Fourth Amendment's scope and protection.

The Supreme Court applied this language in 1976 in *United States v. Miller*[9] to hold that there can be no reasonable expectation of privacy in information held by a third party. The case involved cancelled checks, to which, the Court noted, "respondent can assert neither ownership nor possession."[10] Such documents "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business,"[11] and therefore the Court found that the Fourth Amendment is not implicated when the government sought access to them:

---

[2] U.S. Constitution amend. IV.
[3] Akihl Reed Amar, *The Constitution and Criminal Procedure* 3-4 (1997).
[4] 68 *American Jurisprudence 2d*, Searches and Seizures § 166 (1993).
[5] Richards v. Wisconsin, 520 U.S. 385 (1997).
[6] 389 U.S. 347, 361 (1967).
[7] Terry v. Ohio, 392 U.S. 1 (1968).
[8] 389 U.S. at 351-52.
[9] United States v. Miller, 425 U.S. 435 (1976).
[10] Id. at 440.
[11] Id. at 442.

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[12]

The Court's decision in *Miller* is remarkably sweeping. The bank did not just happen to be holding the records the government sought. Instead, the Bank Secrecy Act required (and continues to require) banks to maintain a copy of every customer check and deposit for six years or longer.[13] The government thus compelled the bank to store the information, and then sought the information from the bank on the basis that since the bank held the data, there could not be any reasonable expectation of privacy and the Fourth Amendment therefore did not apply.[14] A majority of the Supreme Court was not troubled by this application of the Fourth Amendment.[15]

The Court reinforced its holding in *Miller* in the 1979 case of *Smith v. Maryland*, involving information about (as opposed to the content of) telephone calls.[16] The Supreme Court found that the Fourth Amendment is inapplicable to telecommunications "attributes" (e.g., the number dialed, the time the call was placed, the duration of the call, etc.)—what today we would describe as "metadata"—because that information is necessarily conveyed to, or observable by, third parties involved in connecting the call.[17] "[T]elephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes."[18]

Under the Supreme Court's "third party doctrine," records disclosed to, and held by, third parties receive no constitutional protection. Searches of these records need not be reasonable. And no judicial oversight is involved.

<u>The Stored Communications Act</u>

Congress responded to the Court's decisions with a variety of laws, including the Right to Financial Privacy Act,[19] which deals with access to financial records, and the Pen Register Act,[20] which deals with access to telephone calling records. Congress also enacted the Stored Communications Act—

---

[12] Id. at 443 (citation omitted).

[13] 12 U.S.C. § 1829b(d); see 425 U.S. at 436; California Bankers Assn. v. Shultz, 416 U.S. 21 (1974).

[14] 425 U.S. at 443.

[15] Id. at 444 ("even if the banks could be said to have been acting solely as Government agents in transcribing the necessary information and complying without protest with the requirements of the subpoenas, there would be no intrusion upon the depositors' Fourth Amendment rights").

[16] 442 U.S. 735 (1979).

[17] Id. at 743.

[18] Id.

[19] 12 U.S.C. §§ 3401-3422.

[20] 18 U.S.C. §§ 3121-3127.

Title II of ECPA and the subject of today's hearing—which deals with communications and other records in electronic storage, such as e-mail and voice mail.[21]

The 1986 report on the SCA explains that computer users at that time generally used network services in two ways. First, they used network services to send and receive email. Second, they used those services to remotely store and process data.[22] Both services raised privacy concerns because both involve third parties maintaining copies of individual users' mail, documents, and other records. Under the Supreme Court's third-party doctrine, these materials would receive no Fourth Amendment protection.

The SCA divides stored electronic communications into two categories, reflecting the two predominate uses in 1986. An "Electronic Communication Service" ("ECS") is defined by the statute as the "temporary, intermediate storage of a wire or electronic communications incidental to the electronic transmission thereof" and storage for "backup protection."[23] A "Remote Computing Service" ("RCS") is the "provision to the public of computer storage or processing services by means of an electronic communications system."[24]

Records within an ECS are further divided into subcategories based on duration of storage. Government demands for records held as part of an ECS and that had been stored for 180 days or less require a traditional warrant issued by a competent court.[25] To obtain material within an ECS that has been stored for more than 180 days, or to obtain material stored as part of an RCS, the government has three options: it can use a warrant, it can use a subpoena (an administrative subpoena, a grand jury subpoena, or a trial subpoena), or it can use a court order based on "specific and articulable facts" (sometimes called a "2703(d) order" or a "d order").[26] If the government does not provide notice to the individual, then a warrant is required.[27] If it does provide contemporaneous or, in some cases, delayed notice, then a subpoena or 2703(d) order may be used.[28] Under either category, a service provider may *voluntarily* provide the records to the government (subject to certain limitations).[29]

Complicating this analysis is the fact that the Department of Justice believes, and most courts to consider the issue have agreed, that the warrant requirement for records stored 180 days or less only applies to *unopened* email or other communications content.[30] Under this view, once email has been

---

[21] Pub. L. No. 99-508, Title II, § 201, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2701-2711).

[22] S. Rep. No. 99-541, at 2-3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3556-57.

[23] 18 U.S.C. § 2510(17).

[24] Id. at § 2510(17)(B).

[25] Id. at § 2703(a). See generally Daniel J. Solove, "Electronic Surveillance Law," 72 *George Washington Law Review* 1264, 1283 (2004).

[26] 18 U.S.C. at §§ 2703 (a)-(b).

[27] Id. at § 2703(b)(1)(A).

[28] Id.

[29] Id. § 2702. These are carefully analyzed in Orin S. Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," 72 *George Washington Law Review* 1208 (2004).

[30] See Kerr, supra at nn.82-95 and sources cited therein.

opened, the government may access it from an ECS provider under the lower standard applicable to RCS material. The Ninth Circuit has taken a different view.[31]

information *about* a customer's account, or about communications (but not including the communications content), maintained by a communications provider can be obtained by the government by providing a warrant, a 2703(d) order, or, in the case of telemarketing fraud, upon formal written request.[32] Other "basic subscriber information," including name, address, length of service and types of service, means of payment, and local and long distance connection records, can be obtained with an administrative subpoena, a grand jury subpoena, or a trial subpoena.[33]

The following table summarizes the type of authorization necessary to obtain personal information held by an ECS or RCS provider under the SCA.

Stored Communications Act Summary of Authorization Necessary to Obtain Data			
ECS contents held unopened in "temporary, intermediate storage" or stored for "backup protection" for 180 days or less	ECS contents after they have been opened, or held unopened in "temporary, intermediate storage" or stored for "backup protection" for more than 180 days, or RCS contents	Information about a subscriber account (but no contents of records)	"Basic subscriber information" (but no contents of records)
Search warrant	If no notice: search warrant; if notice: a subpoena or a 2703(d) order	2703(d) order or, in the case of telemarketing fraud, formal written request	A subpoena

Violations of the SCA carry a minimum fine of $1,000; no exclusionary rule applies.[34]

Critique

The SCA has been the subject of considerable criticism. That criticism generally might be divided into five broad categories. The first is that the statute is "dense and confusing."[35] Law enforcement officials, service providers, and courts have considerable difficulty understanding and applying the statute. The result is that it is often misapplied. This situation serves no one's interest, because it means that the SCA provides inadequate protection for privacy and inadequate certainty for when law enforcement can access important information.

The second category of criticism is that the SCA is ambiguous, especially in the light of significant changes in online services markets. It is not clear that the market ever divided neatly into

[31] In *Theofel v. Farey-Jones*, 359 F.3d 1066, 1076 (9th Cir. 2004), the Ninth Circuit concluded that all e-mails held by a server are protected under the ECS rules until "the underlying message has expired in the normal course," regardless of whether the e-mail has been accessed.

[32] 18 U.S.C. § 2703(c)(1).

[33] Id. § 2703(c)(2).

[34] See Daniel J. Solove, "Electronic Surveillance Law," 72 *George Washington Law Review* 1264, 1284 (2004).

[35] See Kerr, supra.

communications services and remote storage and processing services, but today, with the advent of a massive digital economy, those lines are infinitely more difficult to draw. Similarly, the content versus noncontent information distinction, which might have made sense with physical mail (contents vs. envelope) or even telephone calls (content vs. number dialed), is much harder to apply with digital materials. And even the distinction between voluntary disclosure and law enforcement demands has proved problematic in practice. For example, which is it when a state attorney general contacts an ISP and asks for its "voluntary" assistance identifying child pornography, promising to laud the business if it helps and excoriate it in the press if it does not?

The third category of criticism concerns the lack of publicly available, aggregate statistics detailing the extent to which third party providers are routinely compelled to deliver their customers' communications and other private data to law enforcement agencies. Congress already requires mandatory annual reports for the use of wiretap, pen register, and trap and trace orders. As a result, academics, public interest advocates, and policy makers are generally able to determine the extent to which such surveillance methods are used.[36] Congress has not created similar statutory reporting requirements for law enforcement agencies' use of warrants, "27303(d) orders, and subpoenas to obtain individuals' communications contents and other private data. The only information about the scale of such activities available to policy makers comes from voluntary disclosures by a few service providers willing to discuss such practices.[37] Because most service providers do not disclose this information, Congress and the people have no reliable data to determine the scale of this form of electronic surveillance, which is likely to outnumber the 2,376 wiretap orders granted in 2009, and the 11,126 pen registers and 9,773 trap and trace orders granted in 2008.[38]

The fourth category of criticism concerns the level of protection provided by the SCA as a legal matter. Under the third-party doctrine, the Supreme Court has determined that material in the hands of third parties gets no constitutional protection. In a series of statutes, Congress has clearly indicated that it disagrees. However, the SCA provides quite limited protection for most of the material to which it applies, requiring only a subpoena if contemporaneous notice is given to the affected individual(s). Subpoenas require no judicial oversight; many agencies issue them on their own authority, and prosecutors often issue subpoenas in the name of grand juries without any procedural determination that the information sought is relevant. Moreover, subpoenas do not have to target information about specific individuals; a law enforcement agency could use a subpoena to demand all of the records held by a provider of ECS or RCS. Finally, the SCA does not apply to all data stored in the hands of a third party, or even all data stored electronically in the hands of a third party. ECS and RCS have specific definitions in the statute, and those definitions exclude the significant range of internet sites that provide neither communications services nor remote processing services. As a result, even in 1986, it was an inadequate response to the Court's third-party doctrine.

---

[36] 18 U.S.C. § 2519. See generally, Wiretap Reports, Administrative Office of the US Courts, available at: http://www.uscourts.gov/Statistics/WiretapReports.aspx.

18 U.S.C. § 3126. These reports are not made public, but have been obtained by researchers via the Freedom of Information Act. The reports for the years 1999-2008 can be found at http://www.spyingstats.com/.

[37] For example, see Google's government request tool, available at: http://www.google.com/governmentrequests/.

[38] The pen register reports for 2009 have not yet been obtained by privacy advocates. 2008's report can be found here: http://files.spyingstats.com/pr-tt/DOJ-pen-registers-2004-2008.pdf

The fifth and final category focuses on the extent to which dramatic changes in technologies and online services—especially cloud computing—have rendered both the third-party doctrine and the SCA inadequate to protect privacy today. Professor Daniel Solove has written: "We are becoming a society of records, and these records are not held by us, *but by third parties*."[39] These records are generated through our daily transactions, our searches online, and our internet browsing, but they are also the result of a growing number of online services that provide free storage as a way of attracting customers (and viewers for online advertising). Remote storage is wide available today for financial records, test results from home health devices, photographs, music, data about collections (of books, music, or hobbies), remote computer back-up, and email. Remote storage facilitates off-site back-up and can make data more accessible from different locations.[40]

To take just one practical example, and one of the types of material the SCA was intended to protect, in 1986 email was just coming into widespread use. The norm was for email to be retrieved and stored locally, on the user's machine, because storage was expensive and few vendors wished to provide it. As the price of storage has dropped, and competition in online services has grown, most email service providers now offer vast amounts of email storage—in fact, some now offer *unlimited* storage—as a way to attract customers. Remote storage of email is today a fact of life and a basic consumer expectation. It facilitates ease of access as we move from one computing device to another—so I can access the same email from my office desktop, my laptop, my iPhone, and my home computer; it allows for automatic backup; and it makes it easier to share photos, music, and movies, which is a growing use of email. Moreover, as the price of storage has dropped and processing power and search capabilities have grown, more people are now keeping all of their email as a virtual filing system. Under the framework of which the SCA is a part, email gets one standard of protection while being composed and later retained in their "sent" mail folder, one while in transit, one in remote storage until opened or 180 days has passed, and one standard after being opened or 180 days has passed.[41] Most of the standards of protection provided by the SCA (all of the standards applicable to remove storage for communications or as part of a remote processing service) are substantially weaker than that ordinarily required by the Fourth Amendment, and do not even require judicial oversight. And even these weaker standards of protection do not apply where no communications service or remote processing is involved.

This is inadequate protection: inadequate to protect privacy and inadequate to provide government officials with clarity about what they are permitted by law to access and the procedures they must follow when they do so. The officials run the risk of either moving forward too aggressively, and thereby trampling civil rights and potentially exposing themselves to liability, or holding back through an excess of caution and thus failing to serve national interests effectively. These are not speculative costs; they are well documented in other legal settings in numerous Inspector General and other government reports.[42]

---

[39] Daniel J. Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy," 75 *Southern California Law Review* 1083, 1089 (2002) (emphasis added).

[40] See generally Fred H. Cate, "Government Data Mining: The Need for a Legal Framework," 43 *Harvard Civil Rights-Civil Liberties Law Review* 436 (2008).

[41] See generally James X. Dempsey, "Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology," *Ninth Annual Institute on Privacy and Security Law* (PLI) 543, 562 (2008).

[42] See *Semiannual Report to Congress [on the] Federal Bureau of Investigation, October 1, 2007-March 31, 2008*, supra; *A Review of the FBI's Use of National Security Letters* (2008), supra; *A Review of the FBI's Use of Section 215 Orders for Business Records in 2006* (2008), supra; *The FBI's Use of National Security Letters and Section 215 Requests for Business Records*, supra (statement of Glenn A. Fine);.*A Review of the Federal Bureou of*

Moreover, as consumers embrace ever more complex information technologies, such as GPS enhanced mobile devices and cloud computing services, it becomes less likely that average users understands the technologies on which they depend, and the degree to which their private data is transmitted to third parties. Therefore, the concept of "voluntary disclosure" on which the third-party doctrine depends, and which is reflected in the considerably lower protection that the SCA accords to such information, is simply not warranted. Earlier this month the Third Circuit ruled on this very issue, in a case involving the application of the SCA to stored location data, deciding that:

> A cell phone customer has not "voluntarily"' shared his location information with a cellular provider in any meaningful way . . . [because] it is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information."[43]

Conclusion

There seems unanimous agreement that the SCA needs to be revised. The Digital Due Process Coalition has put forth one set of proposals that command broad industry and academic support, and are specifically designed to provide substantive protection for privacy, while also permitting law enforcement access to relevant documents, and to do so in a way that is clear and easy to understand.[44] As a member of that coalition, I hope you will give those proposals your careful consideration.

As you think about ways forward, I encourage you to remember that none of the protections under the Fourth Amendment, in the current SCA, or in the Digital Due Process Coalition's proposals block access to relevant records or the ability for providers to voluntarily provide law enforcement agencies with such information in emergencies. Rather, the goal is to ensure that an appropriate process is followed and that such a process includes appropriate oversight.

Thank you again for the opportunity to participate today.

Investigation's Use of National Security Letters (2007), supra; *FBI Use of National Security Letters*, supra (statement of Glenn A. Fine); *The FBI's Use of National Security Letters and Section 215 Requests for Business Records*, supra (statement of Glenn A. Fine).

[43] In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, No. 08-4227 (3d Cir., Sep. 4, 2010), available at http://www.ca3.uscourts.gov/opinarch/084227p.pdf.

[44] See http://www.digitalducprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163.

Mr. NADLER. Thank you.

As you may have noticed, the buzzers have rung. We have four votes on—five votes on the floor. It will probably take about 40, 45 minutes, of which 10 minutes have already elapsed. So I thank the witnesses for their indulgence.

I will recess the hearing until immediately after the last of the five votes, and I urge the Committee Members to return as soon as possible immediately after the last vote. Pending the completion of the votes on the floor the Committee is in recess.

[Recess.]

Mr. NADLER. The Committee will reconvene, and I thank everyone for their patience. We are about to hear from Mr. Hurbanek, is recognized.

TESTIMONY OF THOMAS B. HURBANEK, SENIOR INVESTIGATOR, COMPUTER CRIME UNIT, NEW YORK STATE POLICE

Mr. HURBANEK. Chairman Nadler, Congressman Franks, and Members of the Subcommittee, my name is Thomas Hurbanek, and I am a senior investigator with the New York State Police computer crime unit, a statewide detail of specially trained investigators and civilian staff that provides investigative and forensic support to state, local, and Federal law enforcement agencies. Thank you for the opportunity to testify about ECPA reform and the revolution in cloud computing.

Today I would like to highlight the challenges that cloud computing presents to state and local law enforcement officers who are attempting to investigate and prevent crimes in order to protect the citizens and businesses within their jurisdiction.

We can look at cloud computing from two perspectives. First, there is the delivery of computing services to end users over the Internet; second, the migration of business computing infrastructure to shared resources accessed over the Internet, which can be provided within the enterprise or provisioned from third party providers.

The connected consumer of today can be accessing and storing information over the Internet using many devices—home and work computers, one or more smartphones or other devices connected to multiple wireless providers, GPS units, game consoles, e-readers, even vehicles. The consumer can be communicating with thousands of people using social networking sites, multiple e-mail messaging and Internet telephone accounts, and identities avilable from hundreds of possible providers while also transacting business with thousands of companies from around the world.

Criminals have adopted every piece of this technology and used it to improve their ability to commit crimes or to victimize individuals and businesses worldwide with no regard for borders, laws, and jurisdiction. This can make investigations involving the Internet daunting for the majority of police officers and extremely challenging even for highly trained investigators with access to advanced tools and equipment.

One example is the theft of online banking credentials, where highly organized groups are using very sophisticated attacks to compromise legitimate Internet sites, infect the computing devices we rely on, obtain legitimate access credentials, and steal millions of dollars from consumers, small-to medium-sized business, local governments, and school districts. Banking regulators estimate that more money is being stolen in online thefts than through traditional bank robberies.

In the state of New York there are nearly 20 million people. Citizens and businesses expect that when the call the New York State Police or one of over 500 local police agencies because they are a victim of crime that their case can be investigated. When the crime involves the use of devices connected to the Internet one of the primary sources of information are business records maintained by private sector entities from one-person, home-based business to multinational corporations.

In New York State law enforcement does not have administrative subpoena power. Requests for subpoenas must first be reviewed by the district attorney and then presented to a grand jury. Each county has its own procedure and criteria for requesting and obtaining subpoenas, and in some jurisdictions they can be difficult to obtain, especially for investigations involving non-felony offenses.

Time is our enemy in Internet investigations. Records and communications may not be retained or information may intentionally or accidently be deleted or corrupted. Technology has created many new sources of information that may be accessed by law enforcement equalized by the very number of private sector entities that must be contacted to build information during an investigation.

The advances of cloud computing present even more challenges for law enforcement. I would like to highlight a few of these.

Encryption: Companies are using advanced encryption technology to secure data transmitted across the Internet. This may create situations where law enforcement does not have the technological means to access communications regardless of the legal authority to do so. The recent concerns in many countries about the encryption implemented on Blackberry devices demonstrates this problem.

Virtualization: We are rapidly moving to an environment where software applications run on virtual computers and servers that can instantly——

Mr. NADLER. Excuse me. Could you enlighten us what you mean by "virtual computers and servers"?

Mr. HURBANEK. Yes. Virtual computers would be a server that is run in memory, so it loads up and it runs only while the machine is running and then shuts down. It is not a physical device. So I could run—and the Rackspace guys could talk about this—I could run 100 servers in memory on one machine. Does that explain it, or——

So the applications or the computers could instantly be started, stopped, refreshed, removing traces of data that law enforcement has been able to access during the forensic examination of seized computers. These virtual environments can be operated outside of the United States.

Data storage: With the evolution of cloud computing services the storage locations for data will often be out of the jurisdiction of state and local law enforcement. Data will also be stored outside of this country and not only in jurisdictions that have a friendly relationship with the United States.

And apps: Applications in the cloud can be accessed from anywhere and data can be imported from one storage location, processed, and returned to the original location or another location.

At the New York State Police we cannot sit at our computer and access the extensive data about individuals and their transactions with companies on the Internet. There is no database that lets me choose an individual and identify all of the e-mail, messaging, and social networking accounts they use. I cannot access the subscriber information for all Internet-based telephone accounts like we have done in the past with telephone subscriber directories.

I would like to close with an example from a recent case in New York State. While investigating a business and executing a search warrant at the business location it was discovered that there were no financial records about the business stored on site. All records were stored and processed on offshore servers which were accessed from the business and the accountants for the business accessed a limited number of records from a different location to prepare tax returns.

This is just one example of how the technological advances and jurisdictional issues created by cloud computing may already be negating the fact that there are new sources of transactional records being maintained by companies operating on the Internet, especially in the case of state and local law enforcement.

Thank you for the opportunity for the New York State Police to provide testimony.

[The prepared statement of Mr. Hurbanek follows:]

PREPARED STATEMENT OF THOMAS B. HURBANEK

Before the
U.S. House of Representatives, Committee on the Judiciary
Subcommittee on the Constitution, Civil Rights, and Civil Liberties

HEARING ON
ECPA REFORM AND THE REVOLUTION IN CLOUD COMPUTING
September 23, 2010

Written Statement of Thomas B. Hurbanek
Senior Investigator
New York State Police Computer Crime Unit

Chairman Nadler, Ranking Member Sensenbrenner, and Members of the Subcommittee, my name is Thomas Hurbanek, and I am a Senior Investigator with the New York State Police Computer Crime Unit, a statewide detail of specially trained investigators and civilian staff that provides investigative and forensic support to State, Local, and Federal law enforcement agencies. Thank you for the opportunity to testify about ECPA reform and the revolution in Cloud Computing.

Today, I would like to highlight the challenges that Cloud Computing presents to State and Local law enforcement officers who are attempting to investigate and prevent crimes in order to protect the citizens and businesses within their jurisdiction. The Electronic Communications Privacy Act can provide a confusing set of rules regarding law enforcement access to business records, communications, and stored data, yet any reforms must be carefully weighed to preserve the existing balance between individual privacy and the ability of law enforcement to conduct investigations and protect the public. Legislation that targets a specific technology, such as cell phones, could also impact other technologies involving Internet connected devices.

We can look at Cloud computing from two perspectives. First there is the delivery of computing services to end users over the Internet. Second is the migration of business computing infrastructure to shared resources, accessed over the Internet, which can be provided within the enterprise or provisioned from third party providers.

If we look at the historical development of the computing and communications resources available to consumers in just my lifetime, the starting point is a household with one hard line telephone connection provided by a large United States based telephone company. Broadcast television was delivered free through the airwaves with no user interaction, thus providing no investigative usefulness. Mail was delivered to a home address or Post Office box by the United States Postal Service. Business was often conducted face-to-face or over the telephone and business records were in paper form. The sources of information available to a law enforcement investigator were limited, but all shared a powerful nexus to a local address or individual.

This situation advanced with the availability of personal computers, which allowed for the creation and storage of digital documents in the home and office, cellular telephones, which allowed users to combine mobility with communications, and the Internet, which allowed for the connection of these devices, and ultimately led to the convergence of technologies we are faced with today.

The connected consumer of today can be accessing and storing information over the Internet using many devices, home and work computers, one or more smartphones or other devices connected to multiple wireless providers, GPS units, game consoles, e-readers, and even vehicles. The consumer can be communicating with thousands of people using social networking sites, multiple e-mail, messaging and Internet telephone accounts, and identities available from hundreds of possible providers, while also transacting business with thousands of companies from around the world. Documents and

packages related to these transactions are delivered from a variety of global and regional shipping companies.

Criminals have adopted every piece of this technology and used it to improve their ability to commit crimes, or to victimize individuals and businesses worldwide with no regard for borders, laws and jurisdiction. This can make investigations involving the Internet daunting for the majority of police officers and extremely challenging even for highly trained investigators with access to advanced tools and equipment.

One example is the theft of online banking credentials where highly organized groups are using very sophisticated attacks to compromise legitimate Internet sites, infect the computing devices we rely on, obtain legitimate access credentials, and steal millions of dollars from consumers, small to medium sized businesses, local governments and school districts. These thefts can be devastating to the victim and direct countless energy and resources away from productive activity. Banking regulators estimate that more money is being stolen in online thefts than through traditional bank robberies.

In the State of New York there are nearly 20 million people. Citizens and businesses expect that when they call the New York State Police or one of over 500 local police agencies because they are a victim of crime, that their case can be investigated. The investigations cover every possible crime. A person is kidnapped, a child is missing or being exploited, a homicide suspect is at large, an identity is stolen, a bank account is compromised, a company website is shut down by denial of service, or a sophisticated attacker steals corporate secrets or attacks our critical infrastructure. When the perpetrator of this crime is not readily known, law enforcement must develop sources of information to begin the process of identifying suspects. When the crime involves the use of devices connected to the Internet, one of the primary sources of information are business records maintained by private sector entities, from a one person, home based business, to a multinational corporation.

In New York State, law enforcement does not have administrative subpoena power. Requests for subpoenas must first be reviewed by the District Attorney and then presented to a Grand Jury. Each County has its own procedure and criteria for requesting and obtaining subpoenas, and in some jurisdictions they can be difficult to obtain, especially for investigations involving non-felony offenses. This can lead to a situation which forces police officers to triage the number of requests for subpoenas resulting in crimes that go uninvestigated or under investigated.

Time is our enemy in Internet investigations, records and communications may not be retained, or information may intentionally or accidently be deleted or corrupted. Technology has created many new sources of information that may be accessed by law enforcement, equalized by the very number of private sector entities that must be contacted to build information during an investigation.

The advances of Cloud Computing present even more challenges for law enforcement. I would like to highlight the impact of a few technologies:

- Encryption – Companies are using advanced encryption technology to secure data that is transmitted across the Internet. This may create situations where law enforcement does not have the technological means to access communications, regardless of the legal authority to do so. The recent concerns in many countries about the encryption implemented on Blackberry devices demonstrates this problem.

- Virtualization – We are rapidly moving to an environment where software applications run on virtual computers and servers that can instantly be deleted and restarted with a fresh environment, removing traces of data that law enforcement has been able to access during the forensic examination of a seized computer. These virtual environments can be operated outside of the United States.

- Data Storage – With the evolution of Cloud Computing services, the storage locations for data are moving from our personal and business computers to locations on the Internet accessed by multiple devices. Locations in the United States will often be out of the jurisdiction of State and Local law enforcement. Data will also be stored outside of this country and not only in jurisdictions that have a friendly relationship with the United States. This is already creating challenges for large enterprises with business data stored in multiple countries with differing privacy rules.

- Apps – Applications in the Cloud can be accessed from anywhere, and data can be imported from one storage location, processed, and returned to the original location. An example would be photos taken with a smartphone from one manufacturer, uploaded to a storage service maintained by an online service, processed with software by a different online service, and forwarded using one or more communication services.

The combination of Cloud Computing technologies described here could create an environment where entire segments of business activity could be conducted outside of the reach of law enforcement. The effect of capabilities employed on television and in the movies may cause a misconception of the ability of law enforcement to access information on the Internet. At the New York State Police, we cannot sit at our computer and access the extensive data about individuals and their transactions with companies on the Internet. There is no database that lets me choose an individual and identify all of the e-mail, messaging, and social networking accounts that they use. I cannot access the subscriber information for all Internet based telephone accounts like we have done in the past with telephone subscriber directories.

I would like to close with an example from a recent case in New York State. While investigating a business and executing a search at the business location, it was discovered that there were no financial records about the business stored on site. All records were stored and processed on offshore servers which were accessed from the business, and the accountants for the business accessed a limited number of records from

a different location to prepare tax returns. This is just one example of how the technological advances and jurisdictional issues created by Cloud Computing may already be negating the fact that there are new sources of transactional records being maintained by companies operating on the Internet, especially in the case of State and Local law enforcement.

Thank-you again for the opportunity for the New York State Police to provide testimony before the Subcommittee.

Mr. NADLER. Thank you.

Mr. Schmid, you are recognized.

TESTIMONY OF KURT F. SCHMID, EXECUTIVE DIRECTOR, CHICAGO HIGH INTENSITY DRUG TRAFFICKING AREA PROGRAM

Mr. SCHMID. Thank you, Mr. Chairman and Representative Franks.

I appear to you as a law enforcement official with over 40 years of experience, and many of those 40 years dealing with ever-evolving communication and computer technologies and the attendant challenge to preserve law enforcement's lawfully-authorized electronic surveillance capability while maintaining the privacy rights of individuals and sustaining industry's ability to keep pace in a fiercely competitive market. Preserving those intercept capabilities for law enforcement while reforming and aligning the ECPA to address new and emerging communication technologies are the primary themes of my testimony today.

And, Mr. Chairman, if you would convey to Representative Conyers that, like Representative Conyers, I was also here in 1986 in my similar capacity.

The face of crime today—many aspects of the traditional criminal landscape have changed significantly as a direct result of new technology. Law enforcement embraces new and innovative technologies, the entrepreneurial opportunities they present, and all of the other positive impacts these technologies have on our society today.

However, law enforcement must be vigilant in how the criminal exploits them to harm others. Many criminals have exploited new technologies in ways not previously anticipated. As an example, more traditional crimes like prostitution, street corner drug trafficking activity, laundering and moving illicit proceeds, just to name a few, have taken on an entirely new dimension using networked technologies and offers the criminal a cloak of invisibility from traditional public or law enforcement observation and detection.

Criminals have created entirely new, more effective ways to operate their illicit enterprises. Examples include using social networking applications as an instant communication tool to coordinate and conduct violent gang operations and attacks, a recruiting tool that can enlist and indoctrinate criminal cohorts from around the world, or an effective training platform to teach ways to avoid detection. Crimes like identity theft, human trafficking, child exploitation, among others, have taken on a global aspect as a result of access to these powerful technologies.

As more and more users migrate from desktops and laptops to the now ubiquitous and powerful smartphone to conduct their computing and communication functions traditional data retention guidelines under ECPA no longer apply to providers of these services. These data retention gaps have often manifested themselves as an end of a trail of electronic evidence in many major criminal investigations.

Simply stated, law enforcement must preserve its ability to conduct lawfully-authorized electronic surveillance and must have rea-

sonable and expeditious access to stored information that may constitute evidence of a crime committed or about to be committed regardless of the technology platform on which it resides or is transferred. Retention of this information by service providers is of paramount importance to law enforcement, also.

The law enforcement community has repeatedly learned that the criminal quickly adapts new technologies to his repertoire of tools not only to enhance his illicit activities, but also to create—and we hope only a temporary—safe haven in which to operate. Law enforcement, generally lagging the technological capability and/or the legal precedent to intercept or access communication and data, must deal with these difficult situations for sometimes long periods of time before solutions are found. Opportunities to sit at the table with industry, privacy advocates, and lawmakers prior to major technology rollouts are crucial to preventing sometimes years of unintended consequences.

The rollout and subsequent activity facilitated by Congress enacting the Communications Assistance for Law Enforcement Act, or CALEA, in 1994 defined statutory obligations telecom carriers had to implement to help law enforcement preserve its ability to conduct lawful electronic surveillance. This action was taken by Congress to preserve the public safety.

As challenging as it has been, CALEA also created the opportunity for law enforcement to sit at the table with industry and develop standards by which law enforcement requirements can be addressed. Absent CALEA, law enforcement's ability to conduct lawful intercepts would have been significantly diminished or even eliminated.

A similar approach addressing cloud computing and other emerging technologies seems reasonable and necessary in reforming ECPA. Law enforcement's preference to preserving its ability to access relevant electronic data to detect, prevent, and solve crime is to sit at the table with lawmakers, privacy groups, industry, and others to articulate its concerns and requirements. Such a process will more likely result in effective legislation that balances privacy and public safety and sustains a reasonably equitable and level playing field for industry.

If no action is taken to reform ECPA other less desirable outcomes, namely awaiting a court's decision, sometimes promulgated by officials not sufficiently steeped in relevant technology, law enforcement operational or other privacy issues may determine how we deal with these complex issues. This type of undesirable outcome can lead to long periods of having to comply with flawed case law.

In summary, law enforcement is constantly striving to preserve, not extend, its lawfully-authorized electronic surveillance and digital data access authority. A very important component of that preservation involves retaining, not relinquishing, established thresholds when subpoenas and search warrants are appropriate. Subpoenas assist law enforcement to focus on investigative targets, frequently serving as a tool to eliminate innocent persons from being investigated while serving to develop additional leads and evidence on the offender in question.

Our Nation's citizens demand that law enforcement connect the dots to detect, prevent, and retrospectively investigate crime. Subpoena authority assists law enforcement to collect those dots.

We live in a rapidly changing and dangerous world. Any erosion of law enforcement's lawful access to digital information while criminals are continuing to empower themselves with these technologies of unprecedented capability create a perilous dilemma.

State and local law enforcement agencies, unlike government agencies with abundant resources, are particularly susceptible to and challenged by criminals exploiting emerging communication technologies. A tragic but all too common—almost daily—example of this susceptibility is a violent crime, such as a homicide, committed in a local jurisdiction. A cellular smartphone is often the key to solving the crime.

Quick access to data related to that phone often determines whether or not the offender is captured before he commits other egregious criminal acts. Lawful access to digital communication media and sufficient retention of those data by service providers are critical to state and local law enforcement's daily investigative efforts and must be preserved.

Thank you for the opportunity to appear before you today. I applaud your efforts to address this very important issue. Thank you.

[The prepared statement of Mr. Schmid follows:]

PREPARED STATEMENT OF KURT F. SCHMID

TESTIMONY

of

Kurt F. Schmid

Executive Director,

Chicago High Intensity Drug Trafficking Area (HIDTA)

on

ECPA Reform and the Revolution in Cloud Computing

Before the

Subcommittee on the Constitution, Civil Rights and Civil Liberties

Thursday, September 23, 2010

Mr. Chairman and Members of the Subcommittee on the Constitution, Civil Rights and Civil Liberties, my name is Kurt F. Schmid and I am the Executive Director of the Chicago High Intensity Drug Trafficking Area (HIDTA) Program in Chicago, IL. The HIDTA Program enhances and coordinates drug control efforts among local, State and Federal law enforcement agencies. The Program provides participating agencies with technology, equipment, coordination and other resources to combat drug trafficking and its harmful consequences in critical regions of the country[1].

I appear as an individual not representing any particular law enforcement agency or entity, but as a law enforcement official with over 40 years of experience, many of those 40 years dealing with ever-evolving communication and computer technologies and the attendant challenges to *preserve* law enforcement's lawfully-authorized electronic surveillance capability while maintaining the privacy rights of individuals and sustaining Industry's ability to keep pace in a fiercely competitive market(s).

The Face of Crime

Many aspects of the traditional criminal landscape have changed significantly as a direct result of new technology. *While law enforcement embraces new and innovative technologies and their positive impact on our society,* we must also be vigilant in how the criminal exploits them to harm others.

Modern communication tools integrated with Internet services has propelled individuals and businesses well into the 21st century. Correspondingly, many criminals have exploited new technologies in ways not previously anticipated. As an example, more traditional crimes like prostitution, street-corner drug trafficking activity, laundering and moving illicit proceeds, just to name a few, have taken on an entirely new dimension using networked technologies, and offers the criminal a "cloak of invisibility" from traditional public or law enforcement observation and detection.

[1] Office of National Drug Control Policy, HIDTA Program Policy and Budget Guidance, 2009

Further exploitation by criminals has created entirely new, more effective ways to operate criminal enterprises. Examples include using social networking applications as an instant communication tool to conduct gang operations, a recruiting tool that can enlist and indoctrinate criminal cohorts from around the world, or a training platform to teach effective ways to avoid detection. Crimes like identity theft, human trafficking, child exploitation, moving large amounts of ill-gotten capital, among others, have taken on a global aspect.

Diminishing risk of physical harm and more difficult detection also has many criminals migrating to the most elaborate of communication applications. Tendencies to communicate via text messaging and/or e-mail, especially by the upcoming generation (criminal element), has caused a sea change in how law enforcement conducts lawful intercepts and/or accesses (stored) digital evidence. As more users migrate from desktops and laptops to the now ubiquitous and powerful 'smartphones' to conduct their computing and communication functions, traditional data retention guidelines under ECPA do not apply. This data retention gap has manifested itself as the end of a trail of electronic evidence in major criminal investigations.

Cloud Computing

Cloud computing may be the next significant evolution of the Internet in the flexibility and robust nature of services the cloud(s) will offer its users. While the nature and power of these services and the platform upon which they come are unprecedented, preserving law enforcement's ability to lawfully access information related to criminal activity that happen to reside in the cloud(s) or other yet unknown media is not. New and emerging technologies should not, by their unique and secure nature alone, determine law enforcement's lawfully-authorized access to digital information residing in or transiting a particular medium.

Law Enforcement's Requirements & Perspective

Simply stated, law enforcement must preserve its ability to conduct lawfully-authorized electronic surveillance and must have

reasonably expeditious access to stored information that may constitute evidence of a crime committed or about to be committed regardless of the technology platform on which it resides or is transferred. Service providers must retain these records for a reasonable time set forth by statute or regulation. Without these Constitutionally-tested authorities, the safety of the public is put at significant risk. Balancing privacy with public safety in these challenging times, more than ever, requires collaboration and cooperation among law enforcement, privacy advocates and industry.

Lessons Learned

The law enforcement community has repeatedly learned that the criminal quickly adapts new technologies to his repertoire of tools not only to enhance his illicit activities, but also to create a (temporary) safe haven in which to operate. Law enforcement, generally lagging the technological capability and/or the legal precedent to intercept/access the communication/data, must deal with these difficult situations for sometimes long periods before solutions are found. Opportunities to sit at the table with industry, privacy advocates and lawmakers prior to major technology rollouts are crucial to preventing sometimes *years of unintended consequences.*

The rollout and subsequent activity facilitated by Congress enacting the Communications Assistance for Law Enforcement Act (CALEA) in 1994 defined statutory obligations telecom carriers had to implement to help law enforcement preserve its ability to conduct lawful electronic surveillance. This action was taken by Congress to preserve public safety. As challenging as it has been, CALEA also created the opportunity for law enforcement to sit at the table with industry and develop standards by which law enforcement's requirements can be addressed, thus helping preserve public safety. Absent CALEA, law enforcement's ability to conduct lawful intercepts would have been significantly diminished or even eliminated.

A similar approach addressing cloud computing and other emerging technologies seems reasonable and necessary in

reforming ECPA. Law enforcement's preference to preserving its ability to access relevant electronic/digital data to detect, prevent and solve crime is to sit at the table with lawmakers, privacy groups, industry and others to articulate its requirements and concerns. Such a process will more likely result in effective legislation that balances privacy and public safety and sustains a reasonably equitable and level playing field for Industry. If no action is taken to reform ECPA, other less desirable outcomes, namely awaiting a Court's decision sometimes promulgated by officials not sufficiently steeped in relevant technological, law enforcement operational and/or privacy issues may determine how we deal with these complex issues. This type of undesirable outcome can lead to long periods of having to comply with flawed case law.

Summary

Law enforcement is constantly striving to preserve, *not expand* its lawfully-authorized electronic surveillance and digital data access authority. A very important component of that preservation involves retaining, *not relinquishing,* established thresholds when subpoenas and search warrants are appropriate. Subpoenas assist law enforcement to focus on investigative targets, frequently serving as a tool to eliminate innocent persons from being investigated while serving to develop additional leads and evidence on the offender in question. Our nation's citizens demand that law enforcement "connect the dots" to detect, prevent or retrospectively investigate crime; subpoena authority assists law enforcement to *collect* the relevant dots; the process necessary prior to connecting them.

We live in a rapidly changing and dangerous world. Any erosion of law enforcement's lawful access to digital information while criminals are continually empowering themselves with technologies of unprecedented capabilities creates a perilous and paradoxical dilemma.

State and local law enforcement agencies, unlike Government agencies with abundant resources, are particularly susceptible to and challenged by criminals exploiting emerging communication technologies. A tragic but all too common example of this

susceptibility is a violent crime such as a homicide committed in a local jurisdiction – a cellular phone is often the key to solving the crime. Quick access to data related to that phone often determines whether or not the offender is captured before he commits other egregious criminal acts. Lawful access to digital communication media and sufficient retention of those data by service providers are critical to State and local law enforcement's daily investigative efforts and must be preserved.

Applying the ECPA to some of today's technologies has ranged from difficult to impractical. Any reform of the ECPA should address new and emerging technologies without unduly hampering or constraining law enforcement in its mission to protect the public.

Mr. NADLER. Thank you.

And Mr. Zwillinger is now recognized.

TESTIMONY OF MARC J. ZWILLINGER, ZWILLINGER GENETSKI, LLP

Mr. ZWILLINGER. Thank you. Thank you, Chairman Nadler.

I am pleased to be back before this Subcommittee to discuss ECPA reform and cloud computing. As you know, I have worked with ECPA for over 13 years, both as a former DOJ attorney who has taught prosecutors how to apply the law, and now as outside counsel for Internet service providers.

Today I want to focus on three ways in which ECPA no longer strikes the right balance between law enforcement interests and user privacy when it comes to data stored in the cloud. First, e-mails and other private messages lack adequate protection under the law; second, the standard for law enforcement access to stored files like documents and photos is too low; third, ECPA's failure to address civil litigant and criminal defendant access at all generates confusion and needless litigation.

To elaborate on my first point, e-mails are not fully protected because ECPA does not state clearly enough that a search warrant is required to obtain all types of stored e-mails, and it does not protect e-mails regardless of age. In fact, ECPA's protections run counter to user expectations.

If you are a typical e-mail user, the messages that are most likely to be important to you and private are the ones that you have already read and decided to save. Those e-mails might include notes from a friend, communications with a health care provider, or intimate messages from a spouse.

By contrast, the unopened messages in your inbox may be spam, or ads, or automatically-generated confirmations that you will delete without ever reading. Unfortunately, the unimportant and unopened messages may be more protected than the important ones.

Under ECPA the government needs a search warrant to access messages in electronic storage for 180 days or less. But electronic storage is defined as temporary, intermediate storage incidental to transmission and the storage of such message for backup protection.

When ECPA was passed, ISPs stored user e-mails only until the user logged in and downloaded their mail. That storage was, indeed, temporary and intermediate. After the user downloaded the messages the ISP generally kept nothing.

Now services like Yahoo mail and Gmail and social networks retain messages until they are deleted by the user. If users don't download their messages when does temporary and intermediate storage end?

DOJ believes that temporary storage ends the moment a message becomes marked as "read," even if it was only briefly skimmed on a mobile device. That interpretation of ECPA is arbitrary, as nothing magical happens when a user reads a Web mail message. It stays exactly where it has been since it was received—on a server in the cloud. In fact, a message can be marked as "read" or "unread" regardless of whether the user actually looked at it.

Federal statutory protection for e-mails cannot really depend on how a user chooses to mark their mail. This ambiguity about the protections for e-mails stored in the cloud needs to be clarified.

An additional way in which ECPA fails to properly protect e-mail is the 180-day rule. This statutory rule was based on the fact that in 1986 e-mails were only stored briefly by the ISP and any material it had after 6 months was likely to have been abandoned by a user. This assumption, which is described in the legislative history, has proven incorrect and it is time to get rid of that restriction.

As to my second point, ECPA also underprotects stored files, like photos or documents. Here the unilateral delayed notice provisions are the culprit, making it too easy for the government to obtain private content without user notice or judicial oversight.

In fact, the government can get the content of such files more easily than it can get transactional or other subscriber records. Allow me two examples: If the government wants a list of e-mail addresses with whom a user has communicated, it must apply for a court order and it must show specific facts that demonstrate the information is material to a criminal case. Similarly, any data besides basic subscriber information, such as a user's gender or birth date, also requires a court order.

But if a user stores a private journal in a password-protected file online the government can get that private journal with a mere subpoena and no notice to the user if it believes that providing such notice might interfere with a criminal case. If the same user kept the same journal on his laptop, law enforcement would need a search warrant to get it or it would have to serve the user directly with a subpoena so that he could object.

So the government can get a user's private journal from an ISP with a subpoena without judicial review or notice but needs a judge's blessing to learn the user's gender or birth date. That does not strike the right balance between privacy and law enforcement needs.

In revising ECPA Congress should make clear that a subpoena with delayed notice is not enough to access private content stored online. Instead, the government should be required to show a magistrate that there is probable cause to believe a crime has been committed and that the user's account contains evidence of that crime.

Finally, I want to briefly comment on ECPA's silence regarding access by civil litigants and criminal defendants. ECPA prohibits ISPs from disclosing the contents of communications to anyone other than the government.

Often civil parties and criminal defendants are surprised by this and file motions to compel production that are misguided but costly. And while some courts have confirmed the absence of civil discovery provisions in ECPA, other judges do not initially recognize that such a prohibition exist because it is not mentioned in the statute specifically.

This gets more complicated if a criminal defendant cannot get access to files that he believes are exculpatory and key to his defense. Some trial courts have ruled that the restrictions in ECPA are unconstitutional to the extent they interfere with a defendant's right

to due process. An amended ECPA should clarify the general prohibition on disclosure but create exceptions in narrow circumstances with prior judicial review.

In conclusion, changes in technology and user behavior have altered the way ECPA works in practice and the time is right for a revision that restores the prior balance between law enforcement needs and user privacy to reflect the uses of the Internet in the 21st century.

Thank you for the opportunity to testify today.

[The prepared statement of Mr. Zwillinger follows:]

PREPARED STATEMENT OF MARC J. ZWILLINGER

Written Statement of Marc J. Zwillinger

Partner

Zwillinger Genetski LLP

U.S. House of Representatives Committee on the Judiciary

Subcommittee on the Constitution, Civil Rights, and Civil Liberties

Hearing on

ECPA Reform and the Revolution in Cloud Computing

Washington, D.C.

September 23, 2010

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

Thank you for having me back to testify about ECPA reform and specifically about the issues relating to cloud computing, which make up a large component of my legal practice. As the committee knows, I worked as a Trial Attorney in the United States Department of Justice Computer Crime and Intellectual Property Section from 1997-2000, and for the last ten years I have been representing companies, including internet service providers, social networking companies, and wireless providers on issues related to the Electronic Communications Privacy Act ("ECPA"). In my career, I have taught hundreds of law enforcement agents how to apply ECPA and hundreds of compliance paralegals at leading Internet providers how to respond to law enforcement requests for data. I have also litigated ECPA-related issues in federal district and appellate courts. As an adjunct professor at the Georgetown University Law Center in Washington, D.C., I have taught courses covering ECPA. I have also been involved in the Digital Due Process Coalition effort for the last 2 years. I am testifying today solely in my individual capacity and not on behalf of any clients or the Digital Due Process Coalition.

As someone who deals with the real world application of ECPA on a daily basis, I am acutely aware of the strengths and the failings of the statute. Although each of the proposed areas for ECPA reform are important, the most pressing area for legislative action relates to the storage of user data with third party Internet providers, often referred to as storage "in the cloud."

As the testimony from industry representatives will likely make clear, Internet companies are struggling to apply the existing and somewhat outdated categories of information protected by ECPA to their products and services. Back in 1986 when ECPA was passed, companies may have been outsourcing the processing of certain data, but not on the same scale as today. Moreover, individuals were not using third-party services like Yahoo! Mail, Google Documents, or Flickr to store their most private correspondence, writings and photos, nor were they communicating regularly through social networking services. The increasing use of the Internet as a primary repository for users' private documents has made the issue of privacy and law enforcement access to such materials of significant importance to individuals who use the services, companies that offer the services, and to law enforcement. Given the widespread use of cloud computing by U.S. citizens and businesses, the laws governing access to user data should be clear and easy to apply. The Stored Communications Act ("SCA") is exactly the opposite. In fact, the distinctions and categorizations contained in the 1986 statute often make little or no sense in today's environment. Through my testimony, I intend to explain five fundamental problems with how the SCA applies to cloud computing and why this Committee should consider passing new legislation to address these issues.[1]

[1] Four of the five issues are addressed in the Digital Due Process ("DDP") principles. The issue that is not addressed pertains to access to communications by non-government actors, such as civil litigants and criminal defendants.

1. For materials such as emails or private messages that are intended to be the most protected, the definition of "Electronic Storage" is difficult to apply.

Take a moment to consider the types of emails that are in your own inboxes. If you are a typical email user, the emails or private messages that are both the most important and the most private are the older messages that you have read through several times and have intentionally decided to save. These emails might include treasured notes from a spouse, a child, or a close friend. By contrast, the unopened emails in your inbox are likely to be commercial solicitations that you have not yet had time to delete. Unfortunately, under the current structure and interpretation of the Stored Communications Act ("SCA"), the latter messages are clearly protected from government access except when law enforcement obtains a search warrant. The protection for the more important messages – the ones you purposely chose to save – however, is much less certain or is insufficient. Let me explain why.

The SCA affords the highest protection to materials that are in "electronic storage" for 180 days or less by preventing the government from accessing these types of communications without a search warrant. The SCA defines "electronic storage" as "(A) any temporary intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. . . . " 18 U.S.C. § 2510(17). Email communications meeting either condition (A) or (B) and that are less than 181 days old are protected from disclosure to anyone except to the government pursuant to a search warrant.

Under this definition of "electronic storage," the Department of Justice has taken the position that a search warrant is required only for messages that have never been read or opened by a user. This argument is based on the theory that when an email has been downloaded to a user's computer, the storage by the ISP is no longer temporary or intermediate, because a copy of the message has been delivered to the user.

When the SCA was passed in 1986, this type of distinction may have made some sense. In the 1980s, ISPs would store user email on their systems only briefly until the user connected to the ISP and downloaded the mail. That brief storage was temporary and intermediate, as described in the definition of electronic storage. Today, however, webmail is the predominant form of personal email communication and webmail is seldom delivered to a user for local storage on his or her own PC.[2] Rather, it stays in the cloud and the user interacts with the mail on the provider's servers. The ability to access webmail from mobile devices and portable computers is one of the chief advantages of webmail and is one reason why webmail has come to dominate the non-business user email market. But for webmail providers, there is no longer any "temporary intermediate" storage in the manner initially contemplated by the statute. Rather, whether or not a user reads an email, it will continue to be stored in the cloud forever—or at least so long as the user's account is active. Thus, the act of "reading" the email is of no legal moment, because it does not transform the storage from "temporary" to

[2] If webmail resides on a user's computer at all, it is in a temporary web-browsing cache.

permanent. Nor does the user's action or inaction have any impact on the physical location of the email – it remains on the provider's servers and is not downloaded to a computer that is within the realm of what is covered by the user's Fourth Amendment rights.

Over DOJ's objection, the Court of Appeals for the Ninth Circuit extended the definition of electronic storage to all emails stored by an ISP – whether read or unread – under the theory that even after any "temporary" period of storage has ended, any further storage by the ISP is within the backup prong of the definition of electronic storage because it is a "backup" for the user.[3] This is the correct outcome as a policy matter – the statutory protections for email should not vary depending on whether the email has been delivered or read, yet, the Department of Justice takes issue with this position and continues to seek to compel the production of opened mail by subpoena in all judicial districts except the Ninth Circuit.[4] In fact, earlier this year I was poised to litigate this issue against the U.S. Attorney's office in Colorado after it moved to compel Yahoo! to respond to a subpoena for emails that were less than 180 days old but which the user had not read. After Yahoo! filed its opposition to the motion to compel and amicus briefs had been submitted supporting Yahoo!'s position, the government withdrew its motion.

Lest any future courts accept the Department's position, the SCA should be amended to remove any question that the standard the government has to meet in order to access email is not dependent on whether the email is opened or unopened.

2. The 180 day rule is arbitrary and based on a false assumption

Like the purported distinction between opened and unopened mail, the provision in ECPA that automatically diminishes a user's protection vis-a-vis the government as email ages is arbitrary and irrational. Under the SCA, private messages or emails 180 days or older may be obtained by the government with a mere subpoena or a § 2703(d) order with prior notice, unless such notice is authorized to be delayed. However, law enforcement must obtain a warrant to obtain emails stored with a provider for 180 days or less. This may have made sense in 1986, but it is no longer rational, much less compelling.

At the time ECPA was passed in 1986, data sent through an electronic communication system was not stored by the provider for long periods of time.[5] Thus, if not already deleted by the ISP, any data stored for more than 180 days was not deemed to be the type of data worth protecting. Emails over 180 days old were likely unread emails that no user had bothered to retrieve and download to their own computer – probably most often associated

---

[3] *See Theofel v. Forey-Jones*, 341 F.3d 978 (9th Cir. 2003).

[4] *See* U.S. Dept. of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence Manual*, Chap. 3, a 2009 edition, found at www.cybercrime.gov/ssmanual/03ssma.htm); *United States v. Weaver*, 636 F. Supp. 2d 769, 772-73 (C.D. Ill. 2009). The government also believes that the "backup protection" reference in the statute refers only to backups created by the mail provider.

[5] *See* H.R. Rep. No. 99-647 at 65 ("Most—if not all—electronic communication systems (such as electronic mail systems), however, only keep copies for a few months.")

with dormant or abandoned accounts. In fact, it was expressly assumed that storage of that duration would make the private email more akin to a business record of the ISP than content belonging to the user.[6] The intervening years, however, have proven that the original assumption was incorrect. Online storage services for all types of communications, including music, files, photos, and emails, have become the rule and storage capacity in the cloud is virtually unlimited with little or no financial cost to the user. Thus, a user who stores online content for more than 180 days, is now more, not less, likely to have a strong interest in that data, and no one would consider such data to be merely a business record of the ISP. Yet the Stored Communications Act still contains the original arbitrary six month dividing line for privacy protection such that even materials that are obtainable only through a search warrant for the first 180 days of their existence become obtainable via a subpoena (with prior or delayed notice) on the 181st day. This is true despite the fact that it remains a criminal offense for a third party to hack into an email system and obtain access to the same message regardless of its age.[7] This arbitrary time limit on privacy should be eliminated.

3. Congress intended content to be more protected than transactional records in theory, but in practice content does not get enough protection.

Lawyers who work regularly with ECPA generally describe the statute as providing greater protection for content, like photos, than for transactional or subscriber records, like log files. This can be clearly seen by the fact that the highest level of protection under the SCA is reserved for the contents of communications in electronic storage and the lowest for certain limited types of basic subscriber records that are identified in 18 U.S.C. § 2703(c)(2), which consist of: name, address, telephone records, length and type of service, other subscriber number or identity including any network address, and means and source of payment.

Of the two other categories in the SCA, the protection for the contents of communications stored by a remote computing service was intended to be at least as robust, if not more, than the protection provided to transactional records. This is not, however, the way ECPA works in practice. When Congress passed ECPA, it expected that the means by which the government would get access to the types of private content not deemed to be "in electronic storage" – such as files stored with a remote computing service – was through a court order under 18 U.S.C. § 2703(d) or a subpoena with prior notice to the user. With such prior notice, a user would know of the request for his or her documents and would have the opportunity for prior judicial review before the contents of the account were turned over – either by the court who initially issued the order, or subsequently if the user challenged the request. The delayed notice provisions of 18 U.S.C. § 2705 were intended to be used sparingly, as the requirement of prior notice to the subscriber was identified as an important statutory protection provided to

[6] *See id.,* ("To the extent that the record is kept beyond that point it is closer to a regular business record maintained by a third party and, therefore, deserving of a different standard of protection.")

[7] *See* 18 U.S.C. § 2701.

the user.[8] By contrast, when requesting transactional data or subscriber data not specifically listed in § 2703(c)(2), the government was not required to give user notice, even though the same basic showing was required.

But, in modern law enforcement practice, it often works the opposite way – transactional data receives more protection than the contents of files stored by a remote computing service. By regularly relying on the exception in the SCA that allows it to delay notice to the subscriber whenever there is a "written certification of a supervisory official" that providing notice would have an adverse effect on the investigation, the government can obtain contents of stored files with a subpoena, when transactional records require a court order under § 2703(d). And users whose content is sought by subpoena have no opportunity to challenge the request before production. As a result, contents of files and messages – except those that are in electronic storage for 180 days or less – are easier to obtain than transactional records. This switch in protection from the way ECPA was originally designed is significant in light of the vast amount of user data that is currently stored in the cloud.

In revisiting ECPA, Congress should make clear that a subpoena with delayed notice is not an acceptable way to access the contents of any private stored content belonging to a user by requiring the government instead to demonstrate probable cause before gaining access to such content.[9]

4. The SCA is not technology neutral

One reason why the standard for law enforcement access for private stored content should be reevaluated is to make the SCA truly technology neutral. When choosing between storing documents locally on an individual's own PC, or using a password-protected storage service in the cloud, the key considerations should relate to efficiency, accessibility, security and cost, not law enforcement's ability to access the data from a third party. That is not the situation today. The SCA pushes a personal or business user seeking to protect his or her data from access by third-parties, including the government, towards choosing a local storage option to maximize the protection for the data. If a business owner stores confidential files on a local server, the government must either execute a search warrant or serve a subpoena for the documents, allowing the personal or business user who receives the subpoena to have an opportunity to object to the subpoena or assert relevant privileges. By contrast, if those same files are stored with a third-party provider in the cloud, the government could serve a lesser form of process on the provider with delayed notice and prevent the business owner from learning the documents had been subpoenaed until after they had already been provided to the government.

---

[8] See H.R. Rep. No. 99-647 at 68 ("[T]he purpose of such notice is to provide the subscriber or customer with an opportunity to contest the propriety of such a disclosure.")

[9] One district court has already held that SCA violates the Fourth Amendment by permitting the seizure of emails without a warrant and without prior notice to the subscriber on less than a showing of probable cause. *Warshak v. U.S.*, No. 1:06-CV-357, 2006 WL 5230332 (S.D. Ohio July 21, 2006), *vacated in part on other grounds*, 532 F.3d 521 (6th Cir. 2008).

The purported justification for decreased privacy protection where the documents are hosted in the cloud is the third-party doctrine: that documents that a user has knowingly shared with a third-party are understood to be less private. But that assumption is flawed in several respects. First, as a practical matter, documents stored in the cloud may be more secure than documents stored on a local server. For example, third-party technology providers generally spend more time and resources securing data than the average user does on his or her home PC where they may be unprotected from intrusion or secured only by a firewall that the user is not particularly adept at configuring, without an intrusion detection system or 24 hour monitoring. Second, by storing data on password-protected third party systems, users are not generally providing the third party with any broad right to review, access or disclose the data for its own purposes. In fact, the third-party generally has limited rights to automatically screen data for harmful or malicious content that may cause damage to their network, and no rights to access the private files. Thus, users should not be considered to have waived the confidentiality of private documents by hosting them in the cloud. In fact they may be enhancing their confidentiality compared to storing them on a home PC where other household members could view them when using the computer. Consequently, as a policy matter, there is no legitimate reason for U.S. law to provide more robust privacy protections for users who elect local storage over secure storage in the cloud.[10]

5. The complete silence on access by civil litigants, criminal defendants and estates of deceased users creates uncertainty and unnecessary litigation

An often overlooked but increasingly important issue associated with the application of the SCA is access by civil litigants, criminal defendants and estates of deceased users. In the course of representing Internet service providers, I have witnessed firsthand the confusion that is the result of the absence of guidance in the SCA regarding access by civil litigants and criminal defense counsel and how frequently ISPs receive unlawful subpoenas seeking to compel production of the contents of Internet communications.

The SCA contains clear and unequivocal prohibitions on disclosure of both types of content records that may be in the possession and control of a third-party ISP: materials in "electronic storage" and "contents of wire or electronic communications in a remote computing service." There are eight specific exceptions to these prohibitions that provide specific avenues for disclosure to government entities, disclosures based on consent, or disclosures by the ISP in order to render service or forward communications. However, there is not a single provision that authorizes any type of disclosure of customer communications in response to legal process issued by a civil litigant or criminal defendant. [11]

---

[10] Certainly, there are circumstances where data stored in the cloud is made less private because it is shared with multiple users, just as data within a local work environment may also be shared with multiple users. The test, however, should be applied neutrally whether the storage is local or in the cloud.

[11] *See O'Grady v. Superiar Court*, 139 Cal. App.4th 1423 (2006); *Crispin v. Christian Audigier, Inc.*, __ F. Supp. 2d ___, 2010 WL 2293238 (May 26, 2010); *Flagg v. City of Detroit*, 252 F.R.D. 346, 366 (E.D. Mich. 2008); *Viacom Int'l v. YouTube*, 253 F.R.D. 256 (S.D.N.Y. 2008); *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606, 611-12 (E.D. Va. 2008).

When ISPs inform civil litigants and criminal defendants, as they must, that federal law precludes them from disclosing the communications without the consent of the author or recipient; they invariably meet resistance and are sometimes forced to litigate these issues. Even judges are astounded that they have not been given the power, under any circumstances, to require the production of email content by an ISP in a civil case. In recent years, the storage of increasing amounts of content in the cloud has only increased the importance of addressing these issues.

The problem is even more complicated when a criminal defendant seeks information, where this lack of access may lead to due process concerns. Because ECPA contains a flat prohibition against the disclosure of contents of communications to non-governmental entities, criminal defendants have no mechanism to obtain emails even when there is no subscriber who can consent to the disclosure. One solution is to rely on law enforcement to request the data on a criminal defendant's behalf, but in some cases, defense attorneys are unwilling to disclose their defense strategy to the government and in others, the prosecutors are unwilling to cooperate. Judges, for their part, can be reluctant based on separation of power issues to require the government to use its investigative powers at the behest of a defendant to retrieve the materials. And the third-parties who sent or received these emails may be unwilling or unable to consent to their disclosure.

For this reason, some trial courts in California have issued bench orders and oral rulings finding that the restrictions in ECPA threaten to interfere with the defendant's constitutional rights to due process and effective assistance of counsel. Furthermore, civil litigants are equally stymied by the prohibitions of the SCA. Although many problems are solved by requiring the civil party to serve their discovery subpoena on the third-party who is the account holder, rather than the ISP, there are some circumstances where the account holder is a third-party who is not within the court's jurisdiction, or is unable to access their account to obtain the emails, or is deceased. These situations often lead to litigation. I am currently involved in a case in Massachusetts where my client has been sued for a declaratory judgment to declare that the emails in a deceased user's account should be turned over as property of the estate. Even if the plaintiffs succeed in invalidating the 'no right of survivorship' clause in the contract, the ISP would be barred under ECPA from disclosing the contents of the emails, and would be forced to appeal the decision.

ECPA clearly needs an escape valve of some sort to allow for disclosure of the contents of communications or stored files in very limited and narrow circumstances. I have previously proposed the text of such an escape valve in a law review article[12] about the SCA in 2007, whereby a criminal defendant or civil litigant would be able to seek a court order to obtain

---

[12] Marc J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not A Level Playing Field*, 97 J. CRIM. L. & CRIMINOLOGY 569 (2007).

stored content after making a rigorous showing that other methods of gaining access to the data have been unsuccessful, that the information is relevant and material to the case and that the subscriber/user and the ISP have been given notice and an opportunity to be heard. I continue to believe the addition of such a provision would reduce some of the confusion and unnecessary litigation generated by the current law.

ECPA has functioned fairly well during its first 20 years in striking the right balance between law enforcement needs and the privacy expectation of U.S. citizens. But when it was initially passed in 1986, Congress recognized that the "law must advance with the technology to ensure the continued vitality of the fourth amendment."[13] Based on my experience as an ECPA practitioner for the past 13 years, I believe the time is ripe for another advancement. I hope you will consider these perspectives in crafting legislation that balances law enforcement needs and user privacy in a manner that reflects the reality of the uses of the Internet in the 21st century and no longer relies on outdated assumptions.

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

[13] . S. Rep. No. 99-541, at 5, *reprinted in* 1986 U.S.C.C.A.N. at 3559.

8

Mr. NADLER. Thank you very much.

I recognize myself first for questioning.

Professor Werbach, we are mainly concerned with balancing necessary access to data in the cloud by law enforcement with the consumer's interests and personal privacy. You said, as a number of others of our witnesses have said, that striking that balance cor-

rectly will act as a driver for growth in the cloud computing market and that not doing so would act as a deterrent to business growth.

How could either uncertainty about government access or a popular perception that such access is not adequately governed impair that market, and what recommendations do you have from your perspective as a business expert to make sure that doesn't happen?

Mr. WERBACH. Well, in terms of impairing the market, as I said in my testimony, one issue is trust, that the growth of this Internet economy, which, as I described, is not just a narrow set of services but all the sorts of developments that are happening based on this infrastructure depends on users and service providers having a sense of trust that when they put their data online that it will be protected. And anything that interferes or diminishes that trust is going to have some retarding effect.

Also, we are in a global environment here, so businesses make decisions about where they invest based on the environment. If they are going to invest in building infrastructure, and building services, and marketing, and building up customer bases here in the United States they have to feel a confidence level that the processes and procedures and protections around their data are appropriate, otherwise they may choose to make those investments somewhere else.

So at every level the degree to which access to data and protection of data is carried out is going to have some influence on the decisions that get made and on the speed and trajectory of this marketing.

Mr. NADLER. Thank you.

Professor Cate, in your testimony you described several broad categories of criticism of the Stored Communications Act. One category concerns the lack of publicly available aggregate statistics detailing the extent to which third party providers are routinely compelled to deliver customers' communications and other private data to law enforcement agencies. You indicate that because most service providers do not disclose this information Congress has no reliable data to determine the scale of requests and disclosures being made under the SCA.

Why do you think Congress should have access to this type of information? What use might Congress make of such information?

Mr. CATE. Thank you very much, Mr. Chairman. In most of the laws which Congress has enacted which provide for access by the government to private records it has required the government to file reports with Congress on either an annual or a semiannual basis saying how often do they use that authority and with what effect. So this is true of wiretaps; it is true of pen registers; it is true of trap and trace orders.

Having those statistics gives Congress a sound empirical basis on which to evaluate how its laws are being used and whether they need to be changed. It also provides that same information for people such as those of us gathered at this table when making recommendations to Congress. And it provides information to the public and the press so that they know how those laws are being used and to what effect.

But there is an additional value which I think is really quite important and should not be overlooked, and that is by making the

government agencies themselves keep those statistics, and therefore have to account internally for how they are using those, we get stronger oversight internally. So, for example, when the FBI, in reporting its use of national security letters, grossly underestimated its use of those, as pointed out by the Office of the Inspector General and the Department of Justice, it provided the Department of Justice an opportunity to go in and help build better procedures for making sure that the FBI was using its authority given to it by Congress appropriately. It is only by having that reporting requirement you see that opportunity carried out.

Mr. NADLER. Thank you.

Mr. Hurbanek, I was intrigued by one thing you said. You talked about a law enforcement investigation in which a warrant was served on a business and that warrant proved fairly useless because there was no information there; everything was stored in the cloud.

Now, I assume that if you had the warrant—or if the law enforcement agency, not you—if the law enforcement agency had the warrant for the business they could have gotten a warrant, if necessary, to look at the same information in the cloud. But would that have done any good if the cloud is stored in a virtual situation? In other words, you seem to have indicated a situation for which the issue is not whether—I mean, there has been an implicit discussion here today as to whether we should require a warrant for some of these things, but you have described a situation where whether you have a warrant seems to be irrelevant because given the warrant you can't get the information.

Mr. HURBANEK. Yes, Mr. Chairman, and that—we have evolved from where we used to drive to a business and take all of their computers out on a big truck.

Mr. NADLER. You should turn on your microphone.

Mr. HURBANEK. It is on.

Mr. NADLER. Okay. Go ahead.

Mr. HURBANEK. Okay. So we no longer drive to the business and take the records in a truck; we would go to a business and extract whatever data we had in our warrant. This is moving so now the data——

Mr. NADLER. You would go to the business and extract whatever data you had in the warrant by accessing their computers on the site?

Mr. HURBANEK. Yes.

Mr. NADLER. You wouldn't take the computer?

Mr. HURBANEK. No. We don't take boatloads of business computers very often anymore. And so now the data may be hosted by the third party in the cloud which, if in the United States, we would have access to and we could get there and secure the data.

The concern then becomes, what if the data is not in this country? And because of the business means and the opportunities around the world it is quite possible. Now, we have a lot of legitimate businesses testifying here today; those are not the only people offering places to store data.

Mr. NADLER. So if I were an illegitimate business, or if I were a business that wanted to cut some corners I would probably—and if I were thinking about it—I would store it abroad.

Mr. HURBANEK. And you see that a lot with Internet gambling and things like that. Or the recent thing with military secrets—the person who published those on the Internet specifically is doing that from certain countries, not from within the United States.

Mr. NADLER. I see. Now, assume a frequent traveler keeps his private diary online instead of at his bedside table. This user keeps it stored in the cloud so he can type diary entries when he travels so that he doesn't have to ever leave his diary in a strange hotel room; he has been doing so for several years. The account he keeps it in is password-protected and he has shared the password with nobody.

Mr. Zwillinger and others suggest that law enforcement can get access to this diary by serving a subpoena to an online service provider and certifying that providing the user with notice may cause him to destroy evidence or flee the jurisdiction. Is that true? And if so, should that be the law?

Mr. HURBANEK. That is interesting that—and the lawyers have identified all of the problems with ECPA. It is very confusing. We don't know where to begin.

In a traditional criminal investigation we would come upon the existence of a diary maybe through interview, and we might search for the diary. In the virtual world, in the cloud, if we became aware that the person kept a diary the first question we have to ask is, where?

Where might the diary be stored? How would we find it? Who has it? Does it even exist?

We can't make the barriers to even finding the mere existence of the diary so strenuous that we can't conduct our investigation. Whether or not we can access the content and obtain the diary is pretty well written.

Mr. NADLER. Mr. Schmid, do you have anything to say on that?

Mr. SCHMID. Thank you, Mr. Chairman. By example, it gets more and more complex for law enforcement. Back in 25 years ago, when—as an example, when we would conduct a lawfully-authorized court-ordered wiretap we would serve typically one order on the phone company, service provider.

Today it is not unusual for a law enforcement officer or investigation to have to serve seven, eight, nine different court orders to be able to either access or ascertain where some of these data are lying. So it becomes very, very complex. And add that to the dimension of being a foreign-owned business; that really throws us way out of the ballgame.

So it does become extraordinarily complex in just the process of how we access——

Mr. NADLER. Okay. Thank you.

My time is running short so I will ask Mr. Zwillinger one quick question.

As I have listened to your testimony today I am struck by how some of the assumptions that Congress made in 1986 about consumer and business network and how to protect consumer privacy obviously do not hold true in today's technology environment. Everybody has said the same thing.

You make the case in your testimony that, counterintuitively, non-content transactional data sometimes receives more protection

than content. Given your law enforcement background, what might the law enforcement argument be, if any, to justify continuing the legal framework whereby some types of content are more easily obtained than some types of transactional records? Any justification for that?

Mr. ZWILLINGER. Yes. You know, I don't think the Department of Justice or law enforcement disagrees conceptually that content should be more protected than non-content. I think when you shift what the law has evolved to they are going to want to defend the status quo because, as Mr. Schmid said, it is more efficient for them.

But in order——

Mr. NADLER. Excuse me—all this massive confusion is more efficient for them?

Mr. ZWILLINGER. I agree with you, Mr. Chairman. You know, I don't think it is that confusing either, because—let me give you an example.

They would probably try to defend the status quo by saying that when you store things online with a service provider, since the service provider has some right to access the data the individual has given up some of their privacy. But I don't think that is right. That is not the way the law generally works.

If I store my photos in an online album and only my wife and I have the password, and we do that so they don't get burned in a fire and we can see them wherever we go, we are not intending to give up any protection to the service provider, and the fact that a service provider could access them does not take away our privacy interests. It would be like law enforcement saying, "You have photo albums in your house but we can get them without a search warrant because when the photos were developed the person at Kodak could see the pictures, and therefore you gave up your privacy interests."

We don't think that way. We don't say there is no privacy in a phone call because the operator in 1967 could have listened in.

So I think that is what the argument would be. I think they have made that argument before. I just don't think it works well anymore.

Mr. NADLER. I see.

Thank you very much.

I now recognize the distinguished gentleman from Arizona.

Mr. FRANKS. Well, thank you, Mr. Chairman.

Professor Cate, if I could start with you and maybe give a couple of others a shot at it, what do you believe would be the one most significant change to ECPA that would clarify what you believe is not clear and what is confusing to law enforcement officials, and service providers, and courts in general? What is the one thing that we could do to bring some clarity and balance to the whole thing?

Mr. CATE. Thank you very much, Congressman. I would like to see the law move to a requirement that a warrant is required to obtain content without regard for whether the content is in an e-mail that has been opened or not and without regard for how long it has been stored so that we would draw a bright line, universally applied, to say when seeking content the same condition, whether you come to my home computer, you go to my service provider, or

you go to some recipient's computer, it would be the same legal standard in all of those settings.

Mr. FRANKS. Mr. Hurbanek, what would you say to that?

Mr. HURBANEK. I think it requires a case-by-case debate. I think our concern is mostly that the initial records can be obtained, that we—and that the Federal Government take some leadership that helps the states craft statutes that make sense for us.

I know that is a big lift, but right now it is very difficult for us to initiate investigation. It is tough to get subpoenas and it is tough to get started. So we need to look at this as to what information is material and relevant early on, and then what steps do we have to take beyond that.

Mr. FRANKS. And what would you—can you first just tell us what the term "going dark" means?

Mr. HURBANEK. Going dark? That is an FBI discussion about the fact that we are losing our ability to see what criminal enterprises are doing. Even if we had the rights to tap into the communication we technologically may not be able to see them.

Mr. FRANKS. Mr. Chairman, that almost seems like the elephant in the room here, is that regardless of the potential accessibility by law enforcement that the technology is outrunning that, and that because of the virtual capability of being able to access the cloud and then essentially disappearing without any, you know, electronic traceable data, it almost seems to me like that is going to be a real boon to the bad guys.

Mr. Hurbanek, I will go ahead and stay with you for a moment. Can you explain what is meant by storing records in the—by storing a record in the cloud and what is a private cloud? Help us understand what a private cloud is.

Mr. HURBANEK. Well, the private cloud—clearly business isn't completely ready to put all of their corporate secrets and enterprises out with a third party. That is an evolution that is taking place.

The private cloud is when a company such as Amazon, Rackspace, Microsoft—all the ones that are here—provide you with the technology within you enterprise. So the data may still be traveling over the Internet; the data may still be stored in multiple locations and accessed remotely. But you do maintain enterprise control of it.

Those will then scale to external third parties partially, and ultimately completely. Even the Federal Government is studying how to outsource to the third party.

Mr. FRANKS. Well, I want to—if I could I just want to go down and ask each one of you to just—a couple sentences at the most—to tell me, from your varying perspectives, what you believe—the same answer would be the question I asked Professor Cate—what is the one thing that you would do that you think would be most significant to protect what you consider to be the most significant issue involved here?

Professor Werbach?

Mr. WERBACH. I would agree with Professor Cate that something to remove these artificial distinctions and to recognize that today putting information on these remote servers is not fundamentally different for users than storing them locally on a computer.

Mr. FRANKS. Skip you here, Professor.

Mr. Hurbanek, would you take a shot at it?

Mr. HURBANEK. And my answer would be that whatever framework is set up it needs to be straightforward and understandable, and we need to efficiently be able to access it through whatever courts or prosecutors, and through whatever third party companies house the data.

Mr. FRANKS. And would that take with it any sort of mandate that the information be indexed in some way that would be proprietary to law enforcement to be able to access?

Mr. HURBANEK. We don't normally ask companies to index the data for us. They are indexing data and storing data for their business purposes. We just ask that if it is relevant that we can get access to it.

Mr. FRANKS. Mr. Schmid?

Mr. SCHMID. To appropriately align the statutory and regulatory aspects of a reformed ECPA to the current technology. And that involves actually bringing clarity not only to this body but also brings clarity to law enforcement. And that seems to be where a lot of the confusion and a lot of the issues that really, really prevent us from doing our job effectively have come.

Mr. FRANKS. The way things are going that might also include trying to discover a new type of physics. You know, it looks like——

Mr. ZWILLINGER. On the same question I would agree with the professor at the other end of the table. I think a probable cause requirement for content in the cloud is the one thing you could do.

And just to respond to Mr. Schmid earlier, the types of materials we are discussing were not generally in the cloud or stored online in 1986. That is, a content requirement where you have a probable cause for all content really restores the balance to where it was; this content was stored locally.

So it is not relinquishing or giving up law enforcement access and law enforcement will still have the building blocks for investigations through records—transactional records, subscriber information. But content should be protected by a warrant.

Mr. FRANKS. And there is no one on the group here that believes that having some type of warrant requirement for content specifically would severely restrict or significantly restrict law enforcement's capability to protect us? Anyone? No?

Mr. CATE. If I may, Congressman, I would just point out that the Congress, again, in ECPA put in place a very significant wiretap warrant requirement, and in the time since that has been put in place we have seen just over 40,000 wiretap orders granted and fewer than 40 denied by courts. So the argument that is often made about warrants is that it is not a new impediment; it doesn't result in the data becoming unavailable. It is a new process for getting access to the data that requires that some other person other than just the investigator be involved, play some oversight role.

Mr. FRANKS. Yes.

Mr. CATE. Thank you, sir.

Mr. FRANKS. Thank you all very much.

Thank you, Mr. Chairman.

Mr. NADLER. I thank all the witnesses. It is clear we have two problems, one of which we can address here, and that is the proper

standards, and subpoenas, and warrants, and so forth, and the other is advancing technology.

I would simply observe that that advancing technology is part of the war between offense and defense that has been going on since time immemorial and will continue to go on. And at one point offense has got the trump hand and at the other hand the defense, and that will continue going on. But we have to deal with the legal consequences of as it is now and as it will be in the reasonably foreseeable technological future.

So I want to thank all the witnesses for the helping hand you have given us today.

Without objection, all Members 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.

And again, thanking our witnesses. And with that, this hearing is adjourned.

[Whereupon, at 2:12 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 and the Revolution in Cloud Computing

September 23, 2010

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

Cloud computing is Internet-based computing. It is a general term used for an Internet-based service that remotely stores data. Descriptions of cloud computing vary, but it broadly refers to storing information or software on computer servers that can be accessed from multiple locations around the world instead of on more localized storage methods where data can only be retrieved by someone who has physical access to a local computer or hard drive. Gmail, YouTube, Flickr, Facebook, and online payroll services are examples of these Internet-based applications.

Cloud computing has become very popular because the data and applications can be accessed anywhere at any time. Moreover, cloud computing is preferable because of our access to faster broadband connections and the lower-cost of mobile devices.

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

I look forward to hearing from our witnesses today because I am concerned that the Electronic Communications Privacy Act has fallen out of step with the way that most people use computers, and the internet with regards to cloud computing.

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

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

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

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

If businesses are continuously having trouble applying ECPA and courts are issuing conflicting decisions with differing standards, regarding law enforcement access to data and communications stored in the cloud, Congress should step in and act accordingly.

I am anxious to hear from the witnesses today as I have a number of questions.

Many of us can agree that the Electronic Communications Privacy Act is outdated, so the question is how should Congress step in and reform the Act?

I am very concerned that the Electronic Communications Privacy Act, which was enacted in 1986, may be failing to protect reasonable privacy expectations of Americans in 2010. How can Congress strike the proper balance between individual privacy, business interests, and law enforcement?

In this day and age, what is the justification for a rule that lowers the protection for electronic communications because it is six months old or has been viewed by the user?

Should we revise the Act to require law enforcement authorities to demonstrate probable cause and obtain a search warrant from a judge before gaining access to electronic communications covered under the Act, regardless of whether or not it has been opened or is six months old, rather than allowing law enforcement to access data by only issuing a subpoena issued by a prosecutor?

I hope our witnesses can shed light on these questions and I yield back the balance of my time.

House Committee on the Judiciary
Subcommittee on the Constitution, Civil Rights, and Civil Liberties
Hearing on EPCA Reform and the Revolution in Cloud Computing
Responses to Questions for the Record
Richard Salgado, Law Enforcement and Security Counsel, Google Inc.
November 11, 2010

Responses to Questions from Chairman Nadler

1. What position you generally take regarding classifying services or information as Electronic Communications Storage "ECS", Remote Communications Storage "RCS" or neither. Or, if you are unable to state a specific classification for each category, please explain the challenges you face in determining whether law enforcement requests for these types of information fall under ECS or RCS and in your explanation, please use examples drawn from the list of services/information below:

A) Web Mail
B) Search
C) Names or IP addresses of users who searched for a specific phrase
D) Word processing, spreadsheets and online calendars
E) Online photo and video storage services
F) Geo-location information (historical or prospective)
G) Instant Messaging communications
H) Social networking
I) Blogs

When determining whether any particular service is an "electronic communication service," as defined in 18 U.S.C. section 2510(15), a "remote computing service" as defined in section 2510(17), or neither, we look to the statute itself, the scant case law interpreting the statute and the policy considerations described in the legislative history. Many of the services that Google offers did not exist at the time the Electronic Communications Privacy Act was enacted, and there has been little in the way of case law to provide guidance. Indeed, the few cases available often describe the difficulty and complex nature of the distinction between ECS and RCS.

The example of email should be one of the easiest of the services to categorize because, unlike the other services listed, it was contemplated in at least some form in 1986. The email example, however, illustrates the challenges that modern communications providers face in attempting to classify services and data as either ECS or RCS. More importantly, it illustrates that even if the classification was a simple matter, the rules around what legal process is required to compel the product of the contents of email remain complex and non-intuitive.

Google takes the position that Gmail is an Electronic Communication Service and that email residing in a Gmail account is always in "electronic storage", as that term is defined. See 18 U.S.C. section 2510(17); Theofel v. Farey-Jones, 359 F.3d 1066, 1075-77 (9th Cir. 2004).

The analysis for Google, however, does not end with the determination that Google holds all Gmail content

as an ECS provider. When presented with a demand from a government entity to disclose Gmail data, Google must ascertain if the legal process issued complies with the rules set out in section 2703. This requires a message-by-message determination. If an email is over 180 days old, the government entity can use one of the subpoenas types listed in section 2703(c)(2), or use an order issued under section 2703(d). In either case, the government entity must provide the user with prior notice, but the entity can delay the notice if one of the factors listed in section 2705 is satisfied. The government entity can also use a search warrant issued consistent with section 2703 to compel the production of the message , in which case no notice to the user, delayed or otherwise, is required under the statute. If the message is no older than 180 days, then the government entity must use a search warrant issued consistent with section 2703 to compel the provider to disclose the contents of the message. There is no statutory obligation for the entity to provide notice to the user.

As I described in my written testimony, the Department of Justice takes a different position -- arguing that if a user has retrieved an email, then the provider holds the email as an RCS. Under this interpretation, a government entity can use a subpoena or a court order issued under section 2703(d) to compel production of the message from the provider regardless of the age of the email. DOJ Search and Seizure Manual at 129 & 138; see also Government's Motion to Compel Compliance with 2703(d) Order, In re Application of the United States of America for an Order Pursuant to 18. U.S.C. section 2703(d), Misc. No. 09Y080-CBS (D. Colo. Mar. 9, 2010).

The other services listed in your question were largely unanticipated in 1986 when ECPA was passed, and determining whether a particular piece of information held by Google for any one of those services is held as an ECS or RCS is no trivial task. Variables that go into the calculus can include whether the datum constitutes "content," its age, the nature of the service being offered, and many others. That some of the rules, such as the 180-day threshold, are non-intuitive and contrary to the reasonable expectation of our users, adds to the challenge of applying the law to any specific facts.

2. The legal process you require before disclosing information when you get law enforcement requests. If you are unable to identify the legal process for the specific categories, please explain the challenges you face in determining the appropriate legal process to require under the Electronic Communications Privacy Act by using examples drawn from the list of services/information below:

A) Web Mail
B) Search
C) Names or IP addresses of users who searched for a specific phrase
D) Word processing, spreadsheets and online calendars
E) Online photo and video storage services
F) Geo-location information (historical or prospective)
G) Instant Messaging communications
H) Social networking
I) Blogs

What legal process a government entity can use to compel a provider like Google to disclose information relating to electronic communication or remote computing services is specified in ECPA. Google complies with the law, and scrutinizes legal process that it receives from government entities for such user data to help

ensure that the process is valid and otherwise unobjectionable. Generally, the data a government entity can seek through ECPA falls into three main categories, each with slightly differing requirements for production: (i) subscriber information, (ii) content, and (iii) other records. When Google receives legal process seeking information about a subscriber, Google will attempt to notify the subscriber where practical and legally permissible and if Google understands that doing so would not jeopardize an investigation.

Subscriber information. Upon issuance of a valid administrative, trial or grand jury subpoena seeking information about a subscriber or customer that is otherwise unobjectionable, an ECS or RCS provider is required by ECPA to produce information specified in 18 U.S.C. section 2703(c)(2) to the extent the provider has such information and that information is requested in the legal process.

Specifically, section 2703(c)(2) permits a government entity to use one of the listed subpoena types to compel an ECS or RCS provider to disclose the:

> (A) name, (B) address, (C) local and long distance telephone connection records, or records of session times and durations, (D) length of service (including start date) and types of service utilized, (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and (F) means and source of payment for such service (including any credit card or bank account number),
>
> of a subscriber to or customer of such service….

18 U.S.C. section 2703(c)(2). Government entities can also use orders issued under 2703(d), and search warrants issued in compliance with section 2703, to compel a provider to disclose this above types of information.

Content: As described in response to the first question, under ECPA, a government entity can require providers to disclose contents of a wire or electronic communication held by an RCS or ECS upon submission of a valid search warrant issued in compliance with to 18 U.S.C. section 2703. Under the statute, a government entity can also use a court order issued under 18 U.S.C. section 2703(d) or an administrative, trial or grand jury subpoena to compel the production of such content held by an RCS or from an ESC where the content is older than 180 days. The use of anything other than a search warrant to compel the production of such content requires that the government first give notice to the customer or subscriber of the service, but there are circumstances in which the government can delay giving the notice. See 18 U.S.C. section 2705(a)(1)(B).

Other Records: To compel an ECS or RCS provider to disclose information that is neither subscriber information enumerated in section 2703(c)(2) nor content, a government entity must serve on the provider a court order issued under 2703(d) or a search warrant issued in compliance with 2703.

As discussed in response to question 1, the ECPA rules around content are particularly difficult to apply in practice, though in certain cases even determining what data falls within the self-contained list of subscriber information can be difficult. The email example illustrates the conflicting interpretations of when content is "in electronic storage" and when it is not, and the troubling lessening of privacy protection for content that is more than 180days old. These same challenges and counter -intuitive results exist for every service listed in

the question.

We appreciate the opportunity to be heard, and the time and effort devoted by this Subcommittee to examine this important matter. Google looks forward to assisting the Congress in updating FCPA.

Microsoft Corporation Response to Questions from the House Subcommittee on the Constitution, Civil Rights and Civil Liberties

November 2010

For the categories of user information listed in (A)-(I)[1] below, please tell us:

1. ***What position you generally take regarding classifying services or information as Electronic Communications Storage "ECS", Remote Communications Storage "RCS" or neither. Or, if you are unable to state a specific classification for each category, please explain the challenges you face in determining whether law enforcement requests for these types of information fall under ECS or RCS and in your explanation, please use examples drawn from the list of services/information below;***

Technology has changed drastically since ECPA was enacted in 1986. It was not possible at that time to contemplate the manner and extent of the changes that have occurred in the 24 years since the ECS and RCS definitions[2] were drafted. Technological changes, coupled with the rather ambiguous definitions, create significant challenges for online service providers in determining the appropriate classification for their services.

Today, cloud service providers offer a wide range of services – some that have traditionally been categorized as ECS and some as RCS. Increasingly, providers are developing robust, feature-rich services that offer functionality associated with both ECS and RCS. How services that fall into the last category should be treated under ECPA, however, is not entirely clear. For example, web-based Office applications now offer multiple users the ability to collaborate to create, edit, share and even publish Office documents online. This service mixes functions traditionally categorized as RCS (i.e., storage and remote processing) with functions traditionally categorized as ECS (i.e., the ability to publish and communicate while working collaboratively on Office documents).

Classifying new services that did not exist when ECPA was enacted, such as the provision of a search engine, is also challenging. Users send queries to a search site, the queries are processed and then the service sends back results consisting of links and a brief summary of relevant content. Search can be used to find current news, map a location, find movie listings at local theatres, find posts by social networking users, and locate online images. Thus, search provides a new kind of service, mixing both remote processing as well as enabling users to send and receive communications.

---

[1] For purposes of this response, Microsoft has combined categories "(b) search" and "(c) IP addresses of users who searched for a specific phrase" since both are a part of the same service -- search. Due to this combination, Microsoft's response moved each of the categories (c) through (i) up a letter so we are responding to categories (a) through (h). All categories are addressed in the response.

[2] ECPA defines an "Electronic Communication Service" (or ECS) as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). "Remote Computing Service" (or RCS) is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).

Simply interpreting the definitions of an ECS or RCS to apply them to a service can be challenging under ECPA since services can also be used by different people in different ways. One person may use an online photo service, for example, to create a back-up copy of photos they store on their home computers, while others may publish images on the Internet or open up a discussion about a particular image.

Even courts have been divided on issues related to classifying services under ECPA. Some courts have held that a single service must be *either* an ECS or a RCS, and others that it can be *both* an ECS and a RCS. Compare *Quon v. Arch Wireless Co.*, 529 F.2d 892 (9th Cir. 2008) (service provider is either an ECS or a RCS, but not both) with *Flagg v. City of Detroit*, 252 F.R.D. 346, 362 (E.D. Mich. 2008) (finding that a service provider can provide services that are both ECS and RCS).

As a general rule, when a service has properties of both an ECS and an RCS, Microsoft will treat the service as an ECS and will require for disclosure the legal process required for an ECS.

a. Web Mail[3] –Web mail enables users to send and receive communications. While we appreciate that users are increasingly relying on their web mail accounts for storage, the principle purpose of the service is to enable communications, and we would, therefore, categorize this service as an ECS.

b. Search, Names or IP addresses of users who searched for a specific phrase – We consider search to be a challenging service to categorize under ECPA, since the service was clearly not contemplated in either the ECS or RCS definitions. However, Microsoft would take the position that search is an ECS since the search queries contain the content of communications, and search results often deliver the content of communications (e.g. news, images, social networking posts, etc.).

c. Word processing, spreadsheets and online calendars – The classification of services offering word processing, spreadsheets and online calendars will depend on the particular functionality and features. Where a service enables collaborative communication or the ability to publish communications to others on the Internet, Microsoft would classify the service as an ECS. Where the service is intended to provide access to the application and remote storage of content the service would be classified as a RCS because the service then would be providing classic RCS processing and storage functionality.

d. Online photo and video storage services – Because online photo and video services typically offer the ability for users to publish images to others and communicate through comments, Microsoft would generally consider such services to be an ECS. If

[3] Microsoft's responses to this question are based upon our view of the typical features of a service falling within an identified category. In order to make a definitive classification for a particular service falling within an identified category, we would need to conduct a detailed review of the features of such service.

the service only provided backup or remote storage services, Microsoft would consider such services to be an RCS.

e. Geo-location information (historical and prospective) — We are interpreting geo-location information to be location information related to the use of mobile communication devices, such as cellular telephones. Since the information is related to a service providing the ability to send or receive communications, Microsoft would classify such information as relating to an ECS.

f. Instant Messaging communications – Because this is principally a communications service, we categorize instant messaging communications as relating to an ECS.

g. Social networking – The classification of a social networking service is dependent upon the features of the particular service. Generally speaking, most social networking services have one or more features that provide its users with the ability to send and receive electronic communications, as well as to publish the content of communications on the Internet. Accordingly, Microsoft would classify such a service as an ECS.

h. Blogs – Because a blog provides a user with the ability to send or receive communications, we would categorize a blogging service as an ECS.

2. The legal process you require before disclosing information when you get law enforcement requests. If you are unable to identify the legal process for specific categories, please explain the challenges you face in determining the appropriate legal process to require under the Electronic Communications Privacy Act by using examples drawn from the list of services/information below.

ECS: In response to a Federal or State grand jury subpoena, or an administrative subpoena authorized by a federal or state statute, a provider of an ECS should disclose the six categories of basic subscriber information listed in ECPA, 18 U.S.C. § 2703(c)(2), which are name, address, records of session times and durations, length and type of service utilized, subscriber or other identity number (including any temporarily assigned Internet protocol address), and means or source of payment for service ("basic subscriber information"). When compelled, a provider should also release any stored communications older than 180 days when the government has provided notice to the subscriber or customer, unless delayed notice is authorized under 18 U.S.C. § 2705.

In response to a federal or state court order complying with the requirements of 18 U.S.C. § 2703(d), a provider should disclose log files, other non-content records or information pertaining to a subscriber or user of that service, as well as any information described above that can be compelled to be disclosed with a subpoena (with the same notice caveat described in the preceding paragraph).

In response to a federal or state search warrant issued by a court of competent jurisdiction, a provider should disclose the stored content of all requested communications for a user, as well as all other account records described above that can be compelled with a subpoena or court order complying with 18 U.S.C. §2703(d).

To compel the disclosure of geo-location data, a governmental entity would need to obtain a court order that complies with the requirements of 18 U.S.C. § 2703(d) or a federal or state search warrant. To obtain geo-location information prospectively, a governmental entity would need to obtain a court order authorizing the installation and use of a pen register and trap and trace device pursuant to 18 U.S.C. § 3123.

RCS: In response to a Federal or State grand jury subpoena, or an administrative subpoena authorized by a federal or state statute, a provider of an RCS should disclose any content stored by the user where the government has provided notice to the subscriber or customer unless delayed notice is authorized under 18 U.S.C. § 2705, plus basic subscriber information.

In response to a federal or state court order complying with the requirements of 18 U.S.C. § 2703(d), a provider should disclose the information described above for a subpoena, as well as log files and other non-content records or information pertaining to a subscriber or user of the service (with the same notice caveat described in the preceding paragraph).

In response to a federal or state search warrant issued by a court of competent jurisdiction, a provider should disclose the stored content for the service, as well as all other account records described above that can be compelled with a subpoena or court order complying with 18 U.S.C. §2703(d).

FEDERAL LAW ENFORCEMENT OFFICERS ASSOCIATION
P.O. Box 326 Lewisberry, PA 17339
www.fleoa.org
(717) 938-2300

Representing Members Of:
AGENCY for INTERNATIONAL DEVELOPMENT
AGRICULTURE and FOREST SERVICE
COMMERCE
Export Enforcement, OIG
& NOAA Tolerant Law Enforcement
DEFENSE
Air Force – OIG
Army – CID
Defense Criminal Investigative Service
Naval Criminal Investigative Service
OIG
EDUCATION – OIG
ENERGY – OIG
ENVIRONMENTAL PROTECTION AGENCY – CID & OIG
FEDERAL HOUSING ENTERPRISE OVERSIGHT – OIG
GENERAL SERVICES ADMINISTRATION
HEALTH & HUMAN SERVICES
Food & Drug Administration & OIG
HOMELAND SECURITY
Border Patrol
Coast Guard Investigative Service
Immigration & Customs Enforcement
Secret Service
Federal Emergency Management Agency
Federal Protective Service
OIG/Inspector Service
Transportation Security Administration
HOUSING & URBAN DEVELOPMENT – OIG
INTERIOR
Bureau of Indian Affairs
Bureau of Land Management
Fish & Wildlife Service
National Park Service
OIG
U.S. Park Police
JUSTICE
Bureau of Alcohol, Tobacco, Firearms & Explosives
Drug Enforcement Administration
Federal Bureau of Investigation
U.S. Marshals Service
OIG
U.S. Attorney's Offices
LABOR – OIG & Inspections
NATIONAL AERONAUTICS & SPACE ADMIN. – OIG
NUCLEAR REGULATORY COMMISSION – OIG
POSTAL SERVICE – OIG & Inspectors
RAILROAD RETIREMENT BOARD – OIG
SECURITIES & EXCHANGE COMMISSION – OIG
SMALL BUSINESS ADMINISTRATION – OIG
SOCIAL SECURITY ADMINISTRATION – OIG
STATE DEPARTMENT
Bureau of Diplomatic Security & OIG
TRANSPORTATION – OIG
TREASURY
IRS-CID & OIG
Internal Revenue Service – IG
TIGTA
U.S. COURTS JUDICIAL
Probation, Pretrial & Pretrial Services
VETERANS AFFAIRS – OIG

NATIONAL OFFICERS
President
RON MUREA
Immediate Vice President
NATHAN CATERA
Vice President – Operations
LAZARO GOMEZ
Vice President – Agency Affairs
CHRIS SCHUPMANN
Vice President – Membership Outreach
JOHN RAMSEY
Secretary
MARIA COSCIA
Treasurer
JAMES OTTEN III
Legislative Executive
DONNA CHAMPLESON
National Chapter Director
RASHEED TAHIR
National Awards Director
SHAUN MARTAMCPHERSON
Legislative Coordinators
Abdiaziz Farah Osman
Andy Lewis
Legislative Counsel
Jenny A. Hoffman
Brian M. Hoey

October 12, 2010

The Honorable John Conyers, Jr.
Chairman, Judiciary Committee
United States House of Representatives

The Honorable Lamar S. Smith
Ranking Member, Judiciary Committee
United States House of Representatives

Dear Chairman Conyers and Ranking Member Smith:

As the National President of the 26,000 members of the Federal Law Enforcement Officers Association (FLEOA), I am writing to you to express my members' concerns regarding some of the Electronic Communications Privacy Act (ECPA) proposals put forth by the Digital Due Process coalition. As active Criminal Investigators, the FLEOA membership is concerned that the Digital Due Process[1] alleged good intentions are paving a road that will enable criminals and stall out law enforcement officers. To wit:

- The Digital Due Process coalition has advanced proposals that would place new restrictions on law enforcement. These would negatively impact a variety of crucial law enforcement techniques including the production of stored communications, the disclosure of cell phone location information, the use of pen register and trap and trace devices and a restriction on subpoenas issued under the Stored Communications Act.

- FLEOA does not support raising the evidentiary standard for any of these techniques. FLEOA does support any measure to clarify areas where there currently exists ambiguity as to what a service provider must provide to a lawful request, and what procedure a law enforcement entity must take to obtain this information. Clarification does not mean increased evidentiary hurdles for law enforcement.

- FLEOA believes that current legal standards strike the appropriate balance between law enforcement needs and the protection of privacy and civil liberties. Again, clarification of the law does not mean raising the legal standard. Law enforcement representatives should be at the table during any discussions of any specific proposals to change the Electronic Communications Privacy Act.

- Many of the investigative techniques that would be impacted by the principles put forth by the Digital Due Process Coalition are used by investigators at the very early stages of an investigation, long before the government could develop probable cause and satisfy a warrant requirement. The DDP proposal to raise the standard for Pen Registers and Trap and trace devices has already been rejected by Congress and the proposal that would have raised the requirements for using these devices have been rejected by law enforcement and prosecutorial organizations.

- FLEOA recognizes that regardless of what legal standards might be imposed on law enforcement, even after meeting such a standard, law enforcement might not be able to obtain the information they seek either because of collection problems caused by new technologies or because there was no legal requirement for a service provider to retain the sought after data. Additionally, recent court decisions and legal commentators have called into question the applicability of "the plain view doctrine" in searching commuters or email accounts(i.e., you are supposed to ignore evidence of other crime that you find if it is unrelated to the crime for which you are conducting the search).

- Cell site location information, being non-content information should not require a warrant to obtain. While clarification is probably needed in this area based on confusion in the Federal courts, a warrant

should not be required for what is often times very general location information. The Digital Due Process coalition proposes the warrant requirement as a way to clarify existing ambiguity, but legislation that allows any type of non-content, cell-site location information based on a showing of "specific and articulable facts that the information is relevant and material to an ongoing criminal investigation," would do the same thing and would provide greater public safety protections.

- For any provision of ECPA that requires a "2703(d)" order, if the government makes the showing that is currently required under 18 U.S.C. 2703(d), than the court should be required to issue the requested court order (change "may" to "shall"). Allowing a magistrate judge to deny the order if the showing is made is contra to public safety concerns and only adds to the confusion.

While there are other areas of the Electronic Communications Privacy Act that could use clarity, public safety should not be set aside because the "privacy groups" are louder. FLEOA would welcome any opportunity to provide input to the legislative process regarding these or other issues as Congress continues to examine the issue and ultimately consider legislative solutions.

Respectfully submitted,
J. Adler
J. Adler
National President

CITIZENS
AGAINST
GOVERNMENT
WASTE

Center for Financial Privacy and Human Rights
Free markets are a necessary condition of liberty, prosperity and tolerance

Written Statement of the
Competitive Enterprise Institute, The Progress & Freedom Foundation,
Citizens Against Government Waste, Americans for Tax Reform, and
The Center for Financial Privacy and Human Rights

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

September 23, 2010

Hearing on
ECPA Reform and the Revolution in Cloud Computing

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

The undersigned public interest groups, think tanks, and advocacy organizations respectfully submit these comments to the United States House Committee on the Judiciary to urge Congress to amend U.S. laws to better safeguard citizens against unwarranted governmental access to private information held electronically by third parties. Such information includes emails, instant messages, and mobile locational data. We recognize the importance of ensuring that law enforcement agencies possess the tools necessary to effectively enforce the law and successfully prosecute criminals, but we also believe that the unnecessary vagueness and complexity of the current electronic privacy regime actually impede law enforcement efforts. We have joined the Digital Due Process Coalition (www.digitaldueprocess.org) to express our strong support for updating the Electronic Communications Privacy Act (ECPA). The Coalition has proposed that Congress establish clear, consistent, and technologically neutral rules governing the compelled disclosure by law enforcement of electronic information stored with service providers.

Obsolete Federal Privacy Laws Threaten the Emerging Cloud Computing Industry, Endangering Job Creation and Economic Growth at Home and Abroad.

To date, cloud computing[1] has transformed both global commerce and the daily lives of individuals worldwide for the better.[2] Cloud computing's rapid growth is expected to continue for the foreseeable future. Some experts believe that its ultimate impact on business, communications, and productivity will be nothing short of revolutionary.[3] Market research firm IDC estimates that cloud services will grow more than five times faster than traditional information technology products through 2014.[4] Growth in cloud-based services is also expected to fuel the creation of hundreds of thousands of jobs worldwide while also enabling significant productivity gains and economic growth.[5]

The success of cloud computing—and its benefits for the U.S. economy—depends largely on updating the outdated federal statutory regime that currently governs electronic communications privacy.

The privacy of sensitive information stored with cloud computing providers is a major concern for many consumers and business executives. According to a 2010 Harris Interactive poll, 81 percent of online Americans are concerned about the security of cloud computing services, while 62 percent say they would not entrust files containing personal information to cloud computing services.[6] A 2010 Zogby International poll found that 88 percent of Americans believe consumers "should enjoy similar legal privacy protections online as they have offline."[7] A 2009 survey commissioned by Microsoft found that 90 percent of senior business leaders and members of the public are "concerned about the security and private of personal data" in the cloud.[8] Federal government officials have reiterated these concerns. U.S. Chief Information Officer Vivek Kundra recently stated that government should "address various issues related to security, privacy, information management and procurement to expand cloud computing services."[9]

---

[1] According to NIST, "cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

[2] *Use of Cloud Computing Applications and Services*, Pew Internet & American Life Project, Sep. 12, 2008, pp. 4. *Available at* http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.

[3] *See* Jeffrey F. Rayport & Andrew Heyword, *Marketspace Point of View: Envisioning the Cloud: The Next Computing Paradigm*, March 20, 2009, pp. 2. http://www.marketspaceadvisory.com/cloud/Envisioning-the-Cloud.pdf.

[4] IDC, "Aid to Recovery: The Economic Impact of IT, Software, and the Microsoft Ecosystem on the Global Economy," October 2009 http://www.businesswire.com/portal/site/home/permalink/?ndmViewId=news_view&newsId=20100623005419&newsLang=en.

[5] Frederico Etro, "The Economic Impact of Cloud Computing on Business Creation, Employment, and Output in Europe," Review of Business and Economics, 2009/2, pp. 179-208.

[6] David Linthicum, "Cloud security's PR problem shouldn't be shrugged off," *InfoWorld*, April 27, 2010. http://www.infoworld.com/d/cloud-computing/cloud-securitys-pr-problem-shouldnt-be-shrugged-776

[7] Zogby International, Results from June 4-7 Nationwide Poll (June 7, 2010) http://www.precursorblog.com/files/pdf/topline-report-key-findings.pdf.

[8] *See* Brad Smith at the Brookings Institution Policy Forum, "Cloud Computing for Business and Society," January 20, 2010, pp. 3. http://blog.seattlepi.com/microsoft/library/20100120smithspeech.pdf

[9] Vivek Kundra, White House Blog, "Streaming at 1:00: In the Cloud" (Sept. 15, 2009), available at http://www.whitehouse.gov/blog/streaming-at-100-in-the-cloud/

To be sure, storing information in the cloud entails numerous risks and vulnerabilities, many of which government is ill-suited to address.[10] Private firms are, after all, responsible for keeping sensitive user data safe from hackers and other cybersecurity threats.[11] But Congress and the courts are responsible for establishing reasonable safeguards to protect information stored in the cloud from unwarranted compelled disclosure to law enforcement. Unfortunately, the existing statutes governing this are woefully inadequate.

ECPA, the primary federal statute governing privacy in electronic communications, was enacted by Congress in 1986. While the law has been revised several times since then, many key sections remain largely unchanged.[12] In the 24 years since ECPA's initial enactment, technological evolution has profoundly altered how businesses and individuals communicate in ways that policymakers could not have envisioned in 1986. Service providers now house massive quantities of individuals' and businesses' sensitive information on their servers, thanks to the advent of now-ubiquitous communications platforms such as email, the World Wide Web, instant messaging services, blogs, social networks, and smartphones.[13]

Since 1986, computing power has doubled roughly every 18 months—in accordance with Moore's Law—and the cost of digital storage has plummeted.[14] This has enabled service providers to offer dramatically expanded—if not essentially unlimited—storage.[15] Cloud providers now offer a growing array of free, ad-supported data hosting services, such as Gmail, Mediafire, and Dropbox.[16] Such services have gained massive popularity among individual Internet users as well as small businesses.[17] Many large enterprises also use cloud computing services such as Microsoft's Azure, Salesforce CRM, and Amazon Simple Storage Service (S3).[18]

Today, hundreds of millions of individuals around the world take advantage of cloud computing services. Social networking site Facebook has more than 500 million active users, including about 150 million in the United States.[19] In other words, nearly *one out every two* Americans is currently an active Facebook user. Gmail, a leading webmail

---

[10] "Cloud Computing and Privacy," World Privacy Forum website, http://www.worldprivacyforum.org/cloudprivacy.html
[11] Clyde Wayne Crews, "Cybersecurity and Authentication: The Marketplace Role in Rethinking Anonymity—Before Regulators Intervene," *Knowledge, Technology & Policy*, Vol. 20 No. 2, pp. 97-105, http://www.springerlink.com/content/dq8522k3361757r4/
[12] *See* Justice Information Sharing Federal Statutes page. *Available at* http://www.it.ojp.gov/default.aspx?area=privacy&page=1285
[13] Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, at 4 (Feb. 23, 2009) http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf
[14] Clayton M. Christensen, *The Innovator's Dilemma*, 1997, Chapter One http://www.businessweek.com/chapter/christensen.htm
[15] Robert D. Atkinson & Andrew S. McKay, Information Technology & Innovation Foundation, *Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution* at 14 (March 2007) http://www.itif.org/files/digital_prosperity.pdf
[16] *See e.g.* Susie Ochs, "Online Storage Battle: Which Cloud Back-Up Service Reigns Supreme?" *MacLife.com*, June 11, 2009. http://www.maclife.com/article/reviews/online_storage_battle_which_cloud_backup_service_reigns_supreme
[17] Robert Cheng, "'Cloud Computing': What Exactly Is It, Anyway?," *The Wall Street Journal*, February 8, 2010. http://online.wsj.com/article/SB10001424052748703580904574638391318085158.html
[18] Charlton Barreto, "Cloud Computing: Rich Services Cloud: The Value Proposition," Intel Technology Strategy, November 2009, pp. 23. http://charltonb.typepad.com/talks/110209-cbb-cloud/Cloud%20Computing%20-%20Rich%20Services.pdf
[19] *See* Facebook Press Room Statistics. *Available at* http://www.facebook.com/press/info.php?statistics

service, has more than 175 million active users.[20] As the use of cloud services grows, popular awareness of the attendant privacy risks grows alongside it. As a result, individuals and businesses are increasingly demanding robust information security assurances from cloud providers—and cloud providers are responding by competing on privacy and security.[21] But they can do little to assure users that their data will remain free from unwarranted governmental access.

In many cases, ECPA authorizes law enforcement to compel service providers to disclose potentially sensitive information without first obtaining a search warrant based upon probable cause or without any judicial authorization at all.[22] For instance, a law enforcement official who wishes obtain the contents of a communication in "electronic storage" for more than 180 days may be able to compel a provider to disclose the communication through a mere subpoena, which is typically issued with no judicial scrutiny.[23]

In recent months, there has been growing mainstream media attention on the ease with which government can access user information stored with remote service providers.[24] For instance, *PC World*'s 2010 article, "Why ECPA Should Make You Think Twice about the Cloud," discussed in great detail the privacy risks of storing data with cloud providers.[25] Google recently launched a tool disclosing the number of requests for user data it received from U.S. law enforcement in the second half of 2009 (the figure was 3,580).[26] In the first half of 2010, the number of requests Google received rose to 4,287—an increase of 20 percent compared to the previous six-month period.[27] A June 2010 *Wall Street Journal* article chronicled the recent rise of venture capital-backed privacy startups, noting that, "[I]n the wake of recent privacy flaps involving AT&T, Facebook, Apple Inc. and others, consumer awareness has grown."[28] Prompt action by Congress to strengthen federal laws safeguarding the privacy of information stored in the cloud is growing more important by the day as Americans become ever more reliant on cloud computing in all aspects of life.[29]

---

[20] Jessica E. Vascellaro, "Gmail, Too, Seeks to Rival Facebook," *The Wall Street Journal*, February 8, 2010. http://online.wsj.com/article/SB10001424052748703630404575053480962942848.html

[21] David Navetta, "Cloud Providers Competing on Data Security & Privacy Contract Terms," InfoLawGroup.com, April 12, 2010. http://www.infolawgroup.com/2010/04/articles/cloud-computing-1/cloud-providers-competing-on-data-security-privacy-contract-terms/

[22] *See* 18 U.S.C. § 2703(b)(1)(B), http://www.law.cornell.edu/uscode/18/usc_sec_18_00002703----000-.html

[23] *See* U.S. Department of Justice Electronic Surveillance Manual at 25. *Available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf

[24] *See e.g.* Google News search for "Electronic Communications Privacy Act," which lists 320 news articles for 2010. http://www.google.com/search?q=%22Electronic+Communications+Privacy+Act+%28%22&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a#q=%22Electronic+Communications+Privacy+Act%22&hl=en&client=firefox-a&rls=org.mozilla:en-US:official&tbs=nws:1,cd_min:2010,cd_max:2010,cdr:1&source=lnt&fp=180bd06780889f90

[25] Tony Bradley, "Why ECPA Should Make You Think Twice about the Cloud," *PC World*, March 30, 2010. http://www.pcworld.com/businesscenter/article/192989/why_ecpa_should_make_you_think_twice_about_the_cloud.html

[26] *See* Google Transparency Report FAQ *Available at* http://www.google.com/governmentrequests/overview.html

[27] Ryan Singel, "Feds' Requests for Google Data Rise 20 Percent," *Wired Threat Level*, September 21, 2010. http://www.wired.com/threatlevel/2010/09/google-government-requests-rise

[28] Pui-Wing Tam and Ben Worthen, "Funds Invest in Privacy Start-Ups," *The Wall Street Journal*," June 20, 2010. "http://online.wsj.com/article/SB10001424052748703438604575315182025721578.html

[29] Lisa Banks, "Cloud computing to increase annual data growth 24-fold by 2020: study," *CIO*, May 5, 2010. http://www.cio.com.au/article/345435/cloud_computing_increase_annual_data_growth_24-fold_by_2020_study/

If Congress fails to reform privacy laws, some Americans will choose not to take advantage of cloud computing, while others will simply turn to data encryption solutions for protecting their data. Such solutions could distort the evolution of cloud computing in harmful ways. Several services today allow users to store encrypted information in the cloud without sharing the key with the provider.[30] While this arrangement is ideal in many circumstances—encryption maximizes data security and minimizes the risks of unwarranted governmental intrusion—it also comes at a cost.

First, users will bear the direct cost of paying for encrypted services, which are often slower than unencrypted services (a significant cost, since some cloud computing applications already start from a performance disadvantage compared to desktop-based applications).[31] Second, if cloud service providers cannot access in plaintext the information stored by their users, they may not be able to rely on advertising to support those services. The most popular cloud service in use today is webmail, and Google's Gmail service demonstrates how targeted advertising (ads based on algorithmic scanning of keywords in an email) can support *dramatic* improvements in the quality of a service. When Gmail launched in 2004, Yahoo! Mail (then, as now, the leading webmail provider) offered customers less than 10 megabytes of email storage, yet Gmail offered an astounding 1 gigabyte of storage.[32] Today that figure is over 7.5 GB, and Gmail has become much more than a plain vanilla email service, supporting a variety of applications and features unimagined in 2004.[33] But Gmail's ad-serving feature simply would not work if users routinely encrypted their messages and held onto the encryption key. Some users *might* pay for such innovative services, but on the whole, there would likely be less funding available for Gmail and similar cloud services. Consumers would pay more or get less—on top of the cost of encryption itself. In many ways, therefore, ECPA's failure to protect our digital communications and documents amounts to a "tax" on Americans.

The Digital Due Process Coalition's Proposed Reforms to the Electronic Communications Privacy Act Will Preserve the Building Blocks of Law Enforcement Investigations.

The reforms urged by the Digital Due Process coalition will not substantially constrain legitimate law enforcement investigations or other governmental efforts to safeguard U.S. national security and combat terrorism. Our proposed reforms do not alter the Foreign Intelligence Surveillance Act, the statute used to monitor terrorists and spies and to gather foreign intelligence to prevent terrorist attacks. Although our proposed reforms would impose some additional limitations on the ability of law enforcement to compel service

[30] *See e.g.* Mozy Privacy Commitment, "Choose Mozy's encryption key using 448-bit Blowfish or manage your own key using military-grade 256-bit AES to secure your data during storage." http://mozy.com/privacy/commitment/
[31] R. Colin Johnson, "IBM Encryption Breakthrough Could Secure Cloud Computing," *Smarter Technology,* October 14, 2009. http://www.smartertechnology.com/c/a/Technology-For-Change/IBM-Encryption-Breakthrough-Could-Secure-Cloud-Computing/
[32] *See* Chris Anderson, Free: The Future of a Radical Price at 112-118 (2009)
[33] *See* Digital Prosperity *supra* Note 15, 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...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.").

providers to disclose user information in the criminal context, the proposed limitations are consistent with the spirit of the Fourth Amendment to the United States Constitution. Our nation's founders rightly recognized the importance of balancing the need to effectively enforce the laws of the land against the right of citizens to be free from unwarranted governmental intrusion into their private affairs.[34] Therefore, they sought to protect Americans against unreasonable search and seizure by government through the requirement that law enforcement agents first obtain a warrant from a judge upon a showing of probable cause.[35]

U.S. communications privacy laws no longer strike an acceptable balance between the two important priorities of privacy and security. In effect, they fail to protect the "papers and effects" of the Digital Era. Congress never voted for less privacy. Rather, consumers changed the way they communicate as technology evolved, and the law simply has not kept up with those changes. The resulting deficiencies pose a grave threat to the individual freedoms enshrined in the Constitution. Alex Kozinski, Chief Judge of the U.S. Court of Appeals for the Ninth Circuit and a Reagan appointee, observed in a recent dissent in a case involving GPS tracking that, "The needs of law enforcement ... are quickly making personal privacy a distant memory. 1984 may have come a bit later than predicted, but it's here at last."[36]

ECPA and other federal wiretap statutes currently contain a number of special exceptions for child pornography, life-threatening emergencies, kidnapping, and other exigent and serious circumstances.[37] The Digital Due Process coalition is not urging Congress to amend these provisions.[38] Rather, the Coalition's principles for reform would leave existing exceptions untouched, and preserve the building blocks of law enforcement investigations – subpoenas, court orders based on lower standards of proof, and warrants when there is probable cause.

Orin Kerr, a Professor at George Washington University School of Law who formerly served as a computer crimes prosecutor for the Justice Department and as an assistant U.S. attorney for the Eastern District of Virginia, recently testified before the U.S. House Judiciary Subcommittee on the Constitution, Civil Rights, and Civil Liberties that, "[R]eforms [to ECPA] are surely needed."[39] While emphasizing the importance of maintaining a "balanced approach to the new investigations involving new network technologies that the Fourth Amendment strikes in the physical world," Kerr also expressed support for three of the four proposals advocated by the Digital Due Process coalition. In a 2004 *George Washington Law Review* article, Kerr stated that, "[T]he most

---

[34] Orin Kerr, "Applying The Fourth Amendment To The Internet: A General Approach," *Stanford Law Review,* Vol. 62, Issue 4, pp. 1017. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=421860

[35] *Ibid,* pp. 1044.

[36] *See* dissent by Chief Judge Kozinski in *United States v. Pineda-Moreno,* U.S. No. 08-30385, August 12, 2010, pp. 11504. http://www.ca9.uscourts.gov/datastore/opinions/2010/08/12/08-30385.pdf

[37] *See e.g.* Electronic Communications Privacy Act Rule by Exceptions, Cybertelecom.org, *available at* http://www.cybertelecom.org/security/ecpaexception.htm

[38] J. Beckwith Burr, "The Electronic Communications Privacy Act of 1986: Principles for Reform," WilmerHale, pp. 4. http://www.digitaldueprocess.org/files/DDP_Burr_Memo.pdf

[39] *See* Orin Kerr, "Testimony of Orin S. Kerr before the 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. http://volokh.com/wp/wp-content/uploads/2010/05/KerrTestimony.pdf

obvious problem with the current version of the SCA is the surprisingly weak protection the statute affords to compelled contents of communications under the traditional understanding of ECS and RCS" (Electronic Communications Services and Remote Computing Services). He recommended that Congress "bolster the privacy protections that cover stored content held by an RCS or by an ECS for more than 180 days in 18 U.S.C. § 2703(b)."[40]

Conclusion

If Congress wishes to ensure Americans enjoy the full benefits of the cloud computing revolution, it should simply reform ECPA in accordance with the principles proposed by the Digital Due Process coalition, rather than enacting distortionary new subsidies or industrial policies. Requiring that law enforcement obtain a search warrant from a judge upon a showing of probable cause before rifling through the contents of our electronic communications and digital documents should be uncontroversial. Such a requirement would extend the protections of the Fourth Amendment to our digital "papers and effects," and would *not* interfere with law enforcement or national security investigations. We, the undersigned nonprofit organizations dedicated to the principles of limited government and individual rights, ask Members of both parties to lend your support to these proposed reforms.

Respectfully Submitted,

Ryan Radia
Associate Director of Technology Studies
Competitive Enterprise Institute

Berin Szoka
Senior Fellow and Director, Center for Internet Freedom
The Progress & Freedom Foundation

Thomas A. Schatz
President
Citizens Against Government Waste

Kelly William Cobb
Executive Director, Digital Liberty Project
Americans for Tax Reform

J. Bradley Jansen
Director
Center for Financial Privacy and Human Rights

---

[40] Orin Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," *George Washington Law Review*, Vol. 72, 2004, pp. 30-31. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=421860