S. HRG. 111–1002

THE ELECTRONIC COMMUNICATIONS PRIVACY ACT: PROMOTING SECURITY AND PROTECTING PRIVACY IN THE DIGITAL AGE

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

SEPTEMBER 22, 2010

Serial No. J–111–109

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
66–875 PDF WASHINGTON : 2011

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

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
ARLEN SPECTER, Pennsylvania
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois
BENJAMIN L. CARDIN, Maryland
SHELDON WHITEHOUSE, Rhode Island
AMY KLOBUCHAR, Minnesota
EDWARD E. KAUFMAN, Delaware
AL FRANKEN, Minnesota

JEFF SESSIONS, Alabama
ORRIN G. HATCH, Utah
CHARLES E. GRASSLEY, Iowa
JON KYL, Arizona
LINDSEY GRAHAM, South Carolina
JOHN CORNYN, Texas
TOM COBURN, Oklahoma

BRUCE A. COHEN, *Chief Counsel and Staff Director*
MATTHEW S. MINER, *Republican Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Cardin, Hon. Benjamin L., a U.S. Senator from the State of Maryland	2
Feingold, Hon. Russell D., a U.S. Senator from the State of Wisconsin, prepared statement	151
Franken, Hon. Al, a U.S. Senator from the State of Minnesota	3
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	1
prepared statement	185

WITNESSES

Baker, James A., Esq., Associate Deputy Attorney General, U.S. Department of Justice, Washington, DC	6
Dempsey, James X., Esq., Vice President for Public Policy, Center for Democracy and Technology, San Francisco, California	15
Jaffer, Jamil N., Esq., Attorney, Washington, DC	19
Kerry, Cameron F., Esq., General Counsel, U.S. Department of Commerce	3
Smith, Brad, Esq., General Counsel and Senior Vice President, Legal and Corporate Affairs, Microsoft Corporation, Redmond, Washington	17

QUESTIONS AND ANSWERS

Responses of James A. Baker to questions submitted by Senator Leahy, Specter and Feingold	33

SUBMISSIONS FOR THE RECORD

American Civil Liberties Union (ACLU), Laura W. Murphy, Director, Washington Legislative Office, Christopher Calabrese, Legislative Counsel, Washington Legislative Office, and Nicole A. Ozer, seq., Technology and Civil Liberties Policy Director, Northern California, joint statement	47
Baker, James A., Esq., Associate Deputy Attorney General, U.S. Department of Justice, Washington, DC, statement	57
Blaze, Matt, Professor, University of Pennsylvania, Philadelphia, Pennsylvania, statement	64
Burr, J. Beckwith, Partner, Wilmer Cutler Pickering Hale and Dorr, LLP, Washington, DC, statement	78
Competitive Enterprise Institute, Ryan Radia, Associate Director of Technology Studies; The Progress & Freedom Foundation, Berin Szoka, Senior Fellow and Director, Center for Internet Freedom; Citizens Against Government Waste, Thomas A. Schatz, President; Americans for Tax Reform, Kelly William Cobb, Executive Director, Digital Liberty Project; and Center for Financial Privacy and Human Rights, J. Bradley Jansen, Director, Washington, DC, joint statement	101
Computer & Communications Industry Association (CCIA), Washington, DC, statement	108
Constitution Project, Washington, DC, statement	122
Dempsey, James X., Esq., Vice President for Public Policy, Center for Democracy and Technology, San Francisco, California, statement	125
Department of Commerce, Comments of Digital Due Process, June 14, 2010, statement	141
Freeman, Frederick W., Student, George Mason University, statement	153
Jaffer, Jamil N., Esq., Attorney, Washington, DC, statement	156

Page

Kerry, Cameron F., Esq., General Counsel, U.S. Department of Commerce, Washington, DC, statement 171
Schellhase, David, Executive Vice President and General Counsel, San Francisco, California, statement 187
Smith, Brad, Esq., General Counsel and Senior Vice President, Legal and Corporate Affairs, Microsoft Corporation, Redmond, Washington, statement 201

THE ELECTRONIC COMMUNICATIONS PRIVACY ACT: PROMOTING SECURITY AND PROTECTING PRIVACY IN THE DIGITAL AGE

TUESDAY, SEPTEMBER 22, 2010

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 10:10 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Patrick J. Leahy, Chairman of the Committee, presiding.

Present: Senators Leahy, Cardin, Whitehouse, Klobuchar, and Franken.

OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Chairman LEAHY. I apologize for the delay. In the back room, we were settling all the problems of the world with our distinguished witnesses, but I think that one of the things that we have learned very quickly in this area is that the Electronic Communications Privacy Act, or ECPA, is one of the Nation's premier digital privacy laws. But it is only as important as our efforts to keep it up to date might be.

It was 40 years ago that Chief Justice Earl Warren wrote that "the fantastic advances in the field of electronic communication constitute a greater danger to the privacy of the individual." That was 40 years ago. Now, Chief Justice Warren could not have imagined—in fact, I do not know if anybody could have 40 years ago—what types of communications we would have today and the differences in it.

But what he said, even with all the changes, is as relevant today as it was then. For many years, ECPA has provided vital tools to law enforcement to investigate crime and to keep us safe, while at the same time protecting individual privacy online. As the country continues to grapple with the urgent need to develop a comprehensive national cybersecurity strategy, determining how best to bring this privacy law into the Digital Age is going to be one of our biggest challenges, especially here in Congress.

When Congress enacted ECPA in 1986, we wanted to ensure that all Americans would enjoy the same privacy protections in their online communications as they did in the offline world, and at the same time allowing law enforcement to have access under legitimate ways for information needed to combat crime. We put together—and I remember very well the long negotiations we had on

that—a careful, bipartisan law designed in part to protect electronic communications from real-time monitoring or interception by the Government, as e-mails were being delivered and from searches when these communications were then stored electronically. But the many advances in communication technologies have really outpaced the privacy protections that Congress put in place.

ECPA today is a law that is often hampered by conflicting privacy standards that create uncertainty and confusion for law enforcement, for the business community, and for American consumers.

For example, the content of a single e-mail could be subject to as many as four different levels of privacy protections under ECPA, depending upon where it is stored and when it is sent. Now, no one would quibble with the notion that ECPA is outdated, but the question of how best to update this law does not have a simple answer. And I believe there are a few core principles that should guide our work.

First, privacy, public safety, and security are not mutually exclusive goals. Reform can, and should, carefully balance and accomplish each.

Second, reforms to ECPA must not only protect Americans' privacy, but also encourage America's innovation.

And, last, updates to ECPA must instill confidence in American consumers.

I am pleased that we are going to hear from the General Counsel of the Department of Commerce, who has unique insights into the impact of ECPA on American innovation. We will also get the views of the Department of Justice, which relies upon ECPA to carry out its vital law enforcement and national security duties.

Then we will have a panel of expert witnesses to advise the Committee, and I applaud the work of the Center for Democracy & Technology, Microsoft, and other stakeholders who are trying to bring together industry consensus because we want something that works. We want to protect privacy. We do not want to stifle innovation. We want to make law enforcement possible in the way with the privacies this country gives.

So having said all that, I thank those who are here. I would ask my fellow panel members, Senator Cardin, did you have anything you wished to say?

STATEMENT OF HON. BENJAMIN L. CARDIN, A U.S. SENATOR FROM THE STATE OF MARYLAND

Senator CARDIN. Well, Mr. Chairman, let me thank you very much for holding this hearing. I think this subject is one that just the hearing itself will have a beneficial impact. I think we really need to understand that it is difficult to get ahead of technology and we do not want to do anything in our laws that prevents the development of technology. It is amazing what we can accomplish today through our cell phones that we could only imagine when this bill was originally passed.

Now, the question is how do you protect the privacy of Americans, which is critically important and constitutionally protected in a way that also allows for the appropriate law enforcement tools to be effectively used.

I think it is important that we carry out one of the most important responsibilities of the Senate, which is oversight, to see how the current law is operating, to see whether it is being administered—whether those who administer it have the tools they need under existing law to effectively protect the privacy of Americans and carry out their important work.

So I welcome this hearing. I think we come to it without any preconceived thoughts as to what we need to do, but it is important that we protect privacy, give the tools to law enforcement that it needs, and understand that we do not want to do anything that would hamper the development of technology, which is critically important for America's advancement.

Chairman LEAHY. Senator Franken.

STATEMENT OF HON. AL FRANKEN, A U.S. SENATOR FROM THE STATE OF MINNESOTA

Senator FRANKEN. I did not prepare an opening statement, but I am really looking forward to this, just to hear things like what kind of conflicts are inherent in protecting privacy while at the same time protecting against things like identity theft or what kind of conflicts there are in transparency versus protecting business proprietary information, the conflicts between sort of openness and yet protection. So I am looking forward to the hearing, and thank you, Mr. Chairman, for calling this.

Chairman LEAHY. Well, thank you very much.

Our first witness will be Cameron Kerry. Mr. Kerry is the General Counsel of the Department of Commerce, where he serves as the Department's chief legal officer, chief ethics officer, and is Chair of the Department of Commerce Privacy Council. Mr. Kerry is somebody I have known for—I was going to say years—decades, actually. He has been a leader on work across the U.S. Government on patent reform and intellectual property issues, privacy, security, efforts against transnational bribery. Previously he was a partner in Mintz, Levin, a national law firm, with over 30 years of practice. He has been a communications lawyer, litigator in a range of areas, including telecommunications, environmental law, torts, privacy, and insurance regulation. Harvard College under graduate, a law degree at the Boston College School of Law.

Mr. Kerry, delighted to have you here. Please go ahead, sir. Hit the "Talk" button. Is it on red?

STATEMENT OF HON. CAMERON F. KERRY, ESQ., GENERAL COUNSEL, U.S. DEPARTMENT OF COMMERCE

Mr. KERRY. Thank you. Chairman Leahy and members of the Committee, thank you for the invitation to testify today.

I think it is clear that in the 25 years since ECPA, the Electronic Communications Privacy Act, was enacted, the communications and information landscape has been transformed. The authors of the law, including you, Mr. Chairman, recognized that this landscape would evolve continually, but I doubt that anyone foresaw the scale, the scope of the revolution that would be fueled by mobile telecommunications, by the global Internet, and by ever smaller, more powerful devices.

VerDate Nov 24 2008 11:00 Jul 07, 2011 Jkt 066875 PO 00000 Frm 00007 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66875.TXT SJUD1 PsN: CMORC

I welcome the Committee's decision to hold this hearing and to begin another of its periodic reviews of ECPA. The goal of this effort, as always, should be to ensure that as technology and new market conditions change, ECPA continues to serve its original purpose as articulated by this Committee: to establish "a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement."

I am especially pleased to be appearing today with colleagues from the Department of Justice. We work with the Department of Justice on an administration effort to develop policies on commercial data privacy and a range of issues related to information and communications technologies. While our effort is in its early phases, it is guided by our shared belief that legislative review of ECPA must be undertaken carefully and must adequately protect privacy and build consumer trust; must address concerns about competition, innovation, and other challenges in the global marketplace; and must allow the Government to protect the public in timely and effective ways.

I would like this morning to highlight some of the points in my written testimony about the importance of digital communications innovation to the U.S. economy and society and the contribution that ECPA has made to that innovation through its privacy framework.

Over several decades, the explosion of electronic communications, and especially the proliferation of broadband Internet service and Internet-based services and applications, as well as the expansion of wireless communications, has created enormous benefits to our society. By some estimates, the Internet contributes $2 trillion to the Nation's annual GDP and supports some 3 million jobs. ECPA has contributed to this remarkable growth as Congress recognized in 1986 the absence of sound privacy protections for electronic communications discourages potential customers from using innovative communications systems and discourages American businesses from developing innovative forms of telecommunications and computer technology. In this area, trust is an essential element of development.

ECPA created clear, predictable rules for service providers and a protected, trusted environment for digital commerce. It also ensured that law enforcement and national security personnel can gain access to electronic communications, subject to judicial oversight and consistent with the Fourth Amendment and American principles. As your Committee examines ECPA and its ongoing role in this process, you face the question whether the sea changes in the digital communications environment since 1986 call for changes in the statute so as to preserve the balance that Congress struck in 1986 and has maintained over time.

Let me touch on some of the changes that have occurred.

One prominent example is the global growth of cloud computing services. The range of services of platforms, of applications that are available today remotely, and the pervasiveness of their use far exceed the levels that existed in remote computing 25 years ago. According to one projection the Department of Commerce received, cloud computing revenues are going to grow from $46 billion in

2009 to $150 billion in 2012, and by next year, 25 percent of new software deployments are going to be cloud-based applications.

Another example is the growth of wireless service and location services. In the United States alone, roughly 91 percent of the population now has a wireless phone. The use of smart phones in the United States grew by roughly 51 percent from 2008 to 2009, and the sales of those devices are expected to eclipse earlier-generation cell phones by 2011. These phones multiply the use of online services, and they also provide new, unique, and informative data streams.

When a cell phone is on, a cell phone or other wireless devices are in constant communication with nearby cell towers. They supply information about the phone's whereabouts that is necessary to supply the cell service. And, as those phone deploy, many third-party applications providers are now developing innovative services that use location services in real time from carriers or from the devices themselves.

So cloud computing and the growth of wireless services and location services are just some of the wholesale changes in the ways that Americans use electronic communications. They signal a pervasive shift in the volume-sensitive information that we entrust to third parties. Clarity of rules is critical for successful deployment, development, and adoption of innovative services that have become part of the fabric of our society and our economy.

So I want to thank you for the Committee's decision to examine ECPA again. The administration stands ready to work with the Committee as you move forward. We do not come with proposals today, but we come ready to work to maintain the fair balance of reasonable law enforcement access, individual privacy protection, and clarity for service providers, for investigators, and for judges.

Chairman LEAHY. Of course, those are goals that we all seek.

Mr. KERRY. Good.

Chairman LEAHY. Now the hard part is how to fit it in.

Mr. KERRY. I would be happy to answer questions, Mr. Chairman.

[The prepared statement of Mr. Kerry appears as a submission for record.]

Chairman LEAHY. We want innovation, we want clarity, we want people to understand the rules, we want law enforcement to be able to use it, and we do not want to give up our ability to communicate with each other, especially as this has become not just a personal thing but it has become very much of a business-oriented thing.

Your whole statement will be part of the record. I do appreciate very much the offer of working with us because we did this in a bipartisan fashion before, and I expect to do it again as we update this.

In that case, we are very fortunate to have James Baker with us. Mr. Baker is the Associate Deputy Attorney General at the U.S. Department of Justice. He has worked extensively on all aspects of national security investigations and policies with the U.S. Department of Justice for nearly two decades. Am I correct on that? He has also provided the United States intelligence community with legal and policy advice for many years. In 2006, he received the George H.W. Bush Award for Excellence in Counterterrorism. For

those who do not know that, that is the CIA's highest award for counterterrorism achievements. He also taught a course in national security investigation and litigation at Harvard Law School and served as a resident fellow at Harvard University Institute of Politics.

Mr. Baker, please go ahead, and, again, your full statement will be put in the record, but please go ahead and tell us what you would like, sir.

STATEMENT OF HON. JAMES A. BAKER, ESQ., ASSOCIATE DEPUTY ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC

Mr. BAKER. Yes, thank you, Mr. Chairman. Mr. Chairman and members of the Committee, thank you the opportunity to testify today on behalf of the Department of Justice regarding ECPA. It is a pleasure for me to be here with our colleagues from the Department of Commerce, and as Mr. Kerry said, we are working closely with the Department of Commerce on ECPA reform.

I have just a few brief points that I would like to make in my oral remarks today and then respond to any questions that you might have.

For many years this Committee has been a leader in ensuring that our laws appropriately balance privacy and economic considerations with the Government's need to protect public safety and national security. As we have done regularly in the past, the Department looks forward to working with you again as you examine whether ECPA is properly calibrated to address all of these very important interests.

Although Congress has amended ECPA on several occasions since it was first enacted in 1986, the statute has proven remarkably resilient in its ability to keep pace with changes in technology. Many of ECPA's key concepts and distinctions remain fundamentally sound. Where changes have been necessary over the years, we have worked closely with you to ensure that those changes do not upset the delicate balance between individual privacy interests and the needs of public safety. It is essential that we do so again as we move forward.

In addition to getting the balance between privacy and security right, I would like to emphasize a few additional key points.

First, as some have mentioned, the Government relies heavily upon the legal framework that ECPA establishes to protect national security and public safety. ECPA is critical to our ability to effectively and efficiently conduct investigations of terrorists, gangs, drug traffickers, murderers, kidnappers, child predators, cyber criminals, and the whole range of criminal activity.

Second, it is vital that ECPA remain an effective and efficient tool for these investigations. In particular, it is essential that investigators have the ability under ECPA to obtain non-content information about a suspect's activities in a timely and efficient manner, particularly at early stages of an investigation. These types of information are the basic building blocks of our investigations, and if it is unduly difficult for investigators to obtain such data, it may hamper the Government's ability to respond promptly and effectively to these real threats.

For example, in a recent undercover investigation, an FBI agent downloaded images of child pornography and used an ECPA subpoena to identify the computer involved. Using that information to obtain and execute a search warrant, agents discovered that the person running the server was a high school special-needs teacher, a registered foster care provider, and a respite care provider who had adopted two children. The investigation revealed that he had sexually abused and produced child pornography of 19 children. The man pleaded guilty and is awaiting sentencing.

Finally, while we welcome the opportunity to work with the Committee as it considers whether changes to ECPA are needed, we urge you to approach that question with extreme care. It is critical that Congress carefully evaluate any proposed amendments to ensure that they do not adversely affect the ability of Federal, State, local, and tribal authorities to keep us safe from harm.

That said, I want to emphasize that the administration has not taken a position on any particular ECPA reform proposal to date, but we look forward to working with the Committee as it begins consideration of these important matters.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Baker appears as a submission for the record.]

Chairman LEAHY. Thank you very much, Mr. Baker.

We have overlapping concerns here. Let me begin first with Mr. Kerry. You obviously in your work with the Commerce Department understand how our privacy laws are affecting our economy. We are having all kinds of economic problems, and also so many businesses and individuals are using the Internet, e-mail, and everything else to improve their financial condition of their businesses and so on.

Does ECPA still remain important to our economy?

Mr. KERRY. Absolutely, Senator.

Chairman LEAHY. Press the button.

Mr. KERRY. OK. I am looking at the green light. Sorry. It does, Mr. Chairman. One of the important aspects of ECPA is the private rights of action that it creates, the expectations of privacy that it establishes as a matter of law, and the set of rules that it provides that providers as well as customers as well as law enforcement officials and judges and magistrates are able to follow.

Chairman LEAHY. OK. And those rules become confusing enough that it stifles innovation. I mean, even when this was written and everybody thought we were at the cutting edge, it looks pretty old-fashioned to go back to those days.

Mr. KERRY. Certainly the landscape has changed. There is no question about that. I think what Mr. Baker said about the adaptability of ECPA has proven true as well. I think this statute, Mr. Chairman, has proved more adaptable to changes in technology, for example, than the Communications Act. And I think we need to move carefully in how we change because there is a value in stability and predictability, in establishing a set of rules, a known set of rules that everybody can operate by, and certainly we need to look at unintended consequences.

So I think there are important questions about the application to cloud computing, to business models for cloud computing in the

VerDate Nov 24 2008 11:00 Jul 07, 2011 Jkt 066875 PO 00000 Frm 00011 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66875.TXT SJUD1 PsN: CMORC

ways both that customers entrust data and what providers are permitted to do with that data. But——

Chairman LEAHY. Well, when you go from the commercial part to another part—and I am going to be fairly careful in this next question for Mr. Baker because I do not want to go into classified areas. But you are well aware of some of the threats to our National security on cybersecurity.

Mr. BAKER. Yes, sir.

Chairman LEAHY. A lot of it has been in the press, and other parts we have been briefed on are pretty significant. So how do we keep the openness? I was talking about my wife and I e-mailing a friend in Europe back and forth, and it is like doing it from our BlackBerrys and so on, and you do not think anything about it. But you also have some major cyber threats that we face. 2702 tells how providers can voluntarily share electronic communications information with the Government, and you know that has been used. How does that impact the way the Government responds to threats to cybersecurity? And can that be improved?

Mr. BAKER. Well, Senator, I think you put your finger exactly on one of the key points with respect to cybersecurity. The main question is how do we appropriately share information regarding cybersecurity threats between and among the private sector entities that are involved and with those entities sharing it with the Government. That is exactly the right question.

ECPA lays out a framework for this, as do other laws, and so we need to make sure as we go forward, the laws we have are appropriate for today's circumstances with respect to cybersecurity. And when I am talking about cybersecurity in this context, I am talking not about necessarily pursuing a particular criminal investigation of an intrusion of a particular location. I am talking more about, sort of, defensive cybersecurity, and that is where I think some of the issues that you mentioned, the information sharing that ECPA does regulate, are critically important.

And so, obviously, we need to work closely together to make sure that whatever we do addresses our cybersecurity needs of today at the same time is appropriate and gives appropriate protection for the privacy of Americans.

Chairman LEAHY. But you also go into the area of NSL authority, and the Department seeks to expand its ability to get information, electronic information without a court approval.

Mr. BAKER. Well, Senator, what our objective is, our objective is to not expand what we are trying to obtain; it is, rather, to restore the status quo that existed before with respect to our ability to obtain information from providers. Some providers have raised concerns about the way the current statute is drafted. So we look forward to working with you to come up with something that is acceptable to everybody, but our intent is not to expand the scope of what we are doing but to enable us to get what we actually were getting for many years under the NSL authority with respect to this type of record.

Chairman LEAHY. Well, my time is up, but I will work with you and you could have your staff work with mine on this. I know that the way of obtaining information and what is available is a lot different from the days when I was in law enforcement. But also the

threats are a lot greater today, too. So we will work together on that.

Senator Cardin.

Senator CARDIN. Well, thank you, Mr. Chairman. Let me again thank both of our witnesses.

Let me try to get to some of the practical applications here. Several years ago, I visited an employer. It was a hospital that was a new building, implementing new technology at the time. And what they had, their employees all had to wear identification badges, which is not unusual, but that identification badge told the employer exactly where that employee was at all times. So that the hospital could locate the employee, know where the employee was, and provide a more efficient, effective health care for the people that entered the hospital.

I then met with representatives of the employees to see how they felt about that. And they generally were OK, but they said, you know, there are times when we should have privacy, even at work, and that the protections weren't clearly in place; that our employers would use it for management of health care or could be using it to get information about us that really was not appropriate for an employer.

So I raise the same question today with new technology where the Government can track pretty much where everyone is through the use of their cell phones. What protections do we have under ECPA so that I know the Government is not trailing me in private places? What standards are necessary? Is there a difference in regard to whether I am in a public place or a private place? What can you tell us about the current law does as far as protecting privacy, but yet allowing the Government to pursue real-time information that is necessary for law enforcement? And if you had to get a subpoena, does that hamper your ability to get real-time information that may become necessary?

So what are the tradeoffs here and how does the current law apply to a real situation that, I must tell you, does concern me?

Mr. BAKER. Yes, I will start with that one, if that is okay. There are several different parts of your question. So the first thing was that you raised the prospect or the issue with respect to private entities collecting this data and what they——

Senator CARDIN. I used that as an example. I am concerned about Government.

Mr. BAKER. Yes, because what ECPA focuses on, what we are focused on is the interaction between—or the ability of the Government to obtain information from the private sector in certain circumstances.

Senator CARDIN. I am just using that as an example of how technology has changed.

Mr. BAKER. So the basic idea is with respect to the kinds of information you are talking about with respect to cell phones, when you are talking about cell phone records, first of all, just to be clear, my understanding of the technology—and it is changing over time, but, you know, currently it is not pinpoint accuracy with respect to where a person——

Senator CARDIN. And I expect that will change over time.

Mr. BAKER. As the technology develops, it may, Senator. But currently, and at least in the immediate future, it gives you a rough geographic location of where a person is. It does not tell you exactly where they are in a particular building, for example. So——

Senator CARDIN. I do not want to get too technical. I asked that question to some of the experts, and they tell me by looking at the different cell phone towers, you can pinpoint pretty closely to where people are today.

Mr. BAKER. I think, again, it depends if you are in an urban area, a suburban area, a rural area, things like that. But I take your point, Senator.

But just to make clear, when the Government wants to get historical cell site information which is critically important for our investigations to find where someone is, for example, in a kidnapping case, a murder case, a terrorism case. These are all critical examples of where we need location information in certain circumstances. We need to get a court order of some sort. It is under a couple of different particular provisions of ECPA. It is a showing of specific and articulable facts, giving reason to believe that the information is relevant or material to a lawful investigation. That is for historical information and for some of the prospective information. With respect to the prospective information, we combine an order like that with a pen/trap order. So, in other words, to get that kind of information, we do have to go to a court. It is not a probable cause showing, clearly. It's lower than that. But we do have to go to a court.

Senator CARDIN. And that is not hampering you from getting timely information?

Mr. BAKER. I'm not going to say that in any investigation ever that it has never hampered us or slowed us down, but I think we are able to work effectively in the existing legal regime in order to obtain this kind of information.

Senator CARDIN. One more very quick question, Mr. Chairman.

As I understand the current law on e-mail communications, it has some distinctions between the age—whether it is on your home computer or centrally stored, whether it has been opened or not opened, which may have been relevant in the 1980s, which is no longer relevant today because e-mail is very comparable to our traditional letters. Is there any reason for the distinction on the standard necessary for the protection of e-mail communications?

Mr. BAKER. Well, Congress did make the judgment, as you reflect, back in 1986, and since then to differentiate between where a particular e-mail is, how old it is, who has access to it, is it stored as a third-party record, has it been opened yet, in other words, has the transmission been completed. So the administration has not—I mean, that is the law today, but the administration has not taken a position on changing that at this point in time, but we look forward to working with you on that.

Senator CARDIN. Well, I appreciate you dodging the question, and I understand—if there is a rationale, please let us know the rationale. I am trying to figure out a rationale for—I understand back then——

Mr. BAKER. I think——

Senator CARDIN.—e-mails were looked at a lot differently than they are today. We thought they could not be stored forever, and we now know they can be stored forever. So it is——

Mr. BAKER. Well, and I—Senator, I am sorry.

Senator CARDIN. No.

Mr. BAKER. I was just going to say, I mean, I think the law—in a number of different ways, the law differentiates between records that we store in our home, truly in our home, and records that we store with third parties. It makes distinctions in lots of different ways, and it differs depending on whether it is in——

Senator CARDIN. But don't you think we will be storing almost everything in third parties in the near future? As you pointed out, cloud computing is becoming the norm, not the exception.

Mr. BAKER. Well, the consumer, individuals, businesses have to make a determination whether storing something in a cloud is advantageous to them for a whole variety of reasons, including whether it is secure—I mean, not just from the Government but from malicious actors. Issues have been raised with respect to that. Privacy issues, efficiency, accessibility to data, all those kinds of things are different items that folks have to work with.

Senator CARDIN. [Presiding.] I appreciate it. I did not realize that I was temporarily holding the gavel. I could have gone on for a lot longer.

Senator Franken.

Senator FRANKEN. Thank you, Mr. Chairman.

Mr. Kerry, I know that you said that you are not here to make recommendations, and I kind of heard that from you, too, in what I think the Chairman fairly characterized as an evasion. But you guys really have clearly given this stuff a lot of thought. That is kind of your job. So I am going to ask you to ruminate here a little bit. What are the hard choices here that we are going to have to make? This is for both of you or either of you. Could you give me an example of what you might think would be a tempting but unwise change in ECPA? And what is a change we might make that is wise but is not obvious at first blush?

Mr. KERRY. Well, Senator Franken, thank you. We have not gone through all of the thought process that we need to go through as an administration to answer all of those questions concretely. But let me address one about the difficult choices, and it goes back to Senator Cardin's question. It is how the law should apply to location services and location information.

ECPA and the body of laws that it operates on draws a fundamental distinction between content information and non-content information. Interception of content, disclosure of content are subject to higher standards. Location information does not fit the—is not content of communications. Does it necessarily fit within the non-content construct?

As Senator Cardin indicated in his discussion of his experience in the hospital, there are different sets of expectations, depending on the circumstances of the location information, depending on the amount of that information. And I think there is a——

Senator FRANKEN. Can I give you an example? I am sorry to interrupt, but in February, Newsweek reported that police officers in Michigan had requested cell phone—you are talking about loca-

tion—cell phone location data for a group of people congregating for a labor protest. The officer said they were doing it to stop a possible riot. Now, what protections, Mr. Baker, would you say are in place to prevent this sort of thing from happening? I am sorry, but since you brought up location, this seems to be a place where maybe abuse of the location is there.

Mr. BAKER. Senator, I do not know the particulars of that particular investigation, but they should have been—in order to obtain that information, they should have gone to a court. They should have had to articulate what their reason was for wanting that information, and they should have had a legitimate law enforcement purpose to obtain that. If they had some other purpose that they did not say, that they were not up front about, or whether, you know, they covered up exactly what they were doing, I have no way of knowing. But that is more of a question, I think, of the legitimacy of the investigation as opposed to the particular authorities or predication required for obtaining that kind of information.

Senator FRANKEN. OK. And there are different levels of authority. Sometimes you need a warrant. Sometimes you need a subpoena. Sometimes you need a super warrant.

Let me give you an example. Let us say I use Outlook and you use Gmail. I send you an e-mail and you read it. In most circuits, the Government would need to get a warrant to get the e-mails stored on my computer in my Outlook sent messages folder. They actually have to go before a judge and show probable cause that they need this e-mail to investigate a crime. But if the Government does not have probable cause, they can get the e-mail from your Gmail because it is stored remotely in a cloud. They do not need a warrant for that. They can issue a subpoena for that all by themselves.

Do you think that the probable cause standard is weakened when it is so easy to get an e-mail without a warrant?

Mr. BAKER. Senator, I guess I am not sure that the probable cause standard is weakened with respect to the ability to obtain the communications from—I assume your computer is at your home. That is why we need a warrant to get it. I am not sure it is a question of probable cause. I would suggest that it is more a question of whether collectively everyone thinks that the balance between law enforcement interests and privacy is appropriate in that circumstance. And that is one of the things that we do not have a position on. I know it may seem evasive, but we just do not have a position yet on that because we have not finished our review of that.

But in any event, I take your point. I understand the difference. There is a difference, and, again, the law recognizes, and has for a long time, differences when information is stored with a third party than when it is stored in your home.

Senator FRANKEN. OK. I am out of time, but, Mr. Kerry, I did interrupt you, and I wanted to know if you wanted to finish your response.

Mr. KERRY. Thank you, Senator. I think I conveyed the main sense of my response.

Senator FRANKEN. OK. Thank you both.

Thank you, Mr. Chairman.

Chairman LEAHY. Senator Klobuchar.

Senator KLOBUCHAR. Thank you very much, Mr. Chairman. Thank you to both of you. It is good to see you.

As a former prosecutor, I listened to this and I think of my old job. Every day we would be balancing that. One day I would be authorizing a wiretap and sitting in on it, and the next day protecting victims' sensitive information from getting out on the Internet. And just recently, we have been working on two issues in our office that are examples of how we have to update the laws to be as sophisticated as the crooks that are breaking them. One is the cyber stalking that has now become a trend of offenses, as illustrated by the ESPN reporter who got filmed in her hotel room and then it was put out on the Internet. And then the other one was just the one that Chairman Leahy has been leading and a number of us working on it, pirated entertainment that has been sold not just on DVDs but also on the Internet. And the criminal laws are not updated to keep pace with what is happening with what the criminals are basically doing.

So I think this is always a balance, and I guess my first question would be of you, Mr. Baker, and that is, you talked about how we should proceed cautiously when making changes to ECPA, and you mentioned that you do not want us to change the Electronic Communications Privacy Act in a way that would delay law enforcement's ability to access time-sensitive data. And I thoroughly believe in doing things for privacy, but at the same time I know when these crimes occur and there is some madman out on the street, people want to be able to locate him.

So are there changes you think that could be made to ECPA that would make it easier for law enforcement to access information while at the same time protecting our privacy concerns?

Mr. BAKER. Well, at the risk of saying the same thing again that has gotten me in trouble so far, we just——

[Laughter.]

Senator KLOBUCHAR. Try it with me.

Mr. BAKER. We have not finished our—we simply have not finished our review of that. We are looking at them closely, at the various proposals that have been put forward. One of the difficulties right now, frankly, is that we do not have statutory language to actually look at and evaluate. And our experience is that getting these words exactly right—I mean, I have an amazing group of lawyers sitting behind me who are experts in this area, and they spend lots of time trying to understand and prognosticate about if you change this word, what impact is it going to have on our investigations, our ability to locate the kind of people you are talking about.

So, unfortunately, we do not have a position on the reforms today to put forward, but all I would say is to echo what you say. It is very important that we get this right, and we just have to do it carefully.

Senator KLOBUCHAR. You talk about the real-time mobile phone location information. What level of scrutiny is required to get that? And is it the same as GPS information that we now can get?

Mr. BAKER. It is not the same as GPS. So with respect to the cell site information, which, again, is less precise than GPS, you need

to go to court, you need to get an order. It is not a probable cause order. It is less than that. But, nevertheless, you need to get an order.

When you start talking about latitude and longitude, locating type of information, then you are talking about the need to get a warrant because it can reveal that you are in a constitutionally protected location, such as your home, and moving about, let us say, in a home and being able to figure out exactly where you are. So there are different standards depending on how precise the information is that the technology reveals.

Senator KLOBUCHAR. And does that make sense to you? Do you think there could be changes to that? Or do you want to wait until——

Mr. BAKER. Again, we are working on that, but it is a distinction that the law recognizes in other areas as well.

Senator KLOBUCHAR. And then also we talked here about that 180 days with the e-mail protection, with the open e-mail. Does that still make sense to you? Are there privacy concerns there with how that is working?

Mr. BAKER. Well, again, we are looking at that. We are working on it. We understand—I mean, we understand the privacy concerns. We hear what folks are saying, and I have met personally with the DDP Coalition, had a very fruitful discussion with them, and it was very illuminating to me. So we understand all of those concerns, but, again, our position is if changes are to be made, then we just have to get them right.

Senator KLOBUCHAR. OK. Mr. Kerry, I know in your testimony you talked about the clear distinction between content and non-content information at the heart of ECPA. How has technology blurred that distinction?

Mr. KERRY. As new data streams become available, in part the volume of data—location information being one example—provides additional information about consumers' activities that may provide information that begins to make a portrait that is more than just the sort of identity information of a pen register or of transaction records. Certainly when you get to Internet searches and you go beyond simply a URL, that becomes content. So these are areas where those boundaries begin to blur because of the volume of information that becomes available from a host of data streams and there becomes more and more capability of capturing and of analyzing that data.

Senator KLOBUCHAR. I just noted one last thing, that Secretary Locke held a privacy and innovation symposium this year, and I am sure we can get that information from your staff. I head up the Subcommittee on Innovation for Commerce, and obviously in Commerce this is an overlap between these two Committees. We have focused on these privacy issues as well. Did anything come out of that that would be helpful? Or do you want to just send it to us?

Mr. KERRY. We have a number of streams of work that are coming out with that. We are actually collating and drafting a report, a discussion draft of some of the work that comes out of the privacy inquiry and have other inquiries on free flow of information, intellectual property, cybersecurity that are already—I would be happy to share that with you.

VerDate Nov 24 2008 11:00 Jul 07, 2011 Jkt 066875 PO 00000 Frm 00018 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66875.TXT SJUD1 PsN: CMORC

Senator KLOBUCHAR. Are you looking at how innovation and new methods are sort of butting up against privacy concerns or how we can use new technology to get at privacy concerns?

Mr. KERRY. Both of those, Senator. We are looking at really—in parallel to the balance that ECPA strikes in the law enforcement context, the balance between innovation, competition, the global free flow of information, and privacy and security.

Senator KLOBUCHAR. OK. Thank you very much.

Mr. KERRY. Thanks.

Chairman LEAHY. Thank you. Anything else for this panel?

[No response.]

Chairman LEAHY. OK. Gentlemen, I appreciate this. I may have a couple other questions for the record, but I would ask both of you and your staffs to work with us as we try to put together an updated ECPA. I think we know we need that. We just do not want to throw the good out with the bad as we do it. Thank you both very much.

Mr. KERRY. Thank you, Senator. We will look forward to doing that.

Chairman LEAHY. Thank you. And then the staff can set up for our next panel.

Chairman LEAHY. For our next witnesses, first will be James Dempsey who currently serves as Vice President for Public Policy at the Center for Democracy and Technology. Prior to joining CDT in 1997, he was Deputy Director of the Center for National Security Studies, previously served as assistant counsel to the House Judiciary Subcommittee on Civil and Constitutional Rights, concentrating on oversight of the FBI and privacy and civil liberties; former associate in the law firm of Arnold and Porter in Washington; former clerk of Judge Robert Braucher of the Massachusetts Judicial Court; graduate of Yale, law degree from Harvard. He is somebody who has testified here before this Committee numerous times.

Mr. Dempsey, good to have you back, sir. Go ahead, please. And, again, all witnesses' full statements will be made part of the record.

STATEMENT OF JAMES X. DEMPSEY, ESQ., VICE PRESIDENT FOR PUBLIC POLICY, CENTER FOR DEMOCRACY AND TECHNOLOGY, SAN FRANCISCO, CALIFORNIA

Mr. DEMPSEY. Chairman Leahy, Senators, good morning. Thank you for holding this hearing today.

In setting rules for electronic surveillance, we must balance three critical interests: the individual's right to privacy; the Government's need to obtain evidence to prevent and investigate crimes, and the corporate interest in clear rules that provide confidence to consumers and that afford the companies the certainty they need to invest in the development of innovative new services.

When it was adopted, ECPA well served those interests, thanks in large part, Mr. Chairman, to your leadership and to the willingness of companies, privacy advocates, and the DOJ to work together to develop a balanced solution.

Today, it is clear that the balance has been lost. 1986 was light years ago in Internet time. Powerful new technologies create and

VerDate Nov 24 2008 11:00 Jul 07, 2011 Jkt 066875 PO 00000 Frm 00019 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66875.TXT SJUD1 PsN: CMORC

store more and more information about our daily lives and permit the Government to conduct surveillance in ways or at a depth and precision that were simply impossible 24 years ago. It is those new capabilities that need to be addressed.

ECPA has been amended in at least 18 statutes since 1986, but almost all of those changes were at the request of the Justice Department, not in response to privacy concerns. Almost all of them expanded Government access to information. There has never really been a comprehensive look at the statute since 1986.

Consequently, there are a few elements of ECPA that no longer comport with the way people depend on this technology in their personal and professional lives. E-mail, which a number of Senators have cited, is an egregious example. The same e-mail is subject to a judge's warrant one second and is available with a prosecutor's subpoena the next. An open e-mail is covered by the warrant in the Ninth Circuit, and it is available without a judge's approval in the rest of the country. Draft documents, calendars, address books stored online are all available with a mere subpoena regardless of age.

What is perhaps most important to recognize about the e-mail standards is that they are constitutionally vulnerable. Orin Kerr, a scholar well known to this Committee, has concluded in his latest article that ECPA is unconstitutional to the extent that it permits access to e-mail content without a warrant.

The rules are also illogical and possibly unconstitutional with regard to cell phone tracking data. The Justice Department itself believes that it is best to use a warrant to use GPS to track someone. However, the cell phone companies have been making their cells smaller and smaller and have begun offering mini cells, which are basically a cell tower for your home or for your office, making tower data as accurate as GPS in some cases.

Earlier this year, a diverse coalition was launched calling itself Digital Due Process. The coalition said that ECPA needs to be updated to provide full warrant protection to all e-mail content and to location tracking data, subject to exceptions for emergencies and cybersecurity and other exceptions.

The breadth and diversity of this coalition speaks volumes. It includes not only CDT and ACLU, but also major Internet and communications companies: AOL, AT&T, Microsoft, Google, eBay, Salesforce. It includes conservative and libertarian groups: ATR, Americans for Tax Reform; FreedomWorks; libertarian think tanks. Individual supporters include former prosecutors, former members of the CCIPS unit at DOJ. All are saying that the current system is crazy; it just does not make sense anymore and needs to be reformed.

Now, it is very important to appreciate the modesty and reasonableness of this coalition's proposals. A fundamental premise of our recommendations is that it is necessary to preserve the building blocks of criminal investigations. Under our principles we would continue to authorize the use of subpoenas to get stored meta data on telephone calls; that is, the dialed number information. We would continue to permit the use of subpoenas to get subscriber identifying information. We would not change the standard in Section 2703(d) of the statute for getting transactional data regarding

Internet communications. We would preserve all the current exceptions, including the emergency exceptions, which allow interception without a warrant or without even a subpoena. We would preserve the current cybersecurity exceptions. We would not propose any changes to FISA or to the National Security Letter provision. We do not propose changing any rules on getting information directly from the subject of an investigation. So the FTC and the SEC could continue to use subpoenas to get documents from companies under investigation. We have focused on a very few of the most salient problems: the e-mail content issue that a number of Senators have referred to, and the location tracking question.

Now, our proposals are just a first step. The process will require further dialog, the engagement of other stakeholders, and, most importantly, a dialog and discussion and compromise with law enforcement agencies and understanding their positions.

We want to be careful in our amendment of ECPA to avoid collateral damage. We want to be incremental. We are not proposing a general overhaul of the statute. We cannot fix everything. We want to preserve the efficiency and speed and the building blocks of investigations.

But, together, with dialog, with an understanding of the technology and the way it has changed, we can reestablish the goal that ECPA had in 1986: to balance law enforcement, privacy, and business interests.

Thank you. I look forward to your questions.

[The prepared statement of Mr. Dempsey appears as a submission for the record.]

Senator CARDIN. [Presiding.] Thank you very much, Mr. Dempsey.

We will now hear from Mr. Brad Smith, who is the Senior Vice President and General Counsel, Corporate Secretary, and Compliance Officer for Microsoft. He leads the company's Legal and Corporate Affairs Department and is responsible for its legal work, its intellectual property portfolio, and its government affairs and philanthropic work.

Mr. Smith.

STATEMENT OF BRAD SMITH, ESQ., GENERAL COUNSEL AND SENIOR VICE PRESIDENT, LEGAL AND CORPORATE AFFAIRS, MICROSOFT CORPORATION, REDMOND, WASHINGTON

Mr. SMITH. Well, thank you, Senator Cardin, Senator Franken. I very much appreciate the opportunity to be here this morning to offer just a few thoughts to introduce some comments on this topic.

First, not surprisingly, those of us in industry are very enthusiastic about where we think the next generation of computing is going to take us. As we build data centers, as more and more software and information move to the so-called cloud, we make it cheaper for small businesses to implement computing solutions; we make it easier for them to create new jobs; we create more powerful tools for them to reach consumers in new ways; we create new ways for individuals to communicate and interact with each other. There is a lot of good that we see in the new technology that is being created.

VerDate Nov 24 2008 11:00 Jul 07, 2011 Jkt 066875 PO 00000 Frm 00021 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66875.TXT SJUD1 PsN: CMORC

If we are going to go forward and if we are going to go forward successfully, we need the right kind of legal rules in this field. And I think that means three things: First, we want to ensure that the law continues to be balanced—balanced between the rights of citizens and the needs of Government with respect to law enforcement. We need some certainty so that when those of us in industry are designing this technology we can do so with some confidence about how the law is going to be applied to it. And we need some clarity. I might say we need most of all clarity for consumers, for citizens, so that they can understand what their rights and obligations may be.

Listening to this debate on this issue, listening to this hearing this morning, there is obviously a first question, which is: Does the law, does ECPA itself need to be updated. Personally, I listened to that, and I am reminded of the story of the emperor who was walking down the street in the parade. This emperor has lost some of his clothes. And I think we need to recognize that. People may be reluctant to say it until they know exactly how they want to knit the next suit. But the truth is the first step in knitting the next suit is to recognize that the current one is increasingly tattered, and we really do need to roll up our sleeves together and dig into the kinds of questions that are important.

The reality today is that ECPA increasingly falls short of a common-sense test, not because the law was flawed when it was written in 1986, but because technology in some cases—not every case, but in some cases—has simply passed it by. Why should e-mail in somebody's inbox be subjected to a different standard than e-mail in somebody else's sent mail folder? That is the question posed by Senator Franken. Why should e-mail that I move to my junk mail file and choose not to open be subjected to a higher level of privacy protection than an e-mail I receive and decide to read? That is hard to square with common sense.

As we sit here in September, why should e-mail that I sent in early March be entitled to less privacy protection than e-mail that I sent in early April because of the 180-day rule?

Technology really is moving forward. It is continuing to move forward, and we do need the law to catch up. There is no substitute for action by Congress. I think that much has become abundantly clear. We are talking about rights of Americans, fundamental principles that have their roots in the Fourth Amendment to the Constitution. But the reality is that the Supreme Court earlier this year basically signaled that it is not likely to move quickly.

In the *Quon* decision, there was one sentence that stood out above all else, and I think that sentence speaks to it today. The Court said, "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."

There is a lot of wisdom in those words. But they are also discomforting because it takes time for the role of new technology in society to become clear. And there is a certain risk that by the time that role becomes clear, the technology will be well on the road to becoming obsolete. It will be replaced by something else. And if that is the case, then the Fourth Amendment will never really

VerDate Nov 24 2008 11:00 Jul 07, 2011 Jkt 066875 PO 00000 Frm 00022 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66875.TXT SJUD1 PsN: CMORC

catch up, and we must look to Congress to fill the gap. Congress did that in the 1980s. Congress needs to do that again today.

In closing, I am reminded of the advice offered recently by famous basketball coach John Wooden. He said, "One of the important things to do in life is be quick but do not rush." We do need to be quick. We should not rush. We should use hearings like this to sort out the issues. But we do need some decisions to be made because if they are not, then we are going to find that some new issues are going to emerge and there is going to be a lot of pressure on everybody to rush far too quickly.

Thank you.

[The prepared statement of Mr. Smith appears as a submission for the record.]

Senator CARDIN. Thank you, Mr. Smith.

Our next witness is Mr. Jamil Jaffer. Mr. Jaffer is a private attorney in Washington, D.C. From 2008 to 2009, Mr. Jaffer served as an Associate Counsel to President George W. Bush. Prior to that appointment, he served in several senior positions within the Department of Justice, including counsel to the Assistant Attorney General for the National Security Division and Senior Counsel for National Security Law and Policy.

Mr. Jaffer.

STATEMENT OF JAMIL N. JAFFER, ESQ., ATTORNEY, WASHINGTON, DC

Mr. JAFFER. Thank you, Senator Cardin. I would like to thank the Chairman and the Ranking Member for inviting me here today. I would like to actually take on Mr. Smith's remarks and take the advice of John Wooden. I am a UCLA graduate, so I will also try to be quick but not rush.

I would like to address three items briefly today in my oral statement: first, the threat that we face and the use of these tools by the Government; second, briefly touch on the law in this area; and then, third, suggest a path forward for Congress to consider.

First, with respect to the threat, today we face an increasing threat stream from cyber actors, whether they be cyber criminals, child predators, or national security threats: whether they be terrorists or foreign intelligence operatives. Cybersecurity is critical. I know this; in the Government I worked on the Comprehensive National Cybersecurity Initiative, which has now been partially declassified by the Administration. We are engaged in an effort, an ongoing effort, to protect both Government and private networks from these cyber threats. And the tools provided by ECPA play an important role in allowing the Government to assemble the key building blocks of investigations in this area. They help ferret our child predators who hide out in virtual communities. They help ferret out virtual terrorist caves. They help ferret out virtual gang hideouts on the Internet.

They also help find the people who inhabit these virtual hideouts on the Internet, and it is important to remember that the key tools in ECPA, the non-content tools, are the ones that really form the building blocks. And with respect to those non-content tools, the Fourth Amendment does not the use of those tools. As a general matter, the Supreme Court has held that the Fourth Amendment

does not protect information that you give to third parties. That is because you always run the risk that a third party is going to be a Government agent and is going to hand over the information to the Government, whether voluntarily or otherwise. And with respect to non-content data—your dialed number data, who you send e-mails to and from—that information generally also is not protected by the Fourth Amendment because you provide it to a third-party provider to route your data. And that has been the case since *Smith* v. *Maryland* in the 1970s.

And so this is not new law. This is not a change in technology. It is simply what the Fourth Amendment protects.

Now, Congress very wisely decided that is not enough. What the Fourth Amendment offers is not enough. We need to provide statutory protections to ensure that the privacy interests of Americans are protected. In doing so, though, Congress decided that it was important to balance security on the one hand, and privacy on the other, and ECPA is an example of that. A lot of times you will hear today: ECPA does not make a lot of sense. The 180-day rule does not make sense. The opened e-mail rule does not make sense. But these rules are not a product of any constitutional decisionmaking. They are, fundamentally, the compromise that Congress struck in enacting additional privacy protections-beyond what the Constitution-provides in statute.

Now, Congress can and should consider revisiting those privacy protections, but in doing so, it is important to think about is this balance that you heard about on the first panel. And in thinking about that balance, we really have to consider whether, at a time when these cyber threats are dramatically increasing, at a time when cybersecurity is crucial and Congress is considering how to provide tools in industry—and I do not think the answer is regulation of industry; I think the answer is providing tools to allow the Government to share information with industry about cybersecurity threats—does it really make sense to raise the bar on the Government in protecting in the security of American citizens? It may make sense, but Congress needs to do it in a very careful, limited way.

Now, as far as the path forward goes—and I see my time is almost expired—I think the right path forward is as follows:

First, there are consensus things that industry, the Executive Branch, and the Congress can agree to in the very near future about how to fix ECPA. You can make ECPA easier to use for industry. You can make it clearer. You can make it more consistent. One of the fixes you could consider is how the definitions of the various types of providers can be harmonized and made one, because the fact of the matter is that providers today in the cloud computing environment, provide multiple sources, not just e-mail transmission and delivery; they also provide remote computing services. You can harmonize these definitions.

You can also provide industry with clarity about what it can and cannot provide to the Government, and when it can and cannot provide information to the Government; and you can make it a lot clearer than it is today. This does not mean you have to change what the Government can get and how the Government can get it,

but you can provide clarity. That I think can be done in the next session of Congress without a problem.

With respect to the larger changes, some of the changes proposed by the coalition that is out there today, as well as others, about raising the requirements on the Government, in terms of what they might get and how they might get it, those need to be considered very carefully, particularly in light of this growing threat stream.

With that, I appreciate the opportunity to present my views, and I am happy to take questions.

[The prepared statement of Mr. Jaffer appears as a submission for the record.]

Chairman LEAHY. Well, thank you, and thank you for telling me what we in Congress intended to do when we wrote the legislation. As one of those who was there when we did it, it is always good to be told what we were doing and what we were compromising by even if it was somebody who was not there.

I do agree with you that we have got to have a balance that allows us to protect law enforcement and allows us to protect individual liberties and allows us at the same time to have the innovation we need.

Let me go first to Mr. Dempsey. I commend you and the Center for Democracy and Technology for being such persuasive voices in trying to update ECPA, and I appreciate the work you have done in trying to get some diverse voices together on this.

But with your proposal, how would that improve, on the hand, digital privacy but also protect law enforcement and make sure it has the tools it needs to investigate crime?

Mr. DEMPSEY. Mr. Chairman, one thing we were very careful to do in our process here was to focus on preserving the building blocks of investigations. That is, there is some data that is appropriately available with a subpoena: the subscriber identifying information, the telephone dialing information. There is other information, as you go up the ladder, so to speak, where a court order is required, but on less than a finding of probable cause, on less than the constitutional type standard, and we preserve that. And then, clearly, when you get to the top of the stack, so to speak, when you get to the content, that should be protected by the warrant.

Now, right now the courts are struggling with this. As Mr. Smith said, they are not making much progress, but they are casting a lot of uncertainty over the field. Courts are letting some information in, letting it out, granting orders, denying orders, vacating opinions where they came to one conclusion or another.

I think one of the major benefits to law enforcement is the certainty and the clarity. If you leave this to the courts and then evidence gets thrown out, you get all the way through the investigative process and evidence gets thrown out, that is the worst that could happen to the prosecution. If you bring it within ECPA, you have your exceptions, you have your requirements on service providers to cooperate, you have your rules on immunity, your rules on compensation, your rules on how the information can be used. As the Justice Department has said, those are very important rules.

Chairman LEAHY. And so you believe that we can do this and write it in such a way that it would be upheld? Mr. Jaffer has spo-

ken about it in the next session of Congress, although I—and I agree with you, it could be. I also wish—and I am sure you do, too—that we could do it in this session of Congress. But this has been the most dysfunctional session of Congress I can remember. That is just a personal view, but from one who has been here 36 years. But tell me, Mr. Dempsey, can we do that? This is the most difficult thing. I think——

Mr. DEMPSEY. I think we can——

Chairman LEAHY. I think we have a bipartisan coalition on this, but we also want to make sure we have something that is going to be upheld by the courts.

Mr. DEMPSEY. Well, I think that one motto here is to work incrementally. Do not try to solve everything at once. Do not try to disrupt anything that does not need to be fixed or to which we are not sure of the answer.

As Mr. Baker said, it is going to be important to start looking at some legislative language because you really want to make sure you are not having those unintended consequences.

Chairman LEAHY. Well, let us take a specific one. The Department of Justice proposed that we amend Section 2709 to make it easier for the FBI to obtain electronic transaction records. How do you feel about that?

Mr. DEMPSEY. Well, first of all, I think that that is a perfect example of how we are taking a change without considering the other aspects of the statute that might be implicated. And with the Justice Department change, there is a kernel of logic to what they are saying here, and there is a problem with that provision of the statute.

The trouble is the Justice Department has been unwilling to come forward and define for that purpose the key term in the statute, "electronic communications transactional records," which is a very broad term.

Now, if you look in 2703 of the statute on the criminal side, Congress has actually drawn some lines, and I think those are good lines that were drawn in terms of what should be available with a subpoena or its equivalent, the National Security Letter, versus what should require a court order. And I think until the Justice Department is willing to give definition to that term, which is a very broad term, "electronic communications transactional records," I do not think we can move forward on that 2709.

Chairman LEAHY. I suspect they will be listening to what you said here today.

With my colleagues' permission, I will just ask one more question. My time has expired.

I know with Mr. Smith here and Microsoft are doing a great deal to protect information and privacy, and you have called for—the company has called for stricter privacy protections in so-called cloud computing. Can ECPA reform help that?

Mr. SMITH. I definitely think, Senator, that the updating of ECPA fits into a larger set of issues that it is important for Congress to address. As we look to the future, we really think that there are three areas of the law that are related that need attention. One relates to privacy, and part of the privacy issue involves ECPA. Another part of the privacy issue involves ensuring trans-

parency and clarity for what service providers do with customer information. So we believe that it would make sense to take action there.

Second, we think that it is important to take new steps with respect to security. We believe that law enforcement needs new tools to be able to prosecute computer crimes. We believe that service providers, such as ourselves, should have new tools to help protect our customers against computer crimes. So that is the second area.

Third, we believe new steps are needed across borders. Information moves from country to country in such a way today that in truth one cannot rely with confidence on the expectation that only a single country's law will be applied to a single piece of information. So we do need some new international frameworks and some new international cooperation as well.

Chairman LEAHY. I agree with that. I am just trying to figure out how we write it in such a way that it would take care of the problem of the moment and not create new problems as technology changes a week down the way. I go back again to the Earl Warren statement I made at the beginning of the hearing. And we will work with you on that flexibility. That is why what all three of you have been saying here has been so important.

Senator Cardin, and I apologize for taking extra time, but I wanted to hear what Mr. Smith had to say on that.

Senator CARDIN. Well, thank you, Mr. Chairman. I thank all three of our witnesses.

Mr. Jaffer, let me first say that I agree with you that the threats against this Nation are real, particularly as it relates to cybersecurity. We have conducted some hearings on cybersecurity, and the challenges are certainly very serious and very difficult. But I must tell you, I strongly believe that having the appropriate safeguards on law enforcement on getting information makes us safer because then our resources are used more effectively. And we are not flooded with information that has limited value, but that we really are focusing on the threats. I think it makes law enforcement stronger rather than weaker if you do it right, and that is, of course, what we are trying to do here.

Mr. Smith, I want to ask you a question about technology. Are there any cautionary notes that we should be aware of as we look at this statute and modifications of it, that we do not have unintended consequences hampering the development of new technologies that are important for this country?

Mr. SMITH. I think that is a very good question, Senator Cardin. I think there is fundamentally a risk in Congress doing too much and there is a risk in Congress doing too little. I think the definition of doing too much would be to deal with issues before we have some confidence about how we really should address them as a country, and I think that Mr. Dempsey pointed us in the right direction when he said there is real value in incrementalism.

The truth is any law that can go 24 years before people come here and say it needs some updating passes a pretty high bar. I think that if we can look to Congress to take steps once a decade and solve the problems immediately before it, that is a good thing. And if one tries to go farther than that, one does risk creating unintended consequences.

I would say the flip side of the coin would be doing too little because the law at this point is clearly in need of some improvement.

Senator CARDIN. That is good advice. I thank you, Mr. Smith.

Mr. Dempsey, let me ask you a question about how we can anticipate change. I know we do not know what technology is going to look like 10 years from now, but we know it is going to be different. We know that information exchanges are going to take place in a much more timely way.

Is there anything we can do in a statute that protects us with new technologies so that law enforcement can get the information they need and privacy is protected, knowing full well what the Chairman said, that Congress does not always act quickly. Sometimes it takes us a while to get to where we need to be. Is there anything, any advice that you might have for us as to how we draft changes that can at least protect us during transition as new technologies come effective?

Mr. DEMPSEY. Yes, I think that is an excellent question, and I think there are two ways to approach that. One is to look at what are the broad trends, and I think we can identify some—what seem to me to be—pretty inexorable trends in technology that are going to dominate innovation over the next decade, let us say. One would be the cloud; that is, the movement of data off of local servers onto interconnected, Internet-based servers, and that is supported by ubiquitous broadband. It is supported by cost-efficiency reasons why you would do that. The data in the cloud in some ways may actually be more secure and backed up and better protected than the data stored locally. There are a lot of drivers pushing in that direction, and I think so much of the data that we used to hold locally in the office, in the home, on the laptop, on the personal device, the handheld device, is moving into the cloud, and that is where things are going to go. That is why we focused on that as one of our recommendations.

The other major trend, I think, is mobility and the power of that handheld device and the way it can support location-based services and the way that that location data is becoming more and more precise—the map services and the friend-finder services and a whole host of other services that build on—when you see services building on a technology, you can be pretty sure that that is going to represent a significant trend. So that is why of all of the non-content data, if you think of location data as non-content, of all the non-content data, that is one that sort of pops out immediately as this is just not dialed number information, this is just not who is making a phone call. This is very pervasive, very precise, very different from anything we have ever seen before, really.

Another major trend is social networking, obviously, and the social networks are becoming platforms not only for posting photos but for one-to-one communication, real-time communication, et cetera. Those are already included, I think, in ECPA. It maybe would be interesting to pose that question to the Justice Department to make sure they agree. I think those platforms do fit within the statute.

So of the three trends, although a lot of that stored data currently falls outside of the warrant protection, even purely private stuff, the way the definitions work in the statute now. So I think

those three trends look to me as pretty reliable and certain trends, and if we build around those, we sort of know where we are going.

Senator CARDIN. Thank you. I appreciate that answer, and I really do appreciate all three of your testimonies.

Chairman LEAHY. Thank you very much.

Senator Franken.

Senator FRANKEN. Thank you, Mr. Chairman.

Mr. Smith, I was very glad to hear your answer to Senator Cardin's question about essentially responding to the "be quick," because I was worried there that you are basically saying that to keep up with the technology, Congress would have to double the speed that it legislates every year.

[Laughter.]

Senator FRANKEN. And I think that would be highly unlikely. The once-a-decade sounds about right on this.

[Laughter.]

Senator FRANKEN. And Mr. Jaffer did kind of speak to Congress' intent when this was written in 1986, but technology really, really, really, really has changed since then, which you spoke to. And there seems to be something of a divide here between you and Mr. Dempsey and Mr. Jaffer on this, and specifically talking about someone who has an e-mail account and you are in a cloud, you get your thing from a cloud, you are on Gmail or something, and the distinction between something I got 6 months ago and something I got yesterday and something I have read and something I have not read, I think most people would be surprised about this rather than sanguine. And Mr. Jaffer seemed to think that this is settled law and that we should be sanguine about it.

This, I guess, is for Mr. Dempsey. My understanding is that there is a series of Supreme Court precedents that explain that people can have protected Fourth Amendment interests in items they store with third parties or on property that is not theirs. Can you walk us fairly quickly through the precedents?

Mr. DEMPSEY. Well, you know, you can go all the way back to 1878 when the Supreme Court held that the letter passing through the mail—I mean, you give your letter not merely to a third party, but at that time to a Government agency, voluntarily surrender it, and yet the Supreme Court held in 1878 that the Government cannot open that letter without a warrant as it passes through the network.

If you have a storage locker, one of those storage lockers where you store the junk that you do not really want to give away or throw away, but you also do not want in your house, you put it in a storage locker. You have a Fourth Amendment right in that storage locker. The owner of the locker can even go in to make sure nothing is deteriorating in there or going bad. But for the police to get in, they need a warrant. Luggage, closed containers of luggage checked or stored, subject to the warrant protection, whether they are locked or not, whether they are sealed or not.

So we have dealt with this already, and I think those analogies are perfectly applicable now to this digital storage locker or this digital storage function for the content—and we are focusing here on the content. There are a lot of people who argue that now the transactional data associated with the Internet is so much richer

than the dialed number information. And I think there is a good argument there, and if you look back at the original Supreme Court cases on pen registers, they were very, very narrow. But for now, at least our coalition is saying let us leave that content versus non-content distinction in place. Let us provide lower protection for most of the non-content data, but that content, like that letter in 1878, should be protected regardless of where it is.

Senator FRANKEN. OK. Speaking of the distinction, this may be a little bit off topic if we are talking about law enforcement and security. But you did talk about this as business. This is about business. And this is—and individuals. And I have a question about how do you make people feel safe to use the cloud communicating activity and how much of your information can be used by other commercial—can be used commercially. How can one control information that is, you know, about—say your e-mail traffic. And part of this is who you are sending back and forth to, but they can see, like, oh, he went to this or she went to this e-mail site or this website to, you know, Track magazine, and therefore, let us sell them shoes or—you know. What control over your information can you have on the Internet or in your e-mail so you cannot have people use your information commercially without your permission? Is that a good question?

[Laughter.]

Mr. DEMPSEY. That is a good and clear question and a critical one here. Speaking just for my own organization, the Center for Democracy and Technology, we believe that the law needs to be improved on that side, too. Now, we have tended, as you suggest, to look at the law enforcement issues, which to some extent have the foundation of the Constitution underneath them; we look at the law enforcement governmental access issues in one bucket; and we look at the commercial reuse, commercial disclosure and advertising issues in another bucket.

I think it is better to keep them in separate buckets for now if only because, as you are alluding to, this Committee has jurisdiction over the question of governmental access; there are entire other committees that have jurisdiction over the commercial side of things.

Legislation has been introduced—most recently, Chairman Rush of the House Subcommittee on consumer protection issues has introduced some very good legislation that would improve the rules and for the first time ever set baseline Federal rules for all of those issues associated with advertising and cookies and profiling on the commercial side. Like I say, I do think it is best that we keep those separate.

By the way, if I could, Senator, one other point: The question of commercial access should not prejudice the question one way or the other of governmental access.

Senator FRANKEN. I was going to ask Mr. Smith if he had a reaction, but I am way over my time.

Chairman LEAHY. Thank you.

Senator Whitehouse, thank you for joining us.

Senator WHITEHOUSE. Well, based on Senator Franken's very subtle invitation, I would be inclined to offer him the chance to get his answer from Mr. Smith.

Chairman LEAHY. Would you like—go ahead.

Senator WHITEHOUSE. That was very subtle, by the way.

[Laughter.]

Chairman LEAHY. Go ahead, Senator Franken, and this will not come out of Senator Whitehouse's time. Go ahead.

Senator FRANKEN. Well, subtlety is my forte.

[Laughter.]

Senator WHITEHOUSE. That is why I am so surprised that you departed from that strategy this time.

Senator FRANKEN. I just saw that Mr. Smith has a reaction. That is all. And I wanted to know if you wanted to speak to it.

Mr. SMITH. Sure. And being a lawyer, brevity is obviously mine.

There are two relationships here that are really important. There is the relationship between a consumer and a company that is a service provider, and there is the relationship between the citizen and Government. And to get both of these relationships right, I think we need to look to industry to do its part, and we need to look to Government to do its part.

Those of us in industry I think have a responsibility to build technology that is reliable, that is secure, that has privacy protection built in, and we have a responsibility to be transparent with consumers so they know what the practices are, it is easy for them to understand them, and they can make real choices. And then I think Government obviously has an important role to play in both of these areas in terms of ensuring that ultimately there are legal rules that give consumers the confidence they need and strike the right balance between consumer needs, industry innovation, and law enforcement.

Senator FRANKEN. Thank you. Thank you for your brevity, and I thank you, Senator Whitehouse.

Chairman LEAHY. Senator Whitehouse.

Senator WHITEHOUSE. Thank you. I appreciate the discussion that has taken place, particularly with respect to e-mail, that I think is confounding to even experts, let alone an ordinary American who relies on their e-mail to communicate with friends and businesses and has an expectation of privacy, a personal expectation that, frankly, is not matched by questions of what folder you happen to drop it into affecting how Government can access it.

And I counter that to a very different hypothetical, and let me sort of walk through the hypothetical. Let us say that there is a dangerous virus that is out there on the Internet that is potentially causative of harm to American businesses and interests and so forth. And let us say that the virus has an electronic fingerprint of some kind. You can identify it. That is how you find it. And let us say further that that virus can be housed by the people who are propagating it in the content portion of e-mail. And that is how it propagates, that is how it gets around, and that creates the vulnerability to 1 day that virus being triggered by those malign forces.

If there were a device that could do nothing but identify that fingerprint and signal the presence of that dangerous virus, because the virus could be propagated in the content portion of the transmission, that device would have an ECPA problem, would it not?

Mr. DEMPSEY. Senator, that is a good question. I——

Senator WHITEHOUSE. Setting aside any question of voluntariness under the notice under the Fourth Amendment that there was one-party consent or any of that sort of stuff.

Mr. DEMPSEY. The current statute has in it a provision specifically intended to allow service providers to monitor their own networks, and to some extent, ISPs, service providers at all levels, already are doing some of what you are talking about there; that is, they are looking at the content traversing their networks. For example, there is an awful lot of spam that never gets through. The carriers have the total right and discretion under the statute to look for spam and to basically throw it away. And they can get——

Senator WHITEHOUSE. So roll into the hypothesis that it is the Government that is required to—because of the complexity or the nature of the threat that it is the Government that is required to have access to this information, not just the ISP.

Mr. DEMPSEY. So I think that——

Senator WHITEHOUSE. Now it is an ECPA problem.

Mr. DEMPSEY. When you throw the Government in, you get a different set of concerns. I think that there should be more emphasis given to getting those signatures from the hands of the Government into the hands of the service providers so they can, in essence, add them to the list of what they are looking for and what they are blocking and protecting themselves and others——

Senator WHITEHOUSE. Although there is often a very high intelligence and security penalty to doing that because once it is clear that it is known, an enormous amount of other information can be deduced from that conclusion in some circumstances.

Mr. DEMPSEY. In some circumstances, and we have to be careful there. But the service provider——

Senator WHITEHOUSE. So it is not a complete solution, although it is an important direction—you want to maximize that, but you cannot go to that point and say that solves the problem, we are just going to give all the signatures to the ISPs.

Mr. DEMPSEY. I really think we need to keep the Government out of the center of the network here. The carriers do have some ability under current law to disclose to the Government what they find in their networks. And I think that the goal should be that the Government protects its networks and has in essence, I think, under the statute plenary authority to examine traffic to and from the Government itself, on the Government side of the network. On the private sector side of the network, I just do not see how we are going to be able to control getting the Government into the sort of——

Senator WHITEHOUSE. Or more importantly, getting it back out once it is in, right?

Mr. DEMPSEY. Exactly.

Senator WHITEHOUSE. Well, I take your point, and I think that is one of the predicaments we have to work with. But I would also suggest that if you put side by side the restriction on the Government in my hypothetical from being able to do nothing more than identify the fingerprint of a particularly dangerous virus that may be attacking our hospital systems, that may be attacking our electronic grid, that may be attacking our National security structure, and where there is absolutely no inquiring human consciousness

applied to the substantive content of any e-mail, that that should be an ECPA problem, and that it should be not an ECPA problem because an American put something in the wrong file folder for an actual inquiring Government human consciousness to be able to go and read substantive content. Those two do not line up as far as I can tell, and I think that is one of the inconsistencies that we need to try to resolve.

Mr. DEMPSEY. And I think on the cybersecurity side, the——

Senator WHITEHOUSE. Let me ask Mr. Smith on that because you have got all the answer time so far and he was nodding trying to get a word in.

Mr. SMITH. I think it is a very good question. It is an important hypothetical. It is exactly the kind of question we should be focused on as this process moves forward.

I believe we have a lot of tools to deal with that kind of situation today. It is an area where the industry is very focused, and what you are describing is basically something we do every day. We identify new fingerprints, and we are certainly able to work as a service provider to try to keep people from having them erode their computer files.

It is an area of law that is impacted not only by ECPA, but by the Computer Fraud and Abuse Act and other things.

Senator WHITEHOUSE. With all due respect to the industry, a vast majority of our cyber vulnerability would disappear if we could simply get up to basic public, regular, ordinary levels of patching and security, and we have not even been able to do that. So when you get into the smaller percentage where it is really aggressive, really high end, we are dealing at the cutting edge of sophistication with the people who probably have not only the most dangerous capability but the worst intent, it is even more awkward to say, well, rely on our process because, frankly, that process is not even working for getting stuff patched adequately.

Mr. SMITH. Well, I would say one should rely on that process in part, and one needs to look to Government as well. And what we should do—and your question points us in the right direction—is ask ourselves today, Do we have enough tools? Would we benefit from having better and more tools? If the answer is yes, then let us think about what kinds of tools those should be.

Mr. JAFFER. Senator Whitehouse, if I might.

Senator WHITEHOUSE. Well, my time has expired, so we are at the Chairman's discretion. But if you would like to answer, Mr. Jaffer, I will conclude with that. Thank you.

Mr. JAFFER. I appreciate the opportunity, Senator Whitehouse. I think you raise excellent points, and these are very important issues, something that we looked at in the process of developing the Comprehensive National Cybersecurity Initiative. And one of the challenges that we found was how to share this information that the Government has—that you have identified—with the private sector, without sacrificing sources and methods. And I think that one way that Congress can assist both the Government—the executive branch—and the private sector with is creating a process by which that could happen. And I think it is important that that process be housed in the private sector, that there be trusted third parties who can take the Government's information, hold it—with

security clearances—take the private sector's information, match it up, figure out what the threats are, report back to industry to help protect the industry, and if industry is comfortable—and industry might not be—provide anonymized data back to the Government about what threats are being seen at the boundary. And if Congress can create a framework which allows the private sector the ability to protect industry with Government information without giving up sources and methods, that would be a dramatic step forward, I think. And I think that folks on the panel might agree on this very point.

And with respect to Senator Leahy's point on the intent of Congress, I certainly intended no disrespect. In fact, I was hoping to point to the wisdom of Congress in how that balance was struck in ECPA.

Chairman LEAHY. I did not hear any disrespect in it, Mr. Jaffer. It just brought me back to the memory of all the sitting and talking and trying to hold people together before, and my concern about where we will go next. We did this as a bipartisan effort before. We still pass bipartisan legislation. John Cornyn and I passed an update on FOIA in the Senate last night unanimously, and it shows that this can be done. This should not be a partisan issue, and I do not see it that way. I do appreciate the effort that corporations and private groups and others and Government have done in helping us work on this.

I am glad, Senator Whitehouse, that we are not having to feed the meter of all the people who have actually volunteered their time to help us on it. And I have spoken only broadly about the cybersecurity problems, but you only have to pick up the paper and see the number of attacks on our computers at the Department of Defense, at the CIA, and others, and I mean what has been in the public press. And Senator Whitehouse knows from his briefings on the Intelligence Committee, the briefings I get in classified areas, it is a growing and will continue to be a growing concern. It is no longer an idea of fiction, for example, a power grid being shut down in the middle of winter in the northern part of the country and what that might do. We worry about somebody bringing an explosive on an airplane and killing 100 or 200 people. You could have cyber attacks that could kill thousands of people, and we have to guard against that.

At the same time, I like to know that if I am in business, for example, and I am working in my business and somebody is stealing my trade secrets and getting away with it, but I also want to know that if I am—that my own personal e-mails are going around, the Government is not snooping in it just for the sake of snooping in it.

So it is a difficult balance. I am urging the administration to promptly provide the Committee with its proposals to update ECPA. I thank the shareholders for sharing their views on this issue. I would note that we will start work on this very soon, and we are going to be back here for a lame duck session. We will continue to work that. We have superb members of the staff who have been working on it and will continue to.

So this hearing today, any one of the people in the hearing, if you get ideas, if you want to add it to your testimony, feel free to do

VerDate Nov 24 2008 11:00 Jul 07, 2011 Jkt 066875 PO 00000 Frm 00034 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66875.TXT SJUD1 PsN: CMORC

so, because we want that information. And I will again reiterate that I want the administration to come up with their proposals?

Do you have further——

Senator WHITEHOUSE. Mr. Chairman, could I comment on that, also? I do not want to interrupt your remarks, but as you have pointed out, a number of committees that are looking at the concern about cybersecurity are now working together to try to put together a bill that we can move on. We are actually in a fairly late stage in terms of addressing this from a point of view of the risk. We are actually in an overdue stage; just from a point of view of the legislative positioning we are at a fairly late stage. And so I think that I would like to echo your message to the administration that this is—it is getting a little late to come before a Congressional Committee and not have a point of view and not have a proposal. Unless they want to be out of the debate or simply be commentators and let Congress lead, that is their choice. But considering the extent of the administration's role in this, I would hope that they would take a more active role and be more proactive. So I would like to echo that.

And the other thing I just wanted to echo is that I am extremely strongly in favor of pushing as much of this to the private sector as possible, that as much data should go to the private sector, that should get out there; and the private sector should be dealing with this to the maximum possible extent. But you can make that argument until you are blue in the face, and it will not take away the fact that there will remain an area, whether it is because of revealing sources and methods or because of the extraordinarily adept nature of the technology involved or because of other national security concerns, there will ultimately have to be a Government role, and how we apply that in a way that we do not look like idiots when people are out in front of their banks looking for cash because the financial system is down and they cannot count on their electronic receipts any longer; or up in Vermont the grid is down, they are not going to be looking at Microsoft and Verizon then. They are going to be looking at the President of the United States; they are going to be looking at their local police; they are going to be looking at the FBI; they are going to be looking at the Army and the National Guard; and they are going to want results. And we have to be ready to provide that if that happens.

Chairman LEAHY. I could not agree more. It is easy to say we are all against terrorists. Of course, we are against terrorists. We are all against criminals. Of course, we are against criminals. Senator Whitehouse and I were both prosecutors. But it is a different era. You talk about the—without going into war stories, we would have periodic bank robberies. We usually caught them because they were usually dumb. And we would catch them fairly quickly. The most they would have gotten away with is $10,000 or $15,000. I am very much worried about a bank robber who sits offshore and steals several hundred million dollars. And, you know, we worried about the arsonists that burned one building. I worry about somebody who could destroy whole blocks, whole communities.

So, anyway, we could all come up with the darkest scenarios, but what we have to do is make sure we stop that. So I thank you for taking the time. I also thank you for all the time you took leading

up to this and all the others whose comments and testimony are part of the record.

This is going to be a priority, bringing this up to date, of this Committee, and I pass that out to everybody who is interested, and I thank you for your help.

[Whereupon, at 12:01 p.m., the Committee was adjourned.]

[Questions and answers and submissions for the record follow.]

QUESTIONS AND ANSWERS

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

April 5, 2011

The Honorable Patrick Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Enclosed please find responses to questions for the record arising from the appearance of Associate Deputy Attorney General James A. Baker at a hearing before the Committee on September 22, 2010, entitled "The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age."

We apologize for the delay and hope that this information is of assistance to the Committee. Please do not hesitate to contact this office if we may provide additional assistance regarding this, or any other matter. The Office of Management and Budget has advised us that from the perspective of the Administration's program there is no objection to submission of this letter.

Sincerely,

Ronald Weich
Assistant Attorney General

Enclosure

cc: The Honorable Charles Grassley
Ranking Minority Member

Written Questions of Chairman Patrick Leahy
to Associate Deputy Attorney General James A. Baker,
Hearing On "*The Electronic Communications Privacy Act: Promoting Security And Protecting Privacy In The Digital Age*"
Senate Judiciary Committee
September 22, 2010

Cell Phone Location Information

1. In September, the Court of Appeals for the Third Circuit held that the Government could be required to obtain a search warrant before it could access stored cell site location information. The court found that ECPA gives magistrate judges discretion to require a warrant issued on a showing of probable cause, or to require a lesser showing of "specific and articulable facts" that the information sought is relevant and material to an investigation. The court also noted that there is uncertainty in the law about the level of privacy protections for cell site data.

(a) What is the Department's view about the legal standards that should apply in order for the Government to access (i) stored cell site location data, (ii) GPS location data, and (iii) other mobile location information?

Response: The Department has taken the position in federal courts that a court order under 18 U.S.C. § 2703(d), based on a showing of "specific and articulable facts," is the appropriate means of obtaining historical cell-site location records in a criminal investigation. As for the prospective acquisition of GPS (or other similarly precise) location data concerning a wireless phone, the Department has long recommended that federal prosecutors obtain a warrant based upon probable cause. By contrast, the Department has taken the position in court that prospective acquisition of cell-site location information – which is significantly less precise than GPS data, and which does not implicate a Fourth Amendment interest – may be authorized under the authority of the pen register and trap and trace statute in tandem with 18 U.S.C. § 2703(d).

(b) Should Congress clarify these standards under ECPA, and if so, how?

Response: The Administration has not come to any conclusions about particular amendments to ECPA. However, the Department believes that clarifying amendments could be beneficial, provided that they do not imperil public safety or otherwise impair the current ability of prosecutors and agents to obtain such non-content information, including at the preliminary stages of an investigation.

Email Storage

2. **ECPA extends greater privacy protections to emails that are stored for less than 180 days, than for emails that are stored for a longer period. When Congress enacted this provision, most experts believed that an email, once sent, would be deleted. But, today, storing email for extended periods of time is very common**

and there are even new technologies, like cloud computing, that allow users to store mails remotely for years.

(a) How does the distinction regarding the age of stored email impact the Department's ability to acquire evidence in criminal matters?

Response: Under 18 U.S.C. § 2703(a), the government can compel disclosure from a provider of an electronic communication service of electronic communications (such as email) in electronic storage for less than 181 days only pursuant to a warrant. The government can compel disclosure of other communications using a warrant, 2703(d) order, or subpoena. If the government uses a 2703(d) order or subpoena, it must give prior notice to the customer or subscriber. Such notice may be delayed under 18 U.S.C. § 2705 if there is reason to believe that prior notification would cause intimidation of witnesses, destruction of evidence, or other similar harm to an investigation.

The standard for obtaining email is significant because in many cases, investigators may have strong evidence that a target is engaged in serious criminal activity, and they may know that the target uses a particular email account, but they may lack evidence tying the email account to the criminal activity. For example, investigators might know that an individual who engaged in fraud schemes through two Hotmail email accounts also used a third Hotmail account, but they may lack sufficient information linking the third account to the known fraud schemes to obtain a warrant. Or investigators might know that an individual produced child pornography on his home computer and downloaded child pornography from the Internet, but they might still lack sufficient information linking this conduct to the individual's Yahoo! email account to obtain a warrant. In such circumstances, investigators may be able to use a subpoena or 2703(d) order to acquire certain stored email.

(b) Does this distinction make sense and should Congress consider changing, or eliminating this distinction?

Response: The Administration has not come to any conclusions about particular amendments to ECPA. However, any alteration to the current legal framework should take into account the variety of communication and storage services used today, from webmail to corporate mail, from private bulletin boards to social networking sites to public blogs. Access to information from these services is critical to the success of criminal cases. Thus, before requiring a warrant for any particular class of electronic evidence, it is important to consider how such a requirement might play out in practice.

For example, law enforcement needs tools to investigate and build cases in early stages in order to develop probable cause. Allowing the acquisition of certain types of content – with process short of a warrant but with appropriate additional safeguards – can fill this role. In addition, imposing a warrant requirement on compelled production of the contents of communications would cause significant problems in the corporate email context. Currently, if a corporation is suspected of involvement in illegal activities (for example, fraud, antitrust violations, or environmental crimes), the government may subpoena relevant documents from the corporation.

If a warrant requirement were imposed on compelled production of email, the corporation could shelter incriminating documents from subpoena merely by storing them as email or attachments to email. Furthermore, a warrant requirement would also substantially burden investigative agencies, such as the FTC and SEC, that lack authority to obtain search warrants.

Section 2709

3. The Department of Justice recently proposed that Congress amend Section 2709 of ECPA to make it easier for the FBI to obtain Americans' electronic communications transactional records. **How does the Department's proposal address and protect Americans' privacy rights and civil liberties?**

Response: The proposal does not change the way the FBI obtains electronic communication transactional records of Americans. The proposed amendment to 18 U.S.C. § 2709(b)(1) to include the phrase "electronic communications transactional records" is intended by the Department as a technical fix to ensure consistency between the types of records National Security Letter (NSL) recipients are required to provide to the FBI under 18 U.S.C. § 2709(a) and the types of records that are subject to the procedural protection of an FBI certification of relevance pursuant to 18 U.S.C. § 2709(b)(1). Without the proposed fix, the statute is ambiguous. The Department is prepared to discuss other language to remove that ambiguity, so long as it preserves the FBI's ability, consistent with constitutional and statutory rights, to obtain permitted electronic communications transactional records.

The Department and the FBI take seriously the privacy rights and civil liberties of Americans. We have robust policies, procedures and oversight in place to ensure that protection of privacy rights and civil liberties is carefully balanced with the FBI's need to obtain information in support of our predicated national security investigations to protect Americans from terrorist attacks and other threats to the national security.

ECPA Reform

4. During the hearing, you testified that while the Department is currently reviewing ECPA, it is not yet prepared to provide any recommendations to Congress on updating this important law. I advised that the Committee will be moving forward with its work to update this law and urged the Department to promptly get its recommendations to the Committee. **When will the Department provide its recommendations to the Committee on reforms to ECPA?**

Response: The Department and the Administration are working expeditiously on formulating recommendations for ECPA reform, but at this point we cannot provide a certain date for when we will submit these recommendations.

Questions submitted by U.S. Senator Arlen Specter
to Associate Deputy Attorney General James A. Baker

5. **Mr. Baker, in April I introduced the Surreptitious Video Surveillance Act of 2010 (S. 3214) to require any governmental entity conducting video or still surveillance *within a residence* to seek a warrant. Title III of the Omnibus Crime Control and Safe Streets Act, known as the federal Wiretap Act, does not forbid video surveillance or require a warrant. Do you support the legislation's effort to codify a warrant requirement for in-home surveillance? Will you undertake to expeditiously provide comments on the legislation?**

Response: The Department appreciates the important privacy concerns S.3214 seeks to address, and we will be happy to provide formal comments on the legislation. As a practical matter, it is noted that extensive federal court precedent already imposes stringent controls on law enforcement use of surreptitious video surveillance to monitor activity in private areas. In addition, video surveillance does not squarely fit within the framework of the Wiretap Act, which regulates the "interception" of "communications" between and among "parties," because video surveillance does not involve communications between parties. Thus, it is unclear how the provisions of Title III would apply to video surveillance, or why including such surveillance within the Wiretap Act is practically necessary.

6. **Mr. Baker, you testified that the Electronic Communications Privacy Act (ECPA) is a vital tool for the law enforcement community. How does ECPA assist investigations?**

Response: Law enforcement officials rely on ECPA to further important investigations, solve crimes, and apprehend criminals. Criminals involved in terrorism, drug trafficking, violent crime, kidnappings, computer hacking, sexual exploitation of children, organized crime, gangs, and white collar offenses use email, cell phones, and the Internet in furtherance of their offenses, and network service providers retain information critical to solving these crimes. ECPA process is used regularly by the Department of Justice in investigations of all of these types of crime.

Investigators use ECPA to obtain both content and non-content information from service providers. The content of a communication, such as a voice mail or the subject line and body of an email, is often direct evidence of crime. Non-content information associated with a communication can show investigators with whom a subject communicates, at what time, for how long, and it can provide information about the location of a criminal. Such non-content

information - generally available with a lower evidentiary threshold - is a critical building block in investigations and can lead to the development of probable cause to arrest a criminal and search for evidence.

Questions Submitted by U.S. Senator Russell D. Feingold
to Associate Deputy Attorney General James A. Baker

7. At a May 5, 2010, hearing of the House Judiciary Subcommittee on the Constitution, Civil Rights, and Civil Liberties, service provider attorney Albert Gidari submitted written testimony that stated the following with regard to government requests for information in criminal investigations:

> The following issues are faced by service providers every day in response to government demands for acquisition and use of location information:
>
> ***
>
> d. Target v. Associates (hub and spokes). Regardless of the legal standard applicable to the target phone, what standard applies to obtain the location information for all those with whom the target communicates? It is common in hybrid orders for the government to seek the location of the community of interest – that is, the location of persons with whom the target communicates.

a. Do federal prosecutors obtain location information about groups of individuals that include individuals that are not suspected of any crime, such as all individuals who communicate with a particular suspect?

b. If so, what legal theory does it rely on? How frequently is this technique employed?

Response: Federal prosecutors may on occasion have a need to obtain information about wireless telephones carried by individuals not suspected of crimes, where that information may nevertheless be relevant in a criminal investigation. For instance, a fugitive may be known to be

traveling with a family member or other companion carrying a known wireless phone; in such circumstances, determining the location of the companion's phone would be an appropriate means of locating the fugitive.

Regarding "community of interest" location information – as described above, the location of all phones in contact with an identified target phone – we do not believe federal prosecutors seek such prospective "hub and spoke" information with any degree of regularity. For the government to obtain this information, it would have to meet the statutory threshold ("specific and articulable facts" for cell-site information and probable cause for GPS information) for each device it was seeking information about. Meeting this burden would be difficult in practice.

However, there may be some circumstances in which such orders are appropriate. Consider, for example, an investigation in which law enforcement knows that members of a narcotics ring use prepaid cell phones to communicate exclusively with other members of the ring regarding their narcotics enterprise. Under such circumstances, once law enforcement becomes aware of the phone number for a cell phone in current use by the ring, it is appropriate to seek an order to obtain location information for all cell phones in contact with the known phone. If the ring members replace their prepaid phones frequently (as is often the case), requiring law enforcement to obtain an initial order and then subsequent follow-up orders could substantially impede the investigation.

8. **As I understand it from the hearing testimony, the Justice Department believes that in a criminal investigation to obtain retrospective cell-site location information, it should seek a court order under 18 U.S.C. 2703(d); to obtain prospective cell-site location information, it should seek a 'hybrid' court order under 18 U.S.C. § 2703(d) and the pen register/trap and trace statute; and to obtain prospective GPS-based location information, it should seek a probable cause search warrant.**

   a. **Is this accurate?**

Response: Yes.

b. Do all U.S. Attorney's offices follow these standards?

Response: As a result of local rulings, in a number of districts federal prosecutors obtain prospective cell-site information only pursuant to a search warrant. In addition, United States Attorneys' Offices follow local court guidelines to obtain prospective GPS data from service providers.

c. With respect to investigations conducted under the Foreign Intelligence Surveillance Act, what type(s) of legal process does the Justice Department seek to obtain these types of location information?

Response: CLASSIFIED (being transmitted separately)

9. **Please specify how many federal courts of appeals have issued rulings on government access to the types of location information described in Question 2 and what legal process they have held the government must obtain.**

Response: To date, only one federal court of appeals has addressed the issue of cell site location information. In a recent decision, the Third Circuit Court of Appeals held that retrospective cell-site location information "is obtainable under a [Title 18, United States Code] § 2703(d) order and that such an order does not require the traditional probable cause determination." *In re Application Of The United States Of America For An Order Directing A Provider Of Electronic Communication Service To Disclose Records To The Government*, No. 08-4227 (3d Cir. Sept. 7, 2010). At the same time, however, the court also held that the statute "gives the [magistrate judge] the option to require a warrant showing probable cause ... although it is an option to be used sparingly ...." Pineda-Moreno, Maynard, and similar decisions relate strictly to the use of GPS tracking devices installed by the government. Because the question in context calls for information about court decisions involving wireless location data obtained from service providers (and because ECPA, the subject of the hearing, does not impose restrictions on the use of such devices), the omission is intentional and appropriate.

7 |

10. **Please specify how many federal district courts have issued rulings on government access to the types of location information described in Question 2 and what legal process they have held the government must obtain. If judges within a particular district court have come to different conclusions with regard to the same type of location information, please so indicate.**

Response: The number of district courts (including both district judges and magistrate judges) issuing written opinions on the procedures for obtaining cell phone location information are listed below. With respect to all three categories of information described below, we note that these figures present a skewed picture of the practice in most federal districts, as many judges regularly grant the Department's applications -- and thus implicitly endorse our legal positions -- without issuing written opinions.

Retrospective cell-site location information

Judges and magistrate judges in five different federal districts have issued written opinions expressly upholding the use of a court order under 18 U.S.C. § 2703(d) to obtain historical cell-site location records. (This includes two cases in which district court judges reversed magistrate judges on appeal.) Judges in two additional districts have endorsed this approach in dicta. In two other districts, courts have rejected the government's approach and demanded a warrant; one of these decisions, however, was vacated by the recent Third Circuit decision discussed in the response to Question 3 *supra*.

Courts in three additional districts have reached internally conflicting decisions. In the Northern District of Indiana, one court has without analysis denied a government application under 18 U.S.C. § 2703(d) and demanded a warrant; more recently, a different judge in the same district denied a defendant's motion to suppress historical cell-site location records, holding that such records are not protected by the Fourth Amendment. In the Southern District of Texas, a district court judge has approved the use of a court order under 18 U.S.C. § 2703(d) to obtain historical cell-site location records; however, a magistrate judge recently denied such an application and demanded a warrant, reversing his previous policy of approving section 2703(d) orders for these types of records. Finally, a magistrate judge in the Eastern District of New York has held that 18 U.S.C. § 2703(d) on its face allows the government to obtain such records, but that the Fourth Amendment nevertheless requires a warrant.

Prospective cell-site location information

Judges and magistrate judges in five different federal districts have issued written opinions expressly upholding the use of a court order under the pen register and trap and trace statute, in tandem with 18 U.S.C. § 2703(d), to obtain prospective cell-site location information. (This includes two district court judges who reversed magistrate judges on appeal.) In twelve other

districts, courts have rejected this so-called "hybrid" approach and demanded a warrant. We note that in several of these cases, the courts reaching this conclusion have conflated cell-site location information with more precise GPS (or similar) location information.

Courts in two districts have reached internally conflicting decisions. In the Southern District of New York, two judges have endorsed the "hybrid" theory, and two others have rejected it. Similarly, in the Eastern District of New York two district court judges have upheld the Department's approach – in each case reversing a magistrate judge – while one district court judge has rejected it, as one magistrate judge continues to do despite his reversal by the district court.

Prospective geolocation information (GPS or other method)

Courts in two different districts have issued written opinions expressly upholding the use of a search warrant based on probable cause to obtain prospective geolocation information (such as GPS or similarly precise information) concerning a criminal suspect's wireless phone. In a third district, one district court judge has adopted this view, while a magistrate judge has held that in the special case of fugitives the proper authority is an order under the All Writs Act in aid of a pre-existing arrest warrant. Despite reversal of that decision by the District Court, this Magistrate Judge has reasserted the same view in a subsequent opinion.

11. **As was discussed at the hearing, the statutory protection afforded to the contents of an electronic communication depends (among other things) on whether it is stored or in transit, whether it is more than 180 days old, and whether the recipient has opened it.**

    a. **In 2007, 2008 and 2009, how many times did the Department of Justice and/or Federal Bureau of Investigation obtain a court order issued pursuant to 18 USC § 2703(d) for the contents of electronic communications?**

Response: The Department of Justice does not keep records regarding how frequently legal process under 18 U.S.C. § 2703 is used.

    b. **In 2007, 2008 and 2009, how many times did the Department of Justice and/or Federal Bureau of Investigation issue a subpoena for the contents of electronic communications? In these cases, how many times was notice delayed pursuant to 18 U.S.C. § 2705?**

Response: The Department of Justice does not keep records regarding how frequently legal process under 18 U.S.C. § 2703 is used.

12. **What statutory authority does the Justice Department use to obtain content from a website that allows users to store and share photographs?**

Response: If the government sought to compel disclosure of photographs from a website that allows users to store and share photographs, such activity would be covered by 18 U.S.C. § 2703(a) and (b). Under § 2703(a), the government may compel disclose of the content of communications in electronic storage in an electronic communications service for 180 days or less only pursuant to a search warrant. Under § 2703(b), the government may compel disclosure of other communications stored by a remote computing service using a warrant, a 2703(d) order, or a subpoena. When the government uses a subpoena or 2703(d) order, it must provide prior notice to the subscriber or customer. That notice may be delayed if authorized under 18 U.S.C. § 2705 if there is reason to believe that prior notification would cause intimidation of witnesses, destruction of evidence, or other similar harm to an investigation.

A website that allows users to store and share photographs may voluntarily disclose content to the government under the circumstances set forth in 18 U.S.C. § 2702(b). For example, a voluntary disclosure is permissible in "an emergency involving danger of death or serious physical injury to any person" that "requires disclosure without delay of communications relating to the emergency." 18 U.S.C. § 2702(b)(8)

13. **When Justice Department lawyers apply for a court order to install or use a pen register and/or trap and trace device pursuant to 18 U.S.C. § 3121 *et seq.*, do they commonly include in the application a statement of facts explaining why the information likely to be obtained is relevant to an ongoing criminal investigation?**

Response: Practice in this area varies according to local custom. In some districts, prosecutors do include a factual statement; in other districts, prosecutors provide the certification required by the statute, without additional factual recitation.

14. **What specific types of information does the Federal Bureau of Investigation seek and obtain today with a national security letter issued pursuant to 18 U.S.C. § 2709 for "electronic communications transactional records"?**

Response: Generally, the types of electronic communications transactional records (ECTRs) sought and obtained from electronic communications service providers (ECSPs) are: the name, physical address, e-mail address, account number, or other identifying information for a person or entity involved in an electronic communication; the Internet Protocol (IP) address or other network address, including any temporarily assigned IP or network address, for a computer involved in an electronic communication; the period of usage, session time, and the communication routing or transmission information for an electronic communication; the length of the service (including the start date) and types of service utilized by a person or entity involved in an electronic communication; the methods and sources of payment for such service (including any credit card or bank account number); and the means used to access an electronic communication service or account. In late 2009, however, one ECSP stopped providing ECTRs in response to National Security Letters (NSL) issued by the FBI pursuant to 18 U.S.C. § 2709. In late 2010, two other ECSPs also stopped providing ECTRs in response to NSLs issued by the FBI pursuant to 18 U.S.C. § 2709.

15. **What specific types of information did the Federal Bureau of Investigation seek and obtain prior to November 5, 2008, with a national security letter issued pursuant to 18 U.S.C. § 2709 for "electronic communications transactional records"?**

Response: The types of ECTRs sought by the FBI with NSLs today are the same as were sought and obtained prior to November 5, 2008, namely: the name, physical address, e-mail address, account number, or other identifying information for a person or entity involved in an electronic communication; the Internet Protocol (IP) address or other network address, including any temporarily assigned IP or network address, for a computer involved in an electronic communication; the period of usage, session time, and the communication routing or transmission information for an electronic communication; the length of the service (including the start date) and types of service utilized by a person or entity involved in an electronic communication; the methods and sources of payment for such service (including any credit card or bank account number); and the means used to access an electronic communication service or account.

Statement of U.S. Senator Russell D. Feingold
Hearing On "The Electronic Communications Privacy Act:
Promoting Security and Protecting Privacy in the Digital Age"
Senate Judiciary Committee
September 22, 2010

Mr. Chairman, I am pleased that the Judiciary Committee is taking a look at the important issue of reforming the Electronic Communications Privacy Act (ECPA).

When you consider that ECPA was enacted in 1986, it is incredible how forward-looking it was. In 1986, networked computing was in its infancy, and few could have imagined the enormous influence that it would ultimately have on our society. Yet Chairman Leahy, Representative Kastenmeier of Wisconsin and many others in Congress had the foresight to recognize the importance of establishing clear, sensible rules for when the government can access electronic communications in a criminal investigation while also protecting Americans' privacy rights.

Nearly 25 years later, those principles are still vitally important, but not surprisingly ECPA itself has not kept up with the technological change we have experienced. Rules that covered the waterfront a quarter of a century ago now leave gaping holes and a great deal of uncertainty. Other rules that may have made sense in 1986 no longer do.

Indeed, many Americans would be very surprised to learn that the contents of their email communications are not necessarily statutorily protected by the warrant requirement. Under ECPA, an email that is more than 180 days old can be obtained by the government in a criminal investigation without getting a search warrant from a judge. Not only that, but the Department of Justice has taken the position that ECPA also allows it to obtain an email without meeting the probable cause standard simply because it has been opened by the recipient. Do any of us believe that our email no longer deserves the same privacy protection as our phone conversations because we have already read the email, or left it in our inbox for more than 6 months? It is time to fix this anachronism in the law so that the contents of Americans' email conversations cannot be accessed by the government unless a judge agrees there is probable cause and issues a search warrant.

ECPA also provides a set of rules allowing the government to obtain – usually based on mere relevance to an investigation – the non-content information about our electronic communications, such as the email addresses we communicate with, the IP addresses of our computers, and the time and date of our communications. But ECPA could not have foreseen how ubiquitous electronic communications would become, and how much information about a person could be gleaned from information that might not technically be considered "contents." There continue to be difficult grey areas where it is hard to draw the line between content and non-content information, yet the legal ramifications under ECPA are very significant. This is an area that I have been looking at for years,

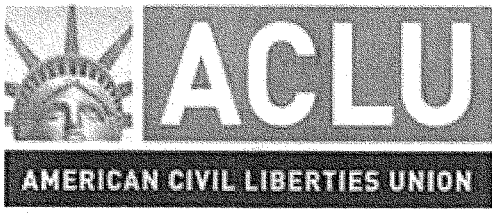
and I hope the committee will consider whether the current certification of relevance standard for the real-time acquisition of this 'transactional' information still makes sense.

Other technological innovations need to be addressed by Congress, as well. The use of mobile phones and other mobile devices can reveal a person's location, often quite precisely, both in the past and in real time. Yet court decisions have not resulted in consistent rules for what the government must show to obtain location information about a suspect, and in fact in some cases different judges in the same federal district have come to different conclusions. Given this lack of clarity, Congress should establish clear rules for location information. Congress also needs to set clear rules to govern access to information that is stored in the "cloud" – on third-party servers – as "cloud computing" becomes more prevalent.

Mr. Chairman, in sum, we need to follow the example that you and others set when you wrote ECPA in the first place. We need to craft clear rules that protect privacy, that give law enforcement the tools it needs, that industry can rely on, and that are as technologically neutral as possible so that they can weather at least a decade or two of innovation before Congress will need to revisit them.

I commend you, Mr. Chairman, for this opportunity to consider carefully the overall framework of surveillance rules in criminal cases. The laws governing the surveillance of Americans have, in the past decade, too often been debated in a politically charged environment, so I appreciate this opportunity for a real discussion.

SUBMISSIONS FOR THE RECORD



Written Statement of the
American Civil Liberties Union

Laura W. Murphy
Director
ACLU Washington Legislative Office

Christopher Calabrese
Legislative Counsel
ACLU Washington Legislative Office

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

before the
Senate Judiciary Committee

September 22, 2010

Hearing on

The Electronic Communications Privacy Act:
Promoting Security and Protecting Privacy in the Digital Age

Chairman Leahy, Ranking Member Sessions, and Members of the Committee:

The American Civil Liberties Union (ACLU) has over half a million members, countless additional activists and supporters, and fifty-three affiliates nationwide. We are one of the nation's oldest and largest organizations advocating in support of individual rights in the courts and before the executive and legislative branches of government. Throughout our history, we have been one of the nation's foremost protectors of individual privacy. We write today to urge the committee to take the first steps toward modernizing the Electronic Communications Privacy Act (ECPA).

The Founding Fathers recognized that citizens in a democracy need privacy for their "persons, houses, papers, and effects." That remains as true as ever. But our privacy laws have not kept up as technology has changed the way we hold information. Thomas Jefferson knew the papers and effects he stored in his office at Monticello would remain private. Today's citizens deserve no less protection just because their "papers and effects" might be stored electronically.

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

Americans Have Embraced Technology

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

- Over 50% of American adults use the Internet on a typical day.[1]
- 62% of online adults watch videos on video-sharing sites,[2] including 89% of those aged 18–29.[3]
- 69% of online adults use "cloud computing"[4] services to create, send and receive, or store documents and communications online.[5]

---

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

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

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

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

[5] Pew Internet & American Life Project, *Use of Cloud Computing Applications and Services*, Sep. 2008 [hereinafter Pew Cloud Report], http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-

- Over 70% of online teens and young adults[6] and 35% of online adults have a profile on a social networking site.[7]
- 83% of Americans own a cell phone and 35% of cell phone owners have accessed the Internet via their phone.[8]
- One in four U.S. adults have used a location-based service[9], and two-thirds of iPhone users access a location-based service at least once a week.[10]

Companies continue to innovate and create new ways for Americans to merge technology with daily activities. Google has spent the last five years building a new online book service and sales of digital books and devices have been climbing.[11] Americans increasingly turn to online video sites to learn about everything from current news to politics to health.[12] As the recently announced Facebook location service "Places" heralds, location-based services are a burgeoning market.[13] There are thousands of location-aware applications available for the 49 million smartphone users in the United States.[14]

These services provide many benefits, but they also have the ability to collect and retain detailed information about individuals: their interests, concerns, movements, and associations. This information can be linked together, allowing a user's Internet searches, emails, cloud computing

---

Services.aspx . 56% of Internet users use webmail services, 34% store photos online, and 29% use online applications such as Google Docs or Adobe Photoshop to create or edit documents.

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

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

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

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

[10] Mobile Marketing Ass'n, U.S. Consumers Significantly More Likely to Respond to Location-Based Mobile Ads than Other Mobile Ad Types, Apr. 21, 2010, http://mmaglobal.com/news/us-consumers-significantly-more-likely-respond-location-based-mobile-ads-other-mobile-ad-types.

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

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

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

[14] Mobile Subscriber Market Share, July 8, 2010, http://www.comscore.com/Press_Events/Press_Releases/2010/7/comScore_Reports_May_2010_U.S._Mobile_Subscriber_Market_Share; Skyhook Wireless, Location Aware App Report, Feb. 2010 http://www.locationrevolution.com/stats/skyhookfebreport.pdf.

documents, photos, social networking activities, and book and video consumption to be collected into a single profile.[15]

Americans Still Expect Privacy

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

- 69% of Internet users want the legal right to know everything that a Web site knows about them.[16]
- 92% want the right to require websites to delete information about them.[17]
- A large percentage of users of cloud computing are "very concerned" about how their personal information may be used and disclosed to law enforcement and third parties.[18]

When user privacy is not protected, users are slower to adopt new technology. A recent poll revealed that 50% of Americans polled have little or no interest in using cloud computing and that 81% of these respondents are reluctant, at least in part, because they are concerned about the security of their information in the cloud.[19]

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

ECPA Rules Are Confusing and Outdated

In the face of rapid technological change and Americans' continuing expectation of privacy, ECPA has fallen behind. Distinctions in ECPA have become increasingly confusing and arbitrary, based on an understanding of technology that is a generation behind that which we use today.[20] Many new technologies, particularly those dealing with location information, are not addressed by ECPA. These failures not only leave holes in the privacy protections in place for individuals, but pose a threat to continuing innovation and business development. We need to update ECPA to encompass all of the ways that Americans use technology today.

---

[15] *See* ACLU of Northern California, *Digital Books*, *supra* note 11 ("[I]f a reader has logged in to other Google services such as Gmail at the time he searches for a book, Google can link reading data to the reader's unique Google Account [and] retains the right to combine all this information with information gleaned from its DoubleClick ad service, which tracks users across the Internet.") More information is available at the ACLU's Demand Your dotRights campaign website. Demand Your dotRights, http://dotRights.org.

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

[17] *Id.*

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

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

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

E-mail exemplifies the gap between the language of ECPA and today's technology. In 1986, e-mail was typically downloaded to a recipient's computer upon receipt and immediately deleted from the e-mail provider's storage. ECPA was written with this behavior in mind: it requires a search warrant to retrieve a message from an e-mail provider's storage only if the message is less than 180 days old, and provides for lower standards if the email is left on the server for more than 180 days.[21] Today, however, e-mail is often both stored on and accessed from remote servers belonging to the e-mail provider, and many people "archive" their e-mail on their provider's server rather than deleting old messages. Basing legal protection on how long an e-mail has been stored is incongruous with current e-mail use. Instead, ECPA should provide full protection for all online documents and communications and dispose of these artificial and outdated distinctions.

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

In addition to the difficulty in anticipating modern uses of technologies existing in that era, lawmakers in 1986 could not predict technological innovations. Mobile phones provide a glaring example, along with the location information gleaned from them. Modern cell phones have become, in essence, portable tracking devices. Technologies including GPS[22] and cell tower triangulation[23] allow mobile phone providers to determine our physical locations in real time and retain records of this location information indefinitely. The legal standard for access to these records is currently being litigated, and Congress has never weighed in on what the appropriate standard should be.[24] In the meantime, law enforcement agents are already aggressively seeking massive amounts of information about consumer location. In 2009, a company employee provided a rare glimpse into the scope of government demands for location data when he

---

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

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

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

[24] *See, e.g., In re Application of the United States for an Order Directing a Provider of Electronic Communications Service to Disclose Records to the Government*, No. 08-4227 (3d. Cir. Sept. 7, 2010) (finding a judge may require law enforcement to show probable cause before obtaining historical cell site location information).

admitted that Sprint received a staggering eight million requests for mobile phone location information from law enforcement in just over a year.[25]

Unfortunately, this data is sometimes sought under questionable circumstances that highlight the potential for abuse. In 2008, the FBI sought and received (without a warrant) location-tracking information not just for a robbery suspect, but for 180 other innocent people;[26] in 2010, Michigan police officers sought information about every cell phones near the site of a planned labor protest;[27] and an Alabama sheriff demanded that a telecommunications company track his daughter's location without a warrant when she didn't come home from a date, claiming that she had been kidnapped.[28] These examples are likely just the tip of the iceberg.

Outdated digital privacy law is not only a threat to individual privacy; it also affects businesses and hinders innovation. User perception of inadequate privacy is one threat that companies face. For example, Microsoft recently announced that its future lies in online cloud computing services, but its own poll found that more than 90 percent of the general population is "concerned about the security, access, and privacy of personal data" stored online,[29] leading the company to explicitly ask Congress for better online privacy protection to promote cloud computing.[30]

Companies are also affected when they receive demands to turn over the personal information of users. Time Warner Cable employs 4 people dedicated solely to responding to law enforcement requests to look up Internet Protocol (IP) addresses.[31] In April 2010, Google released data that it received over 3,500 demands from law enforcement involving criminal investigations in the last six months of 2009.[32]

If Google is receiving thousands of demands digging into the intimate details of individual lives that are captured in emails, search histories, reading and viewing logs, and the like, how many more are going out to Yahoo, Microsoft, Facebook and the thousands of other online services that Americans use every day? And how can companies hope to respond to these requests

---

[25] Kim Zetter, *Feds 'Pinged' Sprint GPS Data 8 Million Times Over a Year*, WIRED, Dec. 1, 2009.
[26] Brief of Amici Curiae in Support of Motion to Suppress, *United States v. Soto*, Case No. 09-cr-200 (D. Conn. June 18, 2010), *available at* http://www.aclu.org/files/assets/2010-6-18-USvSoto-AmiciBrief.pdf. While the details remain unclear because the government surveillance demands are under seal, it appears that the government engaged in dragnet surveillance, seeking and obtaining location information for a large number of innocent people to identify who was involved in the crime.
[27] *See* Michael Iskoff, *The Snitch in Your Pocket*, NEWSWEEK, Feb. 19, 2010.
[28] Transcript of "Where I'm Calling From," On the Media, May 8, 2009, *available at* http://www.onthemedia.org/transcripts/2009/05/08/05.
[29] Microsoft News Center, *Cloud Computing Flash Poll—Fact Sheet*, http://www.microsoft.com/presspass/presskits/cloudpolicy/docs/PollFS.doc. More information is available at http://www.microsoft.com/presspass/presskits/cloudpolicy/materials.aspx.
[30] Microsoft News Center, *Press Release: Microsoft Urges Government and Industry to Work Together to Build Confidence in the Cloud*, Jan. 20, 2010, *available at* http://www.microsoft.com/presspass/press/2010/jan10/1-20BrookingsPR.mspx.
[31] Nate Anderson, *Time Warner Tries to Put Breaks on Massive Piracy Case*, ARS TECHNICA, May 16, 2010, http://arstechnica.com/tech-policy/news/2010/05/time-warner-cable-tries-to-put-brakes-on-massive-piracy-case.ars.
[32] Government Requests Tool, http://www.google.com/governmentrequests. Note this does not include National Security letters or demands received outside of criminal investigations. It also does not count the actual number of users whose records disclosed pursuant to each demand. All of this means this number likely only reflects a fraction of the number of users whose records were demanded.

without improperly over- or under-disclosing information when faced with outdated, confusing laws with questionable applicability to their products or services?

Key Principles for Updating ECPA

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

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

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

Robustly Protect All Personal Electronic Information.

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

But American's privacy interest is not limited to the content of communications. Congress has long-recognized the privacy interests in the transactional records of users of expressive material. The Video Privacy Protection Act prohibits disclosure of video viewing records without a warrant or court order, requires notice prior to any disclosure of personally identifiable information to a law enforcement agency, and requires the destruction of personally identifiable information one year after it becomes unnecessary.[33] The Cable Communications Policy Act similarly prohibits disclosure of cable records absent a court order.[34] Similarly, to safeguard autonomy, privacy, and intellectual freedom, our laws extend protection to library and book

[33] 18 U.S.C. § 2710(b)(2)(B), (b)(3),(e) (2009).
[34] 47 U.S.C. § 551(c) (2008).

records.[35] We need the same protection for digital records that implicate our First Amendment freedoms by recording our expressive actions and choices.

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

Safeguard Location Information.

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

Institute Appropriate Oversight and Reporting Requirements.

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

The House Judiciary Committee recognized this need when it approved HR 5018 (106th Congress) by a vote of 20-1.[36] The proposed bill would have required reporting on all orders, warrants, or subpoenas issued by government entities seeking electronic communications records or content information. Current efforts to modernize ECPA should include this requirement as well.

---

[35] 48 states protect library reading records by statute, *see, e.g.*, N.Y. C.P.L.R. § 4509; Cal. Gov. Code §§ 6267, 6254(j), and federal and state courts have also often frowned upon attempts by the government or civil litigants to gain access to such records, *see, e.g., In re Grand Jury Subpoena to Amazon.com*, 246 F.R.D. 570, 573 (W.D. Wis. 2007) (quashing a government subpoena seeking the identities of 120 book buyers because "it is an unsettling and un-American scenario to envision federal agents nosing through the reading lists of law-abiding citizens while hunting for evidence against somebody else."); *In re Grand Jury Subpoena to Kramerbooks & Afterwords, Inc.*, 26 Media L. Rep. (BNA) 1599, 1601 (D.D.C. 1998) (First Amendment requires government to "demonstrate a compelling interest in the information sought . . . [and] a sufficient connection between the information sought and the grand jury investigation" prior to obtaining book records); *Tattered Cover v. City of Thornton*, 44 P.3d 1044, 1059 (Colo., 2002) (government access to book records only passes muster under Colorado Constitution if "warrant plus" standard is met by the government—i.e, prior notice, adversarial hearing, and showing of a compelling need).

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

Require a Suppression Remedy.

Both the Fourth Amendment and the Wiretap Act provide for an exclusionary remedy: if a law enforcement official obtains information in violation of a defendant's constitutional privacy rights or the Act, that information usually cannot be used in a court of law.[37] The same rule, however, does not apply to electronic information obtained in violation of ECPA. Without an exclusionary rule, there is a lack of deterrence for government overreaching. Unlawfully obtained electronic information should be barred from use in court proceedings. A suppression remedy provision passed the House Judiciary Committee in 2000 as part of HR 5018 and should be included in any current Congressional language to modernize ECPA.[38]

Craft Reasonable Exceptions.

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

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

In addition, exceptions to prohibitions on "voluntary" disclosure need to be revised to prevent coercive abuse by law enforcement. For example the Inspector General for the Department of Justice has reported that the FBI circumvented its National Security Letter (NSL) authority by using "exigent letters" to obtain information with the promise that the agent had already requested a grand jury subpoena or an NSL.[39] To prevent such abuse, all requests for "emergency" voluntary disclosures under ECPA should clearly state that compliance with the request is voluntary and ECPA should require thorough documentation and reporting of all such requests.

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

Conclusion

---

[37] 18 U.S.C. 2515.

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

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

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

Department of Justice

STATEMENT OF

JAMES A. BAKER
ASSOCIATE DEPUTY ATTORNEY GENERAL
UNITED STATES DEPARTMENT OF JUSTICE

BEFORE THE

SENATE JUDICIARY COMMITTEE

AT A HEARING ENTITLED

**The Electronic Communications Privacy Act:
Promoting Security and Protecting Privacy in the Digital Age**

PRESENTED

SEPTEMBER 22, 2010

Good afternoon, Chairman Leahy, Ranking Member Sessions, and Members of the Committee. Thank you for the opportunity to testify on behalf of the Department of Justice. We welcome this opportunity to provide you with our perspective about how the Electronic Communications Privacy Act, as amended (ECPA), is used today by investigators and prosecutors throughout the country. Since its enactment nearly 25 years ago, ECPA has become a vital tool for the law enforcement community. It is also important for national security, law enforcement, and cyber security activities, as well as for protecting privacy interests.

As you know, ECPA is part of a set of laws that controls the collection and disclosure of the content of communications, such as phone calls and emails, as well as content that has been stored remotely. Passed in 1986 and repeatedly amended over the years, ECPA also regulates the collection and disclosure of certain non-content information about communications, which is sometimes referred to as "metadata." These laws (1) restrict communication service providers' ability to disclose such information, and (2) outline the rules governing access to that information by both government and private entities.

Department of Justice attorneys specializing in ECPA regularly give advice about all manner of investigations, including terrorism, drug trafficking, violent crime, kidnappings, computer hacking, sexual exploitation of children, organized crime, gangs, and white collar offenses. Crucial evidence of all of these types of crimes is in the hands of telecommunications and other providers, and with few exceptions, ECPA places the same limitations on the government's access to those records regardless of what type of matter is under investigation. Judgments and balances made in ECPA inevitably will affect not only law enforcement generally, but also critical national security investigations and cyber security programs, as well as the interests of private sector companies trying to protect critical data.

ECPA's provisions are also important for protecting individual privacy. For example, ECPA places limitations on the government's access to content and metadata pertaining to communications of customers and subscribers. Section 2702 of Title 18, United States Code, generally prohibits Internet and telephone service providers from voluntarily divulging such information to the government, with certain limited exceptions. In addition, section 2703 sharply limits the ability of the government to obtain those records even using a subpoena—which, in other investigative contexts, is the most common method for obtaining records held by a third party, such as financial and medical records. Instead, before most metadata can be compelled, section 2703 requires a court order based upon a specific judicial finding of relevance and materiality. ECPA also places some limitations on the circumstances and degree to which Internet and telephone service providers may disclose content to private parties.

In light of the importance of ECPA's provisions today, and the balance the statute strikes between various important interests, there are several considerations we respectfully urge Congress to keep in mind before undertaking major changes to the statute.

1. Public Safety Must Not Be Compromised.

All of us rely on the government to protect our lives and safety by thwarting national security and cyber threats and punishing and deterring dangerous criminals. Information related

to communications, both content and non-content information, is often critical to the investigations that are necessary to achieve these objectives. Compulsory process served on communications companies can be a key tool in thwarting cyber criminals, protecting children from sexual exploitation, and neutralizing terrorist threats.

The type of information that investigators obtain from service providers includes both the content of communications as well as metadata – non-content information – about those communications. Such metadata often represents the cornerstone of an investigation. Investigators use metadata to learn important facts about a suspect's associates and activities and to weed out individuals who are not involved in unlawful activity so that limited investigative resources may be directed most efficiently. Metadata can show investigators with whom a suspect communicates, at what time, and for how long. Importantly, investigators often use such non-content information as a basis for requesting authorization from a court for more intrusive types of searches and surveillance, such as stored communication content or a wiretap. It is essential that investigators have the ability to obtain metadata about a suspect's activities in a timely and efficient manner based upon a level of factual predication – and pursuant to an authorization – that is commensurate with the fact that most requests for metadata occur at early stages of an investigation. If it is unduly difficult for investigators to obtain metadata, it may hamper the government's ability to respond promptly and effectively to real threats.

Here is one example of how communications metadata can help in an investigation. In April 2010, a Sheriff's Office Uniformed Patrol Lieutenant in Baton Rouge, Louisiana attempted to stop a suspect. The suspect shot the Lieutenant through the neck and fled. An investigation later identified the suspect, and an arrest warrant was obtained for attempted first degree murder of a police officer. In their efforts to locate and arrest the suspect, officers determined that the suspect used several cell phones to communicate with his girlfriend and other associates. Officers used ECPA subpoenas and court orders to the cell phone companies to obtain calling records and location records. This information ultimately allowed officers to confirm the suspect's location.

As a second example, in a DEA investigation in 2008, investigators seized approximately $900,000 from a tractor trailer during a traffic stop in Detroit. After gaining the cooperation of the driver, the DEA identified a number of cellular telephones with "Push-To-Talk" features that were being used to contact organizational leaders in Mexico. Telephone toll record analysis along with additional investigation revealed a pattern of switching cellular telephones to avoid detection and law enforcement interception. This technique effectively prevented the agents from obtaining the authority to conduct wiretap intercepts on these phones. The DEA was still able to use ECPA process to obtain cell site data to identify members of the criminal organization near Detroit. Obtaining this information was critical to this outcome. Without the use of telephone toll record data, cell site information, and pen register data, the DEA would not have been able to identify these dangerous drug traffickers.

ECPA legal process has also proven instrumental in thwarting child predators. In a recent undercover investigation, an FBI agent downloaded images of child pornography and used an ECPA subpoena to identify the computer involved. Using that information to obtain and execute a search warrant, agents discovered that the person running the server was a high school

special-needs teacher, a registered foster care provider, and a respite care provider who had adopted two children. The investigation revealed that he had sexually abused and produced child pornography of 19 children: his two adopted children, eight of their friends, three former foster children, two children for whom he provided respite care, and four of his special needs students. This man pleaded guilty and is awaiting sentencing.

One final example illustrates how communications service providers' records are important not only to regular criminal investigations, but also to keeping our law enforcement officers safe. Recently, a homicide detective in Prince George's County, Maryland, reported that, at 2:00 a.m., he and his partner were chasing a man wanted for a triple murder. Consistent with ECPA, they made use of cell tower information about the fugitive's mobile phone. Having this information immediately accessible increased officer safety and allowed them to marshal available law enforcement resources effectively. They successfully captured the fugitive in nine hours without placing officers, or the public, at undue risk.

These are only a few of the countless examples of how ECPA has become a critically important public safety tool. Accordingly, we think it is important that any changes to ECPA be made with full awareness of whether, and to what extent, the changes could affect the critical goal of protecting public safety. If an amendment were to unduly restrict the ability of law enforcement to quickly and efficiently determine the general location of a terrorist, kidnapper, child predator, computer hacker, it would have a very real and very human cost.

As the Department of Commerce notes in its testimony, some U.S. companies say that they find themselves at a competitive disadvantage in foreign markets because some foreign countries have misperceptions about the terms on which U.S. government agencies may obtain communications information. As a result of these misperceptions, U.S. firms have said that they have difficulty offering cloud computing services in some foreign markets if personal information is to be stored in the United States. While not discounting economic considerations, the Department believes that such concerns must be addressed without inadvertently compromising its ability to carry out its mission of enforcing the law and protecting the public from harm.

2. ECPA is Important in Law Enforcement's Efforts to Prevent Privacy Crimes.

Americans today face a wide range of threats to their privacy interests. In particular, foreign and domestic actors of all types, including cyber criminals, and, at times, the governments that harbor them, routinely and unlawfully access data pertaining to individuals that most people would regard as highly personal and private. Unlike the government – which must comply with the Constitution and laws of the United States and is accountable to Congress and other oversight bodies – malicious cyber actors do not respect our laws or our privacy. The government has an obligation to prevent, disrupt, deter, and defeat such intrusions. ECPA plays a key role in that effort.

Criminals pose a significant day-to-day threat to the privacy of American computer users. For example, many Americans' computers are, unbeknownst to them, part of a "botnet" – a collection of compromised computers under the remote command and control of a criminal or

foreign adversary. Criminals and other malicious actors can extensively monitor these computers, capturing every keystroke, mouse click, password, credit card number, and e-mail. Unfortunately, because many Americans are using such infected computers, they are suffering from an extensive, pervasive, and entirely unlawful invasion of privacy at the hands of these actors.

Investigators seeking to protect Americans from this type of crime online must work within ECPA's access restrictions and make use of its tools. For example, the FBI is investigating a vast botnet that was active in 2007 and 2008 and consisted of approximately fifteen million infected computers. The criminals used it to send spam messages to perpetrate online stock manipulation schemes and to illegally sell online pharmaceuticals. Researchers estimate that this botnet was responsible for 20 percent of all spam email in the first quarter of 2008, and that the criminal enterprise collected profits of $3.5 million per year from the online pharmaceutical sales alone. Investigators used ECPA subpoenas and pen register/trap and trace orders to map the administrative structure of the botnet and identify those servers that should be searched with warrants. ECPA subpoenas also revealed that a single customer leased the most important servers and identified certain communication accounts used by that person. ECPA court orders identified that person's IP address.

Similarly, the FBI initiated an investigation in 2008 into an extensive identity theft and computer intrusion scheme. A gang of identity thieves obtained personal data from online sources, such as identity databases, credit reports, and land records. Armed with this information, the criminals contacted the victims' banks, impersonated the victims, and transferred huge sums of money to accounts they controlled. The scheme went on for at least three years and resulted in an estimated $30 million in losses. Investigators used ECPA subpoenas and court orders to obtain subscriber information and trace communications. They also used ECPA court orders to gain real-time location information for the suspects' mobile phones, which helped to identify and ultimately arrest them. To date, fourteen people (eight in the United States) have been convicted, although the primary suspect remains at large.

Safeguarding privacy includes keeping information from criminals and others who would abuse that information and cause harm. Investigating and stopping this type of criminal activity is a high priority for the Department, and investigations of this type require the use of tools that ECPA regulates. In particular, pen register and trap and trace orders have proven invaluable in mapping the complex web of command and control servers used by criminals. These tools, commonly used at the start of an investigation, allow law enforcement to gather the building blocks necessary to establish probable cause for more advanced investigative measures, such as wiretaps. Were ECPA to be amended in a way that increases the burdens on the government's use of these tools, this could decrease our ability to protect citizens from this type of privacy crime, and, consequently, decrease privacy overall.

3. Significant ECPA Changes Must Be Carefully Considered.

The Department of Justice stands ready to work with the Committee as it considers whether changes to ECPA are appropriate. But we urge Congress to proceed with caution; and to avoid amendments that would disrupt the fundamental balance between privacy protection and

public safety. Congress should refrain from making changes that would impair the government's ability to obtain critical information necessary to build criminal, national security, and cyber investigations, particularly if those changes would not provide any appreciable or meaningful improvement in privacy protection. In addition to compromising consumers' privacy, these types of crimes have significant economic ramifications on business and financial institutions that suffer millions of dollars in losses.

Although it was enacted in 1986, Congress substantially amended ECPA in 1994, and then again in 2001; with each amendment, ECPA evolved to account for changing times. The 2001 amendments, for example, extended the protections afforded to the collection of numbers dialed on a phone to the collection of e-mail addresses. In addition, Congress has also amended ECPA on a smaller scale on several additional occasions, most recently in 2009, when this Congress updated its provisions to permit U.S. investigators to assist foreign law enforcement.

Moreover, the statute, as written in 1986, has proven adaptable over time, although some courts have struggled with applying its terms to the Internet and other modern communications and information technologies. To give one example of ECPA's adaptability, in 1986, most electronic mail was sent without using the Internet by relying on dial-up online services or store-and-forward networks. When e-mail shifted to the Internet, ECPA easily accommodated it and came to offer equivalent privacy protections. In fact, there was no serious legal debate about whether ECPA applied to the Internet; its general language left room for no other conclusion than that it did.

To give another example, ECPA was forward-looking and flexible on the issue of cloud computing. With cloud computing, data is stored and processed by online services, rather than by one's personal computer. Yet ECPA was written at a time when this "remote computing" was relatively new. Because of the expense and complexity of computers in 1986, companies routinely sent their sensitive customer and payroll data to third parties for storage and processing. Thus, ECPA has explicitly covered so-called "remote computing services" since its enactment almost 25 years ago. Of course, as discussed in the testimony of my colleague from the Department of Commerce, cloud computing has expanded dramatically in recent years, and the number of people using such services has continued to grow.

It is true that ECPA and other statutes that regulate the collection and disclosure of communications, communications metadata, and stored data constitute a complex legal regime. Such complexity raises serious issues for investigators and privacy advocates alike. But ECPA is complicated because it endeavors to reconcile many competing priorities in a technologically complex realm. EPCA recognizes many distinctions that are critical to maintaining the proper balance between privacy and public safety.

For all these reasons, we believe Congress should proceed carefully before enacting changes that may delay time-sensitive investigations and make crucial evidence and information harder to obtain.

* * *

Technology continues to evolve, and it is natural to ask whether changes to ECPA are appropriate. Should Congress determine that ECPA should be amended again to address changes in technology, amendments will need to adequately protect privacy while not compromising the government's ability to protect the public from terrorists, spies, malicious cyber actors, and other criminals in a timely, efficient, and effective manner. Additionally, the concerns raised by U.S. commercial firms regarding international competition and the economic challenges they face, as highlighted in the testimony of the Commerce Department, must also be taken into account.

The law enforcement agents and prosecutors who work with ECPA on a daily basis have considerable knowledge about the statute's benefits and shortcomings. We believe that knowledge and combined experience will be invaluable to the Committee as it considers particular amendments to ECPA, and what the collateral effects of such amendments are likely to be.

We therefore appreciate the opportunity to share with you information about how the Department uses the legal procedures under ECPA to fight crime, improve public safety, and defend the national security while protecting the privacy of all Americans. We look forward to continuing to work with Congress as it considers these matters.

This concludes my remarks. I would be pleased to answer your questions.

Senate Committee on the Judiciary

Liberties

Hearing on ECPA Reform

Testimony of Professor Matt Blaze

September 22, 2010

1. Introduction and Background

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

I am currently an associate professor of computer and information science at the University of Pennsylvania in Philadelphia, where I serve as director of the Distributed Computing Laboratory and conduct research on computer security, cryptography, network communication, and surveillance technology. Prior to joining the faculty at Penn, I was for 12 years a member of the research staff at AT&T Labs (previously known as AT&T Bell Labs) in New Jersey. I have a PhD in computer science from Princeton University, a Masters degree from

Columbia, and I completed my undergraduate studies at the City University of New York.

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

There is perhaps no more ubiquitous symbol of our highly connected society than the cellular telephone. Over the course of only a few short decades, mobile communication devices have evolved from being little more than an expensive curiosity for the wealthy into a basic necessity for most Americans, transforming the way we communicate with one another, do business, and obtain and manage the increasing volume of information that is available to us.

According to recent estimates, there are today more than 285 million active wireless subscriber accounts in the United States. Many households now forgo traditional "landline" telephone service, opting instead for cellular phones carried by each family member. Wireless carriers have strained to keep up with the explosive demand for cellular service, in many areas deploying new infrastructure (most visibly cellular antenna towers) as quickly as they can find places to put it.

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

Many of the most important and innovative new applications and services that run on mobile devices take advantage of the ability to quickly and automatically detect the user's location to provide location-specific information and advice. At the same time, cellular providers calculate where

phones in their networks are located (and how they move) to manage various network functions and to plan where new infrastructure is required.

2. Wireless Location Technologies

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

There are two different technological approaches for calculating the location of a cell phone. In one approach, the user's phone calculates its own location using special GPS satellite receiver hardware built in to the handset. In the other, the cellular system calculates the location of the phones that are active

in the network, using the normal cellular radio interfaces and without explicit assistance from the users' devices.

2.1 Handset-based GPS

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

Whether or not the calculated GPS location of a handset is sent to the network (or any other third party) depends on the application software that the phone is running. Some applications, as a matter of course, may periodically transmit their location to external services. For example, a mapping application might send its current GPS-calculated location to a network-based service in order to discover, say, the locations of nearby businesses that might be of interest to the user. Network-based services that make use of a phone's GPS location might be offered by the cellular carrier or by a third party, internet-based entity.

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

2.2 Network-based location

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

The precision with which a handset can be located by network-based (non-GPS) approaches depends on a range of factors, but has been steadily improving as technology has advanced and as new infrastructure is deployed in cellular

networks. Under some circumstances, the latest generation of this technology permits the network to calculate users' locations with a precision that approaches that of GPS.

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

2.2.1 Sector identification

At the most basic level, cellular providers record the identity of the particular base station (or sector) with which a cellular phone was communicating every time it makes or receives a call and whenever it moves from one sector to another. How precisely this information by itself allows a phone to be located depends on the size of the sector; phones in smaller sectors can be located with better accuracy than those in larger sectors.

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

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

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

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

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

The decreasing size of cell sectors is not the only factor making network-based location more accurate. New technology allows cellular network providers to

locate not just the sector in which the users' wireless device is located, but its position *within* the sector. By correlating the precise time and angle at which a given device's signal arrives at multiple sector base stations, new technology now makes it practical for a network operator to pinpoint a phone's latitude and longitude at a level of accuracy that can approach that of GPS.

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

Although these enhanced location technologies are not yet universally available in every network, wireless carriers are deploying them because they provide information that is extremely valuable in managing their networks and businesses. By tracking more precisely where mobile devices are located

within sectors (and the directions they are moving), a carrier can better identify where new infrastructure is required, where old infrastructure is redundant, and how and where their customers use different wireless service offerings.

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

3. Cell Phone Location and Law Enforcement Surveillance

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

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

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

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

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

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

The Electronic Communications Privacy Act of 1986: Principles for Reform

J. Beckwith Burr[1]

Background

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

---

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Principles

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

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

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

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

Principle 1: Access to Content in Transit and in Storage

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

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

---

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

16/ Companies often impose email retention policies that require employees to preserve emails for several months before deletion. Contoural White Paper, *How Long Should Email Be Saved?*, at 5 (2007), *available at* http://www.umiacs.umd.edu/~oard/teaching/708x/spring09/t1.pdf. ("Most companies come to the conclusion that many messages should be retained for a few years for business productivity purposes.").

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

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

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

---

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

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

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

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

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

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

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

---

23/ 18 U.S.C. § 2703(a).

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

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

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

180 days old.[27/] Likewise, while as a practical matter law enforcement must secure a warrant to access documents on a personal computer, under ECPA, a mere subpoena issued to a third party will suffice to access confidential documents stored remotely on the computers of a cloud computing service provider.[28/]

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

---

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

---

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

49/ 18 U.S.C. § 2511(2)(g)(1).

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

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

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

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

Principle 2: Access to Mobile Location Data

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

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

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

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

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

---

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

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

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

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

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

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

---

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

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

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

58/ *Id.*

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

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

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

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

---

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

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

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

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

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

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

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

---

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

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

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

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

Principle 3: Access to Transactional Data

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

---

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

[68] Most courts have held that prospective information requires a showing of probable cause. See *supra* note_ 63. Law enforcement requests for retrospective location data are often combined with requests for prospective data. *See, e.g., In re Application Of The United States Of America For An Order Directing A Provider Of Electronic Communication Service To Disclose Records To The Government*, 534 F. Supp. 2d 585, 589 (W.D. Pa. 2008); *In re Application of U.S. for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone*, 460 F. Supp. 2d 448, 453 (S.D.N.Y. 2006).

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

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

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

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

---

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

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

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

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

[74] 18 U.S.C. § 3123(a).

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

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

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.[77/]

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

---

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

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

77/ 18 U.S.C. § 2703(d).

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

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

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

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

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

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

79/ 18 U.S.C. § 2703(c)(2).

80/ *Id.*

81/ 18 U.S.C. § 2703(c)(3).

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

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

Conclusion

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

---

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

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

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
Senate Committee on the Judiciary

September 22, 2010

Hearing on
The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age

Chairman Leahy, Ranking Member Sessions, and Members of the Committee:

The undersigned public interest groups, think tanks, and advocacy organizations respectfully submit these comments to the United States Senate 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.digitalddueprocess.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.digitalddueprocess.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

Statement of

The Computer & Communications Industry Association
(CCIA)

Before the

Committee on the Judiciary
U.S. Senate

"The Electronic Communications Privacy Act:
Promoting Security and Protecting Privacy in the Digital Age"

September 22, 2010

As a non-profit association active in policy debates for over 35 years and whose membership includes companies from all parts of the telecommunications and information technology ecosystem, the Computer & Communications Industry Association ("CCIA") cares deeply about both the economic and civil liberties consequences of privacy regulations and laws. CCIA has been concerned with privacy since its founding and has been a vocal advocate in recent years against overreaching government surveillance. Ensuring the privacy of users and consequently earning their trust is essential for our industry to flourish. However, we also recognize that poorly worded regulations or outdated laws can have disastrous consequences not just for user privacy, but for legitimate, cutting-edge business practices as well.

In today's Internet age, application of the Electronic Communications Privacy Act[1] ("ECPA") to real life situations proves increasingly problematic. Specifically, the information technology and telecommunications industries face two major areas of difficulty and uncertainty in the context of ECPA compliance: (1) the treatment of geolocational information about individuals; and (2) the levels of protection for data in a cloud computing environment. Social networking is yet another alternative platform for private personal communications not addressed by ECPA. Application of ECPA to such new and increasingly prevalent technologies is far from clear. However, these difficulties are of no surprise. The unique challenges and difficulties surrounding these new technologies could not have been foreseen in 1986 when ECPA was enacted. These new and exciting technologies represent leaps in

---

[1] 18 U.S.C. 2510, *et seq.*

innovation and business practices from what Congress was looking at over 25 years ago when it drafted ECPA. As such, ECPA urgently needs a significant update to bring it into harmony with the early 21st century realities of digital electronic commerce and communications.

Service providers need solidified standards on how to handle consumer information and data, especially in the cases of geolocational information and cloud computing. Currently, providers are left with little to no guidance in how to balance operational needs, governmental requirements, and consumers' privacy and security. For instance, certain law enforcement legislation currently requires service providers to maintain large databases of retained consumer information. These requirements not only place extraordinary burdens on the provider companies themselves, but also weaken consumer trust in both the companies and the Internet as a whole. Microsoft Associate General Counsel Michael Hintze recently noted that ECPA has made it difficult for Microsoft to, "market itself as protecting users' privacy."[2] Companies across the information technology and telecommunications industries face the same or similar difficulties.

Mobile devices have fundamentally changed the way we communicate and provide a new way of tracking an individual's location, movements, and patterns of activity. Today, cell phones and mobile broadband devices generate a steady stream of location data necessary both for basic network operations and for innovative location-based services. This location data can be intercepted in real-time and

---

[2] Louis Trager, "Civil Libertarians Wish CDT-Led Coalition Would Go Further on Changing ECPA," Warren's Washington Internet Daily, Vol. 11, No. 165 (August 26, 2010).

stored in logs. Service providers in the telecommunications and information technology industries need a clear standard governing the terms under which they must hand over subscribers' geolocational data to law enforcement authorities. Currently, ECPA lacks such a standard. The sensitivity of geolocational data makes certainty and clarity in its handling that much more important. The collection of an individual's real-time locational data reflecting that person's current exact location is much more intrusive than the collection of past data such as a receipt indicating that person bought a venti latte from a certain Starbucks location this morning. Further, and potentially even more troubling considering the sensitivity of the information, consumers do not always know what kind of information is being collected about them and sometimes don't even know that any information is being collected at all. With more people using smartphones,[3] many of which contain global positioning systems ("GPS") that allow for nearly exact tracking,[4] a growing number of consumers are likely to have their locational information tracked and collected without being aware of it.

---

[3] The percentage of U.S. consumers owning smartphones has risen from 21% in October 2007 to 32% in December 2008 and 42% in December 2009. Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, Annual Report and Analysis of Competitive Market Conditions With Respect to Mobile Wireless, Including Commercial Mobile Services, WT Docket No. 09-66, *Fourteenth Report*, FCC 10-81 at 92 (rel. May 20, 2010). Additionally, CTIA's "Mid-Year 2009 Wireless Indices Report" indicates that 40.7 million smartphones were in service as of June 30, 2009. *Id.*

[4] While GPS is not the only way of tracking and collecting subscribers' locational information, it can provide a more exact and precise location than tracking through triangulation. Providers can track and collect locational information through triangulation by pinging a mobile device with a signal sent from multiple service towers in order to determine where between those towers the device is located.

Cloud computing is another relatively recent technological development that creates widespread legal and business uncertainty regarding compliance with ECPA. Cloud computing utilizes the Internet's high-speed transportation paths to allow users to create, edit, and store data remotely on servers located elsewhere in the world rather than on one's own computer resources. Ten years ago, let alone twenty five years ago when ECPA was enacted, cloud computing was inhibited by slow data transmission and high storage costs. However, since that time data transmission speeds have increased exponentially and the price of data storage has dropped significantly. Data transmission speeds have now increased to the degree of allowing enterprise users nearly instantaneous access to remotely stored data, thus making cloud computing a viable option in the business world. Similarly, cheaper storage costs and search functionality have facilitated the saving and accessing of many years' worth of e-mail messages. Consumers do not necessarily have a lower expectation of privacy with respect to older e-mails as opposed to more recent messages. Thus, the continually increasing speed of data transmission coupled with a decreasing price for storage has created a setting where cloud computing now provides an attractive and affordable alternative for business users to augment or replace costly on-site computer resources. This is especially key for new and small businesses where the start-up costs of purchasing and maintaining on-site computer resources could be prohibitive.

Information technology and telecommunications companies have responded to the increased interest of consumers and enterprise users by developing and offering a wide array of cloud computing services which can be broken down into

three categories: (1) Software-as-a-Service ("SaaS"); (2) Platform-as-a-Service ("PaaS"); and (3) Infrastructure-as-a-Service ("IaaS"). Recent years have seen a proliferation of free or very low cost SaaS services such as e-mail (i.e. G-mail and Hotmail) and personal financial (i.e. mint.com) software that utilize cloud resources to lower prices and the Internet's reach to enhance functionality. E-mail services today provide millions of consumer and business users a nearly limitless storage and access from any computer, all for free or a very low cost. PaaS delivers a computing platform and software stack over the Internet that provides programmers and information technology professionals the resources they need to develop and deploy applications without the added costs and complexity of managing their own hardware and software layers on-site. Some of the biggest names in the Internet industry have noticed the demand for PaaS and now Amazon,[5] Google,[6] and Microsoft,[7] Yahoo!,[8] and others, all offer competitive PaaS services. Lastly, IaaS offers full-service virtual information stacks designed to replace a company's entire server room and network through virtualization technology.

---

[5] Amazon offers PaaS cloud computing services under the name Amazon Web Services. More information on Amazon Web Services can be found online at http://aws.amazon.com/cloudfront.

[6] Google offers PaaS cloud computing services under the name Google Apps. More information on Google Apps can be found online at http://www.google.com/apps/ intl/en/business/index.html.

[7] Microsoft offers PaaS cloud computing services under the names Microsoft Windows Azure and Microsoft Business Productivity Online Suite. More information on Microsoft Windows Azure can be found online at http://www.microsoft.com/windowsazure/. More information on Microsoft Business Productivity Suite can be found online at https://www.microsoft.com/online/business-productivity.aspx.

[8] Yahoo! offers PaaS cloud computing services under the name Yahoo! Developer Network. More information on the Yahoo! Developer Network can be found online at http://developer.yahoo.com/.

Consumers and businesses have increasingly embraced the benefits that cloud computing provides. Cloud computing services allow users more mobility and greater ability to collaborate with others. However, accompanying these advances is a grave concern over privacy: 90% of those excited for cloud computing are also concerned about data security in the cloud.[9] In order to ease these concerns over privacy and security in the cloud, ECPA's applicability to data contained in the cloud must be clarified. ECPA must be updated to give service providers clear standards on how to handle consumers' information in the cloud. Without such clarity, the skepticism of consumers, and especially enterprise users, will ultimately hinder adoption of this very valuable Internet tool.

So long as privacy rules governing the Internet remain unclear, many consumers will remain wary of adopting, or more heavily utilizing, broadband and valuable Internet-based resources. The digital age has produced an Internet that offers a wide range of valuable tools including communication, unfettered information exchange, electronic commerce, civic participation, and online tax preparation. Consumers better realize the benefits of the digital age when they fully participate in what the Internet has to offer, but if users are afraid to use their personal data online, most, if not all, of these benefits are lost.

The skepticism of enterprise users can also be damning to innovation and growth on the Internet. Enterprise users have understandably high thresholds for competitive privacy and security that serve as a major obstacle to the continued

---

[9] "Microsoft Urges Government and Industry to Work Together to Build Confidence in the Cloud," Microsoft press release, Jan 20, 2010, available online at http://www.microsoft.com/presspass/press/2010/jan10/1-20BrookingsPR.mspx (last accessed on August 26, 2010).

adoption of cloud computing services. Unless the current sense of uncertainty surrounding ECPA's application to cloud computing is cured, and adequate and clear protections are provided, skeptical enterprise users will shy away from using cloud computing services to their fullest potential. Enterprise users account for significant amounts of capital and innovative capacity. Thus, discouraging these users from fully adopting the resources offered by cloud computing drastically hurts overall Internet innovation and growth.

The conflicting, ambiguous and, at times, misguided judicial approach to the Fourth Amendment's applicability in the Internet realm highlights the importance of clarifying ECPA for the 21st Century. The Fourth Amendment has historically protected postal mail from governmental inspection during delivery. However, courts have exhibited reluctance to extend this expectation of privacy to electronic communications. While some courts have found Fourth Amendment protection for electronic communications, others have declined to do so, and the Supreme Court of the United States has punted the issue at least once. Consumers have an expectation of privacy in their communications and generally expect the same protections for e-mail as for a handwritten letter or phone call. In a world where e-mail and other electronic communications have become the norm, an absence of Fourth Amendment protections for electronic communications will shake consumer confidence and discourage broadband adoption.

Some court decisions declining to extend an individual's reasonable expectation of privacy to electronic communications highlight the troublesome judicial approach courts have taken to the Fourth Amendment in the context of the

Internet realm. In *In re Application of U.S. for Search Warrant for Contents of Electronic Mail*,[10] a federal district court in Oregon held that law enforcement officials do not have to inform an e-mail account holder of a warrant to search the contents of his or her e-mail account. Instead, the court held that notice to the Internet access provider ("IAP") was sufficient because the information sent by the subscriber passes through and may be stored on the IAP's servers. As such, the court held that the communication was no longer private information contained in the home. Similarly, in *Rehberg v. Paulk*,[11] the Eleventh Circuit held that a person loses a reasonable expectation of privacy in his or her e-mails once the e-mail is sent to and received by another party. Thus, the Eleventh Circuit found a subpoena to the subscriber's IAP for such e-mails not to violate the Fourth Amendment because the e-mails were subpoenaed directly from the IAP and not "an illegal [search of the defendant's] home computer for e-mails."[12]

On the other hand, two federal appellate courts have exhibited an understanding that makes for more appropriate national policy. In *Warshak v. U.S.*,[13] the Sixth Circuit found e-mails stored in a web-based e-mail account to be protected by the Fourth Amendment. Likewise, in *Quon v. Arch Wireless* ("*Quon I*"),[14] the Ninth Circuit found a reasonable expectation of privacy to exist in a person's text messages stored with a service provider. Although the Supreme Court of the United

---

10 *In re Application of U.S. for Search Warrant for Contents of Electronic Mail*, 665 F.Supp.2d 1210 (D.Or. 2009).

11 *Rehberg v. Paulk*, 598 F.3d 1268 (11th Cir. 2010)

12 *Id.* at 1282.

13 *Warshak v. U.S.*, 490 F.3d 455 (6th Cir. 2007), *rev'd en banc on other grounds*, 532 F.3d 521 (6th Cir. 2008).

14 *Quon v. Arch Wireless*, 529 F.3d 892 (9th Cir. 2008) ("*Quon I*"), *rev'd on other grounds City of Ontario v. Quon*, 130 S.Ct. 2619 (2010).

States reversed *Quon* in *City of Ontario v. Quon* ("*Quon II*"),[15] it did so on other grounds. In fact, the Supreme Court explicitly declined to address whether an employee has privacy expectations for communications made on employer-provided equipment due to a concern over the uncertain future implications of any such holding.[16] Nevertheless, although it side-stepped the issue of privacy expectations, some fear that *Quon II*'s holding that a police department's search of text messages on an employee's department-issued device was reasonable reflects a Supreme Court shying away from applying the Fourth Amendment to new technologies.[17]

Similarly, a federal district court extended to cell phone tracking a recent D.C. Circuit holding that requires a warrant for government use of GPS tracking devices to monitor individuals' movements for an extended period of time. In *U.S. v. Maynard*,[18] the D.C. Circuit held that federal agents must obtain a search warrant prior to placing a GPS tracking device on a vehicle parked on a private driveway which transmitted the vehicle's locations to federal authorities every ten seconds for a complete month. The D.C. Circuit specifically noted the extensive intrusiveness of such extended round-the-clock tracking.[19] In *In re Aplication of U.S. for Order*

---

15 *City of Ontario v. Quon*, 130 S.Ct. 2619 (2010) ("*Quon II*").

16 *Quon II* at 2630 (2010).

17 *See e.g.* "Written Statement of Marc J. Zwillinger, Partner, Zwillinger Genetski LLP, before the U.S. House of Representatives Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights, and Civil Liberties," at 7, Hearing on *ECPA Reform and the Revolution in Location Based Technologies and Services*, June 24, 2010, available online at http://judiciary.house.gov/hearings/pdf/Zwillinger100624.pdf.

18 *U.S. v. Maynard*, No. 08-3030, 2010 WL 3063788 (D.C. Cir. Aug. 6, 2010)

19 *Id.* at *12 (finding that it goes beyond the mere observation of a passerby or the following for a single journey to, "another thing entirely...to pick up the scent

Authorizing Release of Historical Cell-Site Information, the Eastern District of New York subsequently applied *Maynard*'s reasoning to reject a government request for an order directing a cell phone service provider to turn over an individual's historical cell phone location information from a two-month period.[20] Finding such cell phone tracking just as intrusive as *Maynard*'s GPS tracking, the Eastern District concluded that, "[t]he Fourth Amendment cannot properly be read to impose on our populace the dilemma of either ceding to the state any meaningful claim to personal privacy or effectively withdrawing from a technologically maturing society."[21]

A judiciary that is, at best, unsure how to apply the Fourth Amendment in the context of electronic communications highlights the need for clarity in the statutory protections ECPA provides in the electronic realm. However, the uncertainty surrounding ECPA described above has resulted in magistrate judges across the country facing difficulties with the everyday application of ECPA. At a June 24, 2010 hearing before the Subcommittee on the Constitution, Civil Rights, and Civil Liberties of the House of Representatives' Committee on the Judiciary, the Honorable Stephen Wm. Smith, a U.S. Magistrate Judge in the Southern District of Texas, testified as to problems he sees first hand in the everyday judicial application of ECPA.[22] Judge Smith's oral testimony raised two primary concerns: (1) the lower

---

again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine.")

20 *In re Application of U.S. for Order Authorizing Release of Historical Cell-Site Information*, No. 10-MJ-0550 (JO), slip op. (E.D.N.Y. Aug. 27, 2010).

21 *Id.* at 30.

22 Video of the House Judiciary Committee's Subcommittee on the Constitution, Civil Rights, and Civil Liberties hearing on *ECPA Reform and the Revolution in*

courts' lack of guidance from higher courts; and (2) the lack of notice provided to the person subjected to the intrusion. With regard to the lower courts' lack of guidance, Judge Smith noted that few appellate courts have actually dealt with ECPA and none have dealt with the issue of cell phone location data.

The uncertainty surrounding the Fourth Amendment and ECPA in the context of electronic communications has resulted in an unfair differential treatment of e-mail that also serves as an implicit preference for last generation hard-copy communications. Instead, a platform-neutral approach should be taken to consumers' privacy expectations in regard to their communications and electronic data. The Fourth Amendment provides greater Fourth Amendment protection to older means of communications, such as postal mail and telephone calls, while ECPA provides lesser statutory protections for e-mails. If such a framework continues, consumers will continue to rely on paper transactions in order to retain the greater privacy protections provided by the Fourth Amendment at the cost of lesser adoption of more efficient and "greener" communications technologies.

Privacy rules also need updating in order to fully appreciate the benefits of technical developments made in health-related Internet technologies ("health IT"). Health IT can provide many benefits to American patients through means of remote monitoring of and consultation with patients, collaboration amongst providers, and electronic prescriptions. These benefits are compounded in sparsely populated rural areas where patients may face great difficulties in reaching providers in

---

location Based Technologies and Services, held on June 24, 1010, can be found at http://judiciary.house.gov/hearings/hear_100624.html.

person. However, without certainty in how their most sensitive and personal medical information is treated, patients will be reluctant to utilize such beneficial technologies.

Additionally, the lesser statutory protections provided by ECPA prove arbitrary in the context of the early 21st century. The 180-day window of protection provided to e-mails may have made sense in the 1980s when e-mails were downloaded onto the hard drives of user's computers rather than left sitting passively on servers. However, today a massive reliance on web-based e-mail exists where all e-mail resides on third-party servers instead of on the user's own computer.

Lastly, even though some government agencies have set up policies providing for heightened standards for searches, ECPA still must be updated in order to provide some mechanism to ensure such policies are followed. For instance, while the U.S. Department of Justice ("DOJ") has a policy to seek prospective real-time information under a warrant standard, a recent ACLU Freedom of Information Act request shows that certain jurisdictions are using a lower standard.[23] This situation exhibits the problem of relying on agency policies: a policy is just a policy. Without updating ECPA to require the heightened standard, there is no statutory authority to point to or make that standard mandatory.

In updating U.S. privacy laws to provide legal certainty and definitional clarity for electronic communications in the 21st century, CCIA supports two general

---

23 "ACLU Lawsuit to Uncover Records of Cell Phone Tracking," ACLU website, June 28, 2010, available online at http://www.aclu.org/free-speech/aclu-lawsuit-uncover-records-cell-phone-tracking.

propositions. First, CCIA supports the application of Fourth Amendment protections from undue search and seizure to electronic communications. Second, CCIA also supports the Digital Due Process Coalition's ("DDP") four recommendations for ECPA reform.[24]

(1) Requiring law enforcement to obtain a search warrant based on probable cause before obtaining private communications or documents stored remotely;

(2) Requiring law enforcement to obtain a search warrant before tracking people's location via cell phones or other devices;

(3) Requiring law enforcement to submit proof that the information sought is relevant to a criminal investigation before electronic surveillance begins; and

(4) Requiring law enforcement to submit proof that the information sought is not only relevant to a criminal investigation, but is in fact needed, before it may obtain bulk information about broad categories of unknown telephone or Internet users.

In the context of these four proposals, an exclusionary definition should be used to define what information makes up "mobile location information." Further, the definition of a "warrant" would use already existing definitions as a touchstone and notice of a warrant, with certain exceptions, would be required at a reasonable time.

---

[24] "Specific Background on ECPA Reform Principles," Digital Due Process Coalition, available online at http://www.digitalddueprocess.org/index.cfm?objectid=C00D74C0-3C03-11DF-84C7000C296BA163.

Statement of the Constitution Project for the Senate Judiciary Committee Hearing on "The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age"

September 22, 2010

The Constitution Project submits this statement in support of reform of the Electronic Communications Privacy Act of 1986 (ECPA). We believe that Congress should simplify and clarify the ECPA standards and ensure that the Act's privacy protections extend to current and emerging wireless and internet technologies. Reforms are needed to provide for 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 Constitution Project urges Congress to consider the constant evolution and improvements in technology in developing reforms to ECPA to ensure that traditional constitutional principles and protections continue to apply.

About the Constitution Project

The Constitution Project is an independent think tank that promotes and defends constitutional safeguards by bringing together legal and policy experts from across the political spectrum to promote consensus solutions to pressing constitutional issues. The Constitution Project's bipartisan Liberty and Security Committee, launched in the aftermath of September 11th, brings together members of the law enforcement community, legal academics, former government officials, and other experts who develop and advance proposals to protect civil liberties as well as our nation's security.

A critical area of concern for the Constitution Project's Liberty and Security Committee has been to ensure that constitutional and legal safeguards keep pace with changes in technology. The Liberty and Security Committee has issued reports, statements, and recommendations for reform to ensure that constitutional safeguards and privacy protections continue to apply to newly developing technology-based tools for law enforcement and intelligence gathering. For example, in September 2009, the Committee issued its "Statement on Reforming the Patriot Act"[1] which stressed the need for Congress to include more robust protections for constitutional rights and civil liberties in connection with these surveillance authorities.

The Committee explored issues of technology outpacing the law in depth in its report "Guidelines for Public Video Surveillance: A Guide to Protecting Communities and Preserving Civil Liberties."[2] In that report, the Committee recommends policies to address "technological advances and social changes [that] have ushered in new and more pervasive forms of public video surveillance with the potential to upset the existing balance between law enforcement needs and constitutional rights and values." The report discusses how ". . . it is understandable that

---

[1] The Liberty and Security Committee's Statement on Reforming the Patriot Act is available at http://www.constitutionproject.org/manage/file/340.pdf.

The Liberty and Security Committee's "Guidelines for Public Video Surveillance: A Guide to Protecting Communities and Preserving Civil Liberties" is available at http://www.constitutionproject.org/manage/file/54.pdf.

authorities would want to use any available means to prevent or deter other serious threats to public safety. But the value of modern video surveillance must be balanced with the need to protect our core constitutional rights and values, including privacy and anonymity, free speech and association, government accountability, and equal protection. The new technologies may help protect the public, but they also enable authorities to more deeply intrude upon these rights. Lawmakers can no longer rely on constitutional law and technological limits—they need to proactively seek ways to harmonize constitutional rights and values with the new surveillance capabilities."

Building on these efforts to extend civil liberties protections in the digital age, last spring the Constitution Project joined the Digital Due Process Coalition (DDP). The Digital Due Process Coalition is comprised of over 35 different technology companies, privacy advocates, and think tanks as well as over 30 different individual members. The full list of members is available at www.digitalddueprocess.org. The coalition members have come together in support of four guiding principles for needed reforms to ECPA. The Constitution Project strongly supports the Digital Due Process Coalition's guiding principles for reform outlined below.

Guiding Principles for Reforms to ECPA Advocated by the Constitution Project and the Digital Due Process Coalition

ECPA should be amended to provide that:

1. **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 applies the safeguards that the law has traditionally provided for the privacy of our phone calls and the physical files we store in our homes to private communications, documents and other private user content stored in or transmitted through the Internet "cloud"-- private emails, instant messages, text messages, word processing documents and spreadsheets, photos, Internet search queries and private posts made over social networks.

   - This proposal is consistent with recent appeals court decisions holding that emails and SMS text messages stored by communications providers are protected by the Fourth Amendment, and is also consistent with the latest legal scholarship on the issue.

2. **The government must obtain a search warrant based on probable cause before it can track, prospectively or retrospectively, the location of a cell phone or other mobile communications device.**

   - This principle addresses the treatment of the growing quantity and quality of data based on the location of cell phones, laptops and other mobile devices, which is currently the subject of conflicting court decisions; it proposes the conclusion reached by a majority of the courts that a search warrant is required for real-time cell phone tracking, and would apply the same standard to access to stored location data.

3. **Before obtaining transactional data in real time about when and with whom an individual communicates using email, instant messaging, text messaging, the telephone or any other communications technology, the government must demonstrate to a court that such data is relevant to an authorized criminal investigation.**

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

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

4. **Before obtaining transactional data about multiple unidentified users of communications or other online services when trying to track down a suspect, the government should first demonstrate to a court that such information is needed for its criminal investigation.**

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

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

The above four principle reforms would provide critical safeguards that are needed to ensure a proper balance of the interests of private parties, constitutional liberties, and national security. The Constitution Project urges Congress to enact reforms incorporating the above principles and establish these much needed safeguards for constitutional and privacy rights. Such reform would help to restore our system of checks and balances, and simultaneously protect national security and individual rights.

Sharon Bradford Franklin
Senior Counsel
The Constitution Project
1200 18th Street, NW
Suite 1000
Washington, DC 20036
202-580-6920

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

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

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

before the Senate Committee on the Judiciary

THE ELECTRONIC COMMUNICATIONS PRIVACY ACT: PROMOTING SECURITY AND PROTECTING PRIVACY IN THE DIGITAL AGE

September 22, 2010

Chairman Leahy, Ranking Member Sessions, Members of the Committee, thank you for the opportunity to testify today.

Introduction and Overview

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

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

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

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

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

- "Cloud computing," which is the use of Internet-based resources for the storage and processing of all kinds of information. More and more private and proprietary information is moving off the desktop or laptop computer and out of our homes and offices onto the computers of service providers, which store the information, protect it, and make it available pursuant to the instructions of the owner of the information.
- The revolution in mobile communications and the associated development of location-based services. Nearly 300 million Americans rely in their business and personal lives on cell phones and other mobile devices, which generate information locating the individual every few seconds.

Under the Electronic Communications Privacy Act of 1986, neither private information stored in the cloud nor location tracking information is accorded the traditional protection of the judicial warrant. According to ECPA, private documents stored in the cloud, including all our email more than 180 days old as well as documents regardless of age, are available to government investigators without a warrant, even though it would require a warrant to immediately seize the very same material directly from the party who created it. Likewise, ECPA does not specify that a warrant is required for the government to track our location through our cell phones. The courts, as they often have been in the past, are being slow in responding to these technological changes.

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

A Brief History of Electronic Surveillance Law

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

In 1878, the Supreme Court stated in *Ex parte Jackson*, 96 U.S. 727, that the Fourth Amendment applied to sealed letters while in the possession of the Post Office. Even though the letter was voluntarily placed in the hands of a third party, the Court concluded, it was still protected by the Constitution and could not be read without a warrant.[2]

In 1928, however, in *Olmstead v. United States*, 277 U.S. 438, the Supreme Court held that a telephone conversation was not protected by the Fourth Amendment if it was intercepted from the facilities of the service provider. The *Olmstead* Court concluded, in essence, that users of the telephone voluntarily surrendered the privacy of their communications by disclosing them to the telephone company: "The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment." 277 U.S. at 466.

[2] "The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be." 96 U.S. at 733.

Justice Brandeis, in his famous dissent, said that the majority opinion was inconsistent with the Court's earlier ruling on the privacy of letters. Quoting the lower court, Brandeis said, "There is, in essence, no difference between the sealed letter and the private telephone message. ... 'True, the one is visible, the other invisible; the one is tangible, the other intangible; the one is sealed, and the other unsealed; but these are distinctions without a difference.'" *Id.* at 475. Justice Brandeis criticized the Court's focus on physical trespass and warned that technology would continue to change in ways that would erode privacy if the law remained static: "The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." Id. at 474.

In 1934, when Congress adopted the Communications Act, it responded to the Olmstead decision by making it illegal for any person to "intercept ... and divulge or publish" the contents of any wire communication. Over succeeding decades, the courts and the Justice Department tussled over the interpretation of Section 605. The Justice Department argued, for example, that its agents were not "persons" under the Act. The Supreme Court rejected that theory. Nardone v. United States, 302 U.S. 379 (1937). The Justice Department nevertheless proceeded to wiretap on the theory that it was legal to do so under Section 605 so long as it did not divulge the intercepts outside law enforcement.

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

Next it was Congress' turn again. To implement the Constitutional ruling of *Katz* and the related case on bugging, *Berger v. New York*, 388 U.S. 41 (1967), Congress in 1968 adopted the federal Wiretap Act, 18 U.S.C. 2510 *et seq.*, establishing detailed procedural rules for obtaining judicial warrants to carry out wiretaps. The statute provided many details the courts would not have been well-suited to develop.[3] Congress, however, forgetting Justice Brandeis' prediction about the steady progress of technology, only covered voice communications carried over a wire and face-to-face oral conversations.

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

[3] See Orin S. Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution," 102 Michigan Law Review 801 (2004).

shadow of doubt over the status of Internet communications, which were stored on network computers as they hopped from node to node and before they were accessed by their intended recipients.

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

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

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

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

Changes in Technology Have Outpaced ECPA

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

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

- **Email**: Most Americans have embraced email in their professional and personal lives and use it daily for confidential communications of a personal or business nature. Because of the importance of email and unlimited storage capabilities available today, most people save their email indefinitely, just as they previously saved letters and other correspondence. The difference, of course, is that it is easier to save, search and retrieve digital communications. Many of us now have many years worth of stored email. Moreover, for many people, much of that email is stored on the computers of service providers.[4] **However, ECPA provides only weak protection for stored email that is more than 180 days old, allowing governmental access without a warrant. Moreover, the Justice Department argues that email loses the protection of the warrant the instant the sender sends it and, on the other end, the minute the recipient accesses it or opens it.**

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

  Most significantly, the precision with which cell phones can be located using cell site data has been steadily improving, as carriers build out their networks with cells covering smaller and smaller areas, so that today cell site location information is sometimes as precise as GPS. As Prof. Matt Blaze of the University of Pennsylvania explained in testimony before a House subcommittee earlier this year, "The effect of this trend toward smaller sectors is that knowing the identity of the base station (or sector ID) that handled a call is tantamount to knowing a phone's location to within a relatively small geographic

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

area. In relatively unpopulated areas with open terrain, this may be an area miles in diameter. But in urban areas and other environments that use microcells, this area can be quite small indeed, sometimes effectively identifying individual floors and rooms within buildings."[5] Consequently, Blaze concluded, the distinction between cell site location data and GPS data "is increasingly obsolete, and as cellular networking technology evolves, it is likely to become effectively meaningless. As microcell technology and enhanced location techniques become more widely deployed in cellular networks, the information revealed though the cell sector identifier pinpoints, under many circumstances, a user's location to a degree once possible only with dedicated GPS tracking devices."

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

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

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

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

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

- **Unclear standards:** ECPA does not clearly state the standard for governmental access to location information. In the past 5 years, no fewer than 30 federal opinions have been

[5] Testimony of Prof. Matt Blaze, House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights, and Civil Liberties, Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services, June 24, 2010, http://judiciary.house.gov/hearings/pdf/Blaze100624.pdf

published on government access to cell phone location information, reaching a variety of conclusions.

- **Judicial criticism:** The courts have repeatedly criticized ECPA for being confusing and difficult to apply. The Ninth Circuit in 2002 said that Internet surveillance was "a confusing and uncertain area of the law."[6] The Third Circuit last month complained that, in trying to determine what standard was appropriate for cellphone tracking, "we are stymied by the failure of Congress to make its intention clear."[7]

The Courts Are Unlikely to Resolve Soon The Questions Posed By New Technology

It appears unlikely that the courts will anytime soon resolve these issues on Constitutional grounds. The courts have been progressing sporadically and inconclusively in assessing the application of the Fourth Amendment to stored email. When a panel of the Sixth Circuit ruled that stored email was protected by the Constitution, an en banc panel vacated the opinion on ripeness grounds. Warshak v. United States, 490 F.3d 455 (6th Cir. 2007), vacated en banc, 532 F.3d 521 (2008). Conversely, in March of this year a panel of the Eleventh Circuit held that stored email was *not* protected by the Constitution, Rehberg v. Paulk, 598 F.3d 1268, and in July the same judges vacated that opinion and substituted for it one holding that, if the Fourth Amendment right existed, it wasn't "clearly established."[8] The Ninth Circuit held in 2008 that the Constitution protected stored text messages, Quon v. Arch Wireless, 529 F.3d 892 (2008). The Supreme Court this summer reversed the Ninth Circuit, but it did so without ruling on the question of whether the Fourth Amendment protects stored text messages. City of Ontario v. Quon. Instead the Court assumed arguendo that there was a reasonable expectation of privacy. The Court emphasized that it was reluctant to "elaborate too fully on the Fourth Amendment implications of emerging technology."

Similarly, the courts have been unable to resolve questions about the Constitutional status of location tracking information. Last month, within a week's time, the D.C. Circuit held that prolonged GPS tracking was a search under the Fourth Amendment, United States v. Maynard, and the Ninth Circuit held that it was not, United States v. Pineda-Moreno. And three weeks after that, the Third Circuit held that ECPA gives magistrates the option of requiring a warrant to obtain cell site location information. Meanwhile, there have been about three dozen opinions by federal magistrates and district court judges on a variety of cell phone tracking questions, with a variety of outcomes although, by our count, a majority of those dealing with real-time tracking have held that a warrant is necessary.

This murky legal landscape does not serve the government, customers or service providers well. Customers are, at best, confused about whether their data is subject to adequate protections when the government seeks access. Companies are uncertain of their responsibilities and unable to assure their customers that subscriber data will be uniformly protected. The current state of the law does not well serve law enforcement interests either, as resources are wasted on litigation over applicable standards and prosecutions are in jeopardy

---

[6] Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002).

[7] 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. Sept. 7, 2010).

[8] http://www.ca11.uscourts.gov/opinions/ops/200911897reh.pdf.

should the courts ultimately rule on the Constitutional questions. The solution is a clear set of rules for law enforcement access that will safeguard end-user privacy, provide clarity for service providers, and enable law enforcement officials to conduct effective and efficient investigations.

The Digital Due Process Coalition

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

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

Updating The Electronic Communications Privacy Act of 1986

Overarching goal and guiding principle: *To simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public.*

These principles would not change, and are subject to, the current definitions, exceptions, immunities and permissions in ECPA:

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

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

3. *A governmental entity may access, or may require a covered entity to provide, prospectively or in real time, dialed number information, email to and*

from information or other data currently covered by the authority for pen registers and trap and trace devices only after judicial review and a court finding that the governmental entity has made a showing at least as strong as the showing under 2703(d).

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

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

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

- **Technology and Platform Neutrality**: A particular kind of information (for example, the content of private communications) should receive the same level of protection regardless of the technology, platform or business model used to create, communicate or store it.[9]
- **Assurance of Law Enforcement Access**: The reform principles would preserve all of the building blocks of criminal investigations – subpoenas, court orders, pen register orders, trap and trace orders, and warrants – as well as the sliding scale that allows the government to escalate its investigative efforts.
- **Equality Between Transit and Storage**: Generally, a particular category of information should be afforded the same level of protection whether it is in transit or in storage.
- **Consistency**: The content of communications should be protected by a court order based on probable cause, regardless of how old the communication is and whether it has been "opened" or not.
- **Simplicity and Clarity**: All stakeholders – service providers, users and government investigators – deserve clear and simple rules.
- **Recognition of All Existing Exceptions**: Over the years, a variety of exceptions have been written into the ECPA, such as provisions allowing disclosures to the government without court orders in emergency cases. These principles should leave all those exceptions in place.

Rather than attempt a full rewrite of ECPA, which might have unintended consequences, it is best to focus just on the most important issues – those that are arising daily under the current

[9] Technology neutrality is a principle to be applied with caution. For example, design mandates developed for the traditional telephone network would not be suited to Internet technologies.

law: access to email and other private communications stored in the cloud, access to location information, and the use of subpoenas to obtain transactional data.

What Would ECPA Reform Mean in Practice

The Digital Due Process recommendations preserve the "building blocks" of criminal investigations. Under current law, government investigators often work their way up the ladder to probable cause, starting with subpoenas for subscriber identifying information and stored transactional data, then moving to court orders under 2703(d) for more detailed transactional data and court orders, based on less than probable cause, for real-time interception of signaling and routing information. Based on analysis of this and other data, they may then have probable cause to obtain a search warrant. The DDP recommendations preserve all these building blocks of the investigative process.

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

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

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

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

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

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

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

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

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

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

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

What the Digital Due Process Principles Would Not Do

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

- They would not affect FISA or the National Security Letter authority of ECPA (18 U.S.C. 2709).

- They would not affect emergency disclosures. The Wiretap Act, the Stored Communications Act, and the pen register/trap and trace provisions all contain emergency exceptions that permit interceptions and service provider disclosure without a warrant (and even without a subpoena). The principles offered by the DDP would not affect any of these emergency disclosures. The warrant requirement for access to location information recommended by DDP would have to be subject to similar emergency exceptions. Calls to 911 would also be exempted from the warrant requirement, under both the consent principle and the emergency exception.

- The principles would not affect cybersecurity. Service providers currently have broad authority to monitor their own networks for cybersecurity purposes and to disclose to the government information about suspected attacks or intrusions. The DDP recommendations would not alter these authorities.

- They would have zero impact on child pornography, child abuse and child safety investigations. The principles were carefully crafted to preserve fully the tools critical to these investigations. They do not alter in any way the child pornography reporting provisions in federal and state law. They do not alter the exceptions or other permissions granted in the statute for providing information to the government in child abduction cases. They do not alter any authority that service providers have to monitor their systems for child abuse images and to disclose such images to NCMEC or law enforcement.

- The recommendations would not cover anything publicly disclosed on the Internet. Moreover, they would not stop a police officer from "friending" someone on Facebook and obtaining access to otherwise private communications. The rules permitting undercover operations and other deceptive techniques would remain unaffected.

- The recommendations, like ECPA itself, focus on compulsory access from service providers. The recommendations would not change the rules for voluntary disclosure by the customers of those service providers. Nor do the recommendations change the rules for use of subpoenas served on the sender or recipient of an email or the creator of a document. The rule applicable to postal mail would also apply to email: the recipient of an email, like the recipient of a letter, could voluntarily disclose that email to the government and could be compelled to disclose it with a subpoena. The sender of an email could be compelled to disclose it with a mere subpoena to the same extent that the sender of a letter can be compelled to disclose a retained copy. If the creator of a document could be compelled with a subpoena to disclose it, under the DDP principles the creator could be compelled to disclose whether the document was stored locally or in the cloud.

Disclosure to a Third Party Does Not Destroy a Privacy Interest

The ECPA reform proposals here are consistent with the long line of cases holding that individuals have privacy rights in materials that they entrust to third parties and in spaces rented from third parties. As noted above, the Supreme Court has recognized a Constitutional expectation of privacy in the contents of sealed packages and letters, even when those letters and packages are voluntarily given to the government-run Post Office. *Ex Parte Jackson*, 96 U.S. 727, 733 (1878). Bank customers have a privacy interest in the contents of their safe

deposit boxes, requiring a warrant for government access. *United States v. Thomas*, No. 88-6341, 1989 WL 72926, at *2 (6th Cir. July 5, 1989). Moreover, this privacy right survives even if the service provider has rights to enter the protected space or inspect the material. Tenants in rented residences and hotel rooms maintain Fourth Amendment privacy rights in their units. *Stoner v. California*, 376 U.S. 483, 489 (1964). The fact that landlords and hotel managers may be entitled to enter the premises for maintenance and other purposes does nothing to diminish the tenants' expectations against the government. *Id.*

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

Other ECPA Issues May Deserve Attention

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

- Civil litigant access. Several court decisions have made it clear that ECPA does not allow civil litigants to compel the disclosure of communications by electronic communications service providers or providers of remote computing service to the public; under these rulings, such requests should be served on the sender or recipient of the communications who can be compelled under normal discovery rules to either retrieve them and disclose them to the litigant or to give consent to the service provider to disclose them. While these cases are a correct reading of ECPA, and while they offer a clear path to discovery in most cases, service providers continue to spend considerable resources defending against civil litigant requests, briefing the issue one court at a time. Some have argued that ECPA could be clarified, while perhaps including a safety valve process for cases in which the user whose communications are sought cannot be found.

- Reporting and transparency. The Wiretap Act requires annual publication of statistics on wiretapping, but there is no comparable requirement for pen register and trap and trace devices or for compulsory disclosure of stored content.

- The Wiretap Act only covers interception of communications. It does not cover the use of video cameras in private places. The recent case in Marion County, PA, in which a school turned on the cameras in computers issued to students and took pictures of the students engaging in a variety of activities inside their homes, highlighted this gap in the law. See Testimony of Kevin Bankston before the Senate Judiciary Committee, Subcommittee on Crime and Drugs (March 29, 2010) http://www.eff.org/files/bankston_video_surveillance_testimony.pdf.

Conclusion

In just the past 5 to 10 years, entrepreneurs have developed and the American public has embraced truly revolutionary changes in communications and information technology. These

changes have yielded remarkable benefits in terms of economic activity, education, democratic participation and support for friendships and family relationships. Further amazing developments are surely on the way. Our economic recovery depends in large part on innovation in information and communications technologies.

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

Appendix A

One Email - Multiple Different Standards

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

Standards for access to the content of an email:

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

Appendix B
Members of Digital Due Process
(as of September 20, 2010)

Companies

Amazon.com
AOL
AT&T
Data Foundry
eBay
Facebook
Google
Hewlett-Packard
IAC
Integra Telecom
Intel
Linden Lab
Loopt
Microsoft
Qwest
Salesforce.com
TRUSTe

Trade Associations, Thinks Tanks and other Organizations

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

UNITED STATES DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

In the Matter of

Information Privacy and Innovation in the Internet Economy **Docket No. 100402174-0175-01**

COMMENTS OF DIGITAL DUE PROCESS

June 14, 2010

In response to the Notice of Inquiry in the above captioned matter, Digital Due Process is pleased to submit the following comments.

Digital Due Process (DDP) is a broad coalition of technology and communications companies, trade associations, advocacy groups, and think tanks, as well as academics and individual lawyers. A full, current list of DDP members appears at the end of this document. On March 30 of this year, DDP issued principles for updating the key federal law that defines the rules for government access to email and private files stored in the Internet "cloud." The coalition effort was prompted by the need to preserve traditional privacy rights in the face of technological change while also ensuring that law enforcement agents can carry out investigations and that industry has the clarity needed to innovate.

To set a consistent standard in line with the traditional rules for law enforcement access in the offline world, the group's recommendations focus on the Electronic Communications Privacy Act (ECPA). Passed in 1986 and not significantly updated since, it establishes standards for government access to email and other electronic communications in criminal investigations.

Technology has changed dramatically in the last 20 years, but the law has not. The traditional standard for the government to search one's home or office and read one's mail or seize one's personal papers is a judicial warrant. The law needs to be clear that the same standard applies to email and documents stored with a service provider, while at the same time be flexible enough to meet law enforcement needs.

The group is reaching out to government officials and anticipates extended dialogue with law enforcement agencies to develop consensus on updates to the law. We urge the Department to join in this process.

ECPA Reform: Why Now?

The Electronic Communications Privacy Act (ECPA) was a forward-looking statute when enacted in 1986. It specified standards for law enforcement access to electronic communications and associated data, affording important privacy protections to

subscribers of emerging wireless and Internet technologies. Technology has advanced dramatically since 1986, and ECPA has been outpaced. The statute has not undergone a significant revision since it was enacted in 1986 – light years ago in Internet time.

As a result, ECPA is a patchwork of confusing standards that have been interpreted inconsistently by the courts, creating uncertainty for both service providers and law enforcement agencies. ECPA can no longer be applied in a clear and consistent way, and, consequently, the vast amount of personal information generated by today's digital communication services may no longer be adequately protected. Concern about the privacy afforded personal and business information can hold back adoption of emerging technologies, discouraging innovation. ECPA's complexity also imposes substantial costs on service providers seeking to review and comply with data requests from law enforcement. At the same time, ECPA must be flexible enough to allow law enforcement agencies and service providers to work together effectively to combat increasingly sophisticated cyber-criminals or sexual predators.

The time for an update to ECPA is now. For more than a year, privacy advocates, legal scholars, and major Internet and communications service providers have been engaged in a dialogue to explore how ECPA applies to new services and technologies. We have developed consensus around the notion of a core set of principles intended to simplify, clarify, and unify the ECPA standards; provide clearer privacy protections for subscribers taking into account changes in technology and usage patterns; and preserve the legal tools necessary for government agencies to enforce the laws and protect the public.

The Economic Context for ECPA Reform

Since ECPA was adopted in 1986, the Internet has evolved from a research network with a few thousand academic hosts into a global platform for communications, commerce, and civic activity. According to the most recent Pew survey, an estimated 74% of Americans use the Internet.[1/] Information technology has driven the U.S. economy in the past two decades,[2/] and could, given the proper policy framework, support re-invigoration of the economy for years to come.[3/] The Internet and information technology could be especially important in job creation.[4]

1/ Pew Research Center, "Internet, broadband and cell phone statistics," (January 5, 2010) http://www.pewinternet.org/Reports/2010/Internet-broadband-and-cell-phone-statistics.aspx. However, the fact that Internet usage has remained essentially static since 2006, *id.*, suggests that continued attention is needed to the policy framework supporting Internet expansion.

2/ *See* Robert D. Atkinson & Andrew S. McKay, *Information Technology & Innovation Foundation, Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution* at 11-14 (March 2007) ("[T]here is a now a strong consensus among economists that the IT revolution was and continues to be responsible for the lion's share of the post '95 rebound in productivity growth.").

3/ *See id.* at 53 ("Many sectors, such as health care, education, and government, have only begun to tap the benefits of IT-driven transformation. Adoption rates of e-commerce for most consumers, while rapid, are still relatively low. And new technologies (*e.g.*, RFID, wireless broadband, voice recognition) keep emerging that will enable new applications. In short, while the emerging digital economy has produced enormous benefits, the best is yet to come. The job

Cloud computing[5/] is a key element of technological innovation today. Businesses and individuals are now increasingly storing data "in the cloud," with huge benefits in terms of productivity, cost, security, flexibility and the ability to work with collaborators around the world.[6/] More than two-thirds of Internet users use some form of cloud computing service.[7] Cloud computing, "by altering the basic economics of access to computing and storage ... has the potential to reshape how U.S. and global businesses are organized and operate."[8/] Most importantly, American tech companies are global leaders in the cloud computing industry today.

---

of policymakers in developed and developing nations alike, is to ensure that the policies and programs they put in place spur digital transformation so that all their citizens can fully benefit from robust rates of growth.").

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

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

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

[7] *Use of Cloud Computing Applications and Services*, Pew Internet & American Life Project, Sep. 12, 2008, Pg. 4, available at http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.

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

The issue of privacy is important to the users of cloud computing. A 2008 study found that 64 percent of American Internet users are concerned about cloud computing companies turning over their files to law enforcement.[9] A survey completed just last week found that a large majority of Americans (88%) believe consumers should enjoy legal privacy protections online similar to those they have offline, while only 4% disagree.[10] Moreover, cloud computing experts warn that potential clients are seeking data storage centers outside the U.S. due to concerns that our laws give the government access to huge quantities of information with little judicial oversight.[11] If this trend continues, American workers may miss out on the jobs that would accompany the growth of this industry.

The use of location information is another trend creating major market opportunities for U.S. companies. There are already a number of innovative, socially beneficial "location aware" applications that employ technologies such as GPS, cell phone infrastructure, or wireless access points to locate electronic devices and provide "resources such as a 'you are here' marker on a city map, reviews for restaurants in the area, a nap alarm triggered by your specific stop on a commuter train, or notices about nearby bottlenecks in traffic."[12] More applications such as these are emerging every day. A 2010 study forecast that revenues from mobile location-based services could grow to more than $12.7 billion by 2014.[13] However, uncertainty about the privacy afforded location information can hold back consumer use of this technology.[14]

---

people and work together. *See* http://www.marketspaceadvisory.com/cloud/Envisioning-the-Cloud.pdf

[9] Id., at p. 7.

[10] Zogby International, Results from June 4-7 Nationwide Poll (June 7, 2010) http://www.precursorblog.com/files/pdf/topline-report-key-findings.pdf. According to the survey, the large majority (79%) believes law enforcement should have to get a warrant, like the one they have to get to wiretap phone conversations, to track where a user goes on the Internet, while 12% do not.

[11] Jeffery Rayport and Andrew Heyward, *Envisioning the Cloud: The Next Computing Paradigm*, Marketspace, Mar. 20, 2009, p. 38, available at http://www.marketspaceadvisory.com/cloud/Envisioning-the-Cloud.pdf.

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

[13] Robin Wauters, *Mobile Location-Based Services Could Rake in $12.7 Billion by 2014: Report*, TechCrunch, Feb. 23, 2010, http://techcrunch.com/2010/02/23/location-based-services-revenue.

[14] Tsai, et al., *Location-Sharing Technologies: Privacy Risks and Controls*, Carnegie Mellon University (Feb. 2010), p. 18, http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.

Changes in Technology Have Outpaced the Law

Justice Brandeis famously called privacy "the most comprehensive of rights, and the right most valued by a free people." Of course, privacy must be balanced against other societal interests. Electronic communications and associated data can provide key evidence in the investigation of many crimes, and the assistance of service providers is often necessary to access such evidence. With respect to communications privacy and law enforcement investigations, the courts and Congress have sought to develop rules for government surveillance that balance three interests: the individual's constitutional right to privacy, the government's need for tools to conduct investigations, and the interest of service providers in clarity and customer trust.

A primary reason that Congress adopted ECPA in 1986 was to provide sound footing for investment and innovation. In 1986, the fledgling wireless and Internet industries wanted to be able to assure potential customers that their communications were private. Congress recognized that consumers would not trust new technologies if the privacy of those using them was not protected. In the quarter century since the enactment of ECPA, there have been fundamental changes in communications technology and the way people use it, including –

- **Email**: Most Americans have embraced email in their professional and personal lives and use it daily for confidential communications of a personal or business nature. Because of the importance of email and unlimited storage capabilities available today, most people save their email indefinitely, just as they previously saved letters and other correspondence. The difference, of course, is that it is easier to save, search and retrieve digital communications. Many of us now have many years worth of stored email. Moreover, for many people, much of that email is stored on the computers of service providers.
- **Mobile location:** Cell phones and mobile Internet devices constantly generate location data that supports both the underlying service and a growing range of location-based services of great convenience and value. This location data can be intercepted in real-time, and is often stored in easily accessible logs files. Location data can reveal a person's movements, from which inferences can be drawn about activities and associations. Location data is augmented by very precise GPS data being installed in a growing number of devices.
- **Cloud computing**: Increasingly, businesses and individuals are storing data "in the cloud," with potentially huge benefits in terms of cost, security, flexibility and the ability to share and collaborate.
- **Social networking:** One of the most striking developments of the past few years has been the remarkable growth of social networking. Hundreds of millions of people now use these social media services to share information with friends and as an alternative platform for private communications.

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

- **Conflicting standards and illogical distinctions:** ECPA sets rules for

governmental access to email and stored documents that are not consistent. A single email is subject to multiple different legal standards in its lifecycle, from the moment it is being typed to the moment it is opened by the recipient to the time it is stored with the email service provider. To take another example, a document stored on a desktop computer is protected by the warrant requirement of the Fourth Amendment, but the ECPA says that the same document stored with a service provider may not be subject to the warrant requirement.

- **Unclear standards:** ECPA does not clearly state the standard for governmental access to location information.
- **Judicial criticism:** The courts have repeatedly criticized ECPA for being confusing and difficult to apply. The Ninth Circuit in 2002 said that Internet surveillance was "a confusing and uncertain area of the law." In the past 5 years, no fewer than 30 federal opinions have been published on government access to cell phone location information, reaching a variety of conclusions.
- **Constitutional uncertainty:** The courts are equally conflicted about the application of the Fourth Amendment to new services and information. A district court in Oregon recently opined that email is not covered by the constitutional protections, while the Ninth Circuit has held precisely the opposite. Last year, a panel of the Sixth Circuit first ruled that email was protected by the Constitution and then a larger panel of the court vacated the opinion.

This murky legal landscape does not serve the government, customers or service providers well. Customers are, at best, confused about the security of their data in response to an access request from law enforcement. Companies are uncertain of their responsibilities and unable to assure their customers that subscriber data will be uniformly protected. The current state of the law does not well serve law enforcement interests either as resources are wasted on litigation over applicable standards, and prosecutions are in jeopardy should the courts ultimately rule on the Constitutional questions.

The solution is a clear set of rules for law enforcement access that will safeguard end-user privacy, provide clarity for service providers, and enable law enforcement officials to conduct effective and efficient investigations.

Guiding Principles for ECPA Reform

The overarching goal of our review of the ECPA was to balance the law enforcement interests of the government, the privacy interests of users, and the interests of communications service providers in certainty, efficiency and public confidence.

We were guided by the following concepts:

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

create, communicate or store it.

- **Assurance of Law Enforcement Access**: The reform principles would preserve all of the building blocks of criminal investigations – subpoenas, court orders, pen register orders, trap and trace orders, and warrants – as well as the sliding scale that allows the government to escalate its investigative efforts.
- **Equality Between Transit and Storage**: Generally, a particular category of information should be afforded the same level of protection whether it is in transit or in storage.
- **Consistency**: The content of communications should be protected by a court order based on probable cause, regardless of how old the communication is and whether it has been "opened" or not.
- **Simplicity and Clarity**: All stakeholders – service providers, users and government investigators – deserve clear and simple rules.
- **Recognition of All Existing Exceptions**: Over the years, a variety of exceptions have been written into the ECPA, such as provisions allowing disclosures to the government without court orders in emergency cases. These principles should leave all those exceptions in place.

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

Our principles do not seek to answer all questions or concerns about ECPA. Though members of the coalition may differ on the specifics, and some individual members would support additional changes, we all agree that these principles provide a framework for opening a public dialogue on the issue.

Specific Background on ECPA Reform Principles

1. The government should obtain a search warrant based on probable cause before it can compel a service provider to disclose a user's private communications or documents stored online.

- This principle applies the safeguards that the law has traditionally provided for the privacy of our phone calls or the physical files we store in our homes to private communications, documents and other private user content stored in or transmitted through the Internet "cloud"-- private emails, instant messages, text messages, word processing documents and spreadsheets, photos, Internet search queries and private posts made over social networks.

- This change was first proposed in bi-partisan legislation introduced in 1998 by Senators John Ashcroft and Patrick Leahy. It is consistent with recent appeals court decisions holding that emails and SMS text messages stored by

communications providers are protected by the Fourth Amendment, and is also consistent with the latest legal scholarship on the issue.

2. The government should obtain a search warrant based on probable cause before it can track, prospectively or retrospectively, the location of a cell phone or other mobile communications device.

- This principle addresses the treatment of the growing quantity and quality of data based on the location of cell phones, laptops and other mobile devices, which is currently the subject of conflicting court decisions; it proposes the conclusion reached by a majority of the courts that a search warrant is required for real-time cell phone tracking, and would apply the same standard to access to stored location data.

- A warrant for mobile location information was first proposed in 1998 as part of the bipartisan Ashcroft-Leahy bill. It was approved 20 to 1 by the House Judiciary Committee in 2000.

3. Before obtaining transactional data in real-time about when and with whom an individual communicates using email, instant messaging, text messaging, the telephone or any other communications technology, the government should demonstrate to a court that such data is relevant to an authorized criminal investigation.

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

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

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

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

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

Members of Digital Due Process:

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

American Booksellers Foundation for Free Expression
American Civil Liberties Union
American Library Association
Association of Research Libraries
Americans for Tax Reform
Bill of Rights Defense Committee
Center for Democracy & Technology
Center for Financial Privacy and Human Rights
Citizens Against Government Waste
Competitive Enterprise Institute
Computer & Communications Industry Association
The Constitution Project
Consumer Action
Distributed Computing Industry Association
Electronic Frontier Foundation
FreedomWorks
Information Technology and Innovation Foundation
NetCoalition
The Progress & Freedom Foundation

Individuals:

Patricia Bellia, Notre Dame Law School
David Berger, Wilson, Sonsini Goodrich & Rosati
Michael Carroll, American University, Washington School of Law
Fred Cate, Indiana University Law School
Danielle Keats Citron, University of Maryland School of Law
Ralph D. Clifford, University of Massachusetts School of Law
Susan Crawford, University of Michigan Law School
Susan Freiwald, University of San Francisco Law School

James Grimmelmann, New York Law School
Eric Goldman, Santa Clara University School of Law
Robert A. Heverly, Michigan State University College of Law
Dan Hunter, New York Law School and The Wharton School, University of Pennsylvania
Charles H. Kennedy, Wilkinson Barker Knauer, LLP
Liza Barry-Kessler, Privacy Counsel LLC
Mark A. Lemley, Stanford Law School
Jennifer Lynch, UC Berkeley Law School
Rebecca MacKinnon, Center for Information Technology Policy, Princeton University
Anthony Martin, Husch Blackwell Sanders LLP
Deirdre Mulligan, UC Berkeley iSchool
Paul Ohm, Professor of Law, University of Colorado
Scott Parsons, Portland State University
Frank A. Pasquale, Seton Hall Law School
David G. Post, Beasley School of Law, Temple University
Ira Rubinstein, New York University School of Law
Pam Samuelson, UC Berkeley Law School and iSchool
Katherine J. Strandburg, New York University School of Law
Jennifer Urban, UC Berkeley Law School
Michael Zimmer, School of Information Studies, University of Wisconsin-Milwaukee
Marc Zwillinger, Zwillinger Genetski LLP

For further information, contact:

James X. Dempsey
jdempsey@cdt.org
202-365-8026

Statement of U.S. Senator Russell D. Feingold
Hearing On "The Electronic Communications Privacy Act:
Promoting Security and Protecting Privacy in the Digital Age"
Senate Judiciary Committee
September 22, 2010

Mr. Chairman, I am pleased that the Judiciary Committee is taking a look at the important issue of reforming the Electronic Communications Privacy Act (ECPA).

When you consider that ECPA was enacted in 1986, it is incredible how forward-looking it was. In 1986, networked computing was in its infancy, and few could have imagined the enormous influence that it would ultimately have on our society. Yet Chairman Leahy, Representative Kastenmeier of Wisconsin and many others in Congress had the foresight to recognize the importance of establishing clear, sensible rules for when the government can access electronic communications in a criminal investigation while also protecting Americans' privacy rights.

Nearly 25 years later, those principles are still vitally important, but not surprisingly ECPA itself has not kept up with the technological change we have experienced. Rules that covered the waterfront a quarter of a century ago now leave gaping holes and a great deal of uncertainty. Other rules that may have made sense in 1986 no longer do.

Indeed, many Americans would be very surprised to learn that the contents of their email communications are not necessarily statutorily protected by the warrant requirement. Under ECPA, an email that is more than 180 days old can be obtained by the government in a criminal investigation without getting a search warrant from a judge. Not only that, but the Department of Justice has taken the position that ECPA also allows it to obtain an email without meeting the probable cause standard simply because it has been opened by the recipient. Do any of us believe that our email no longer deserves the same privacy protection as our phone conversations because we have already read the email, or left it in our inbox for more than 6 months? It is time to fix this anachronism in the law so that the contents of Americans' email conversations cannot be accessed by the government unless a judge agrees there is probable cause and issues a search warrant.

ECPA also provides a set of rules allowing the government to obtain – usually based on mere relevance to an investigation – the non-content information about our electronic communications, such as the email addresses we communicate with, the IP addresses of our computers, and the time and date of our communications. But ECPA could not have foreseen how ubiquitous electronic communications would become, and how much information about a person could be gleaned from information that might not technically be considered "contents." There continue to be difficult grey areas where it is hard to draw the line between content and non-content information, yet the legal ramifications under ECPA are very significant. This is an area that I have been looking at for years,

and I hope the committee will consider whether the current certification of relevance standard for the real-time acquisition of this 'transactional' information still makes sense.

Other technological innovations need to be addressed by Congress, as well. The use of mobile phones and other mobile devices can reveal a person's location, often quite precisely, both in the past and in real time. Yet court decisions have not resulted in consistent rules for what the government must show to obtain location information about a suspect, and in fact in some cases different judges in the same federal district have come to different conclusions. Given this lack of clarity, Congress should establish clear rules for location information. Congress also needs to set clear rules to govern access to information that is stored in the "cloud" – on third-party servers – as "cloud computing" becomes more prevalent.

Mr. Chairman, in sum, we need to follow the example that you and others set when you wrote ECPA in the first place. We need to craft clear rules that protect privacy, that give law enforcement the tools it needs, that industry can rely on, and that are as technologically neutral as possible so that they can weather at least a decade or two of innovation before Congress will need to revisit them.

I commend you, Mr. Chairman, for this opportunity to consider carefully the overall framework of surveillance rules in criminal cases. The laws governing the surveillance of Americans have, in the past decade, too often been debated in a politically charged environment, so I appreciate this opportunity for a real discussion.

SEP-20-2010 MON 03:42 PM GMU PRINT SERVICES JC FAX NO. 7039939081 P. 02

Before the

Senate Judiciary Committee

Dirksen Senate Office Building, Room 226

Washington, D.C. 20510

Hearing on The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age

September 22, 2010

Written Testimony
of
Frederick W. Freeman, Student
George Mason University

(ffreema1@gmu.edu)

09/20/2010 2:41PM

Mr. Chairman and Members of the Subcommittee on the Constitution, Civil Rights, and Civil Liberties, my name is Frederick W. Freeman and I am a student at George Mason University where I have been assigned to comment on my position on reforming the Electronic Communications Privacy Act of 1986 (ECPA). Thank you for the opportunity to submit this testimony concerning the need for reform of ECPA to address new innovations and bring the law into alignment with the advances in communications since the statute was first enacted.

These comments reflect my personal opinions as a student and a private citizen, based on my research on the background and evolution of the law and technological advances, the news, and on my personal observations.

The Electronic Communications Privacy Act (ECPA) was enacted by the US Congress in 1986; it lists provisions for what privacy rights people have when they use telephones, computers, cellphones or other means of electric transmission of communication like faxes or texting. In 1986, the provisions of ECPA did not include some of the newer forms of communication developed since then. The Global Positioning System (GPS), for example, a space-based global navigation satellite system that provides reliable, real-time, location and time information anywhere on or near the earth, is a communication system. It can be argued that GPS tracking would be treated in a similar way to cell-phone tracking. However, the law does not specifically address these communication methods. Yet every form of communication is covered under the law.

The current law, because it has not developed at the same pace as technology, has resulted in confusion in enforcement, and does not address the newer forms of communication technology.

In order to bring clarity to the statute, protect the rights of the individual citizens, protect national security, and assist law enforcement, it is essential that the law be updated to address all the advances in technology, and should be reviewed periodically to incorporate future technology.

Thank you for the opportunity to present these comments in favor of ECPA reform. Laws should provide clarity and reflect the current climate under which they exist. I believe that the goals of privacy advocates as well as law enforcement are similar: they believe the law should exist to protect the right of the individual while balancing against threats to the innocent as well as national security.

09/20/2010 2:41PM

Written Testimony of Jamil N. Jaffer[1]
before the
United States Senate
Committee on the Judiciary

on

The Electronic Communications Privacy Act:
Promoting Security and Protecting Privacy in the Digital Age

September 22, 2010

Good afternoon, Chairman Leahy, Ranking Member Sessions, and Members of the Committee. Thank you for the opportunity to testify today regarding the Electronic Communications Privacy Act of 1986, as amended (ECPA). I want to note, at the outset of my testimony, that the views I present today are my own and are not those of my law firm nor any client of the firm.

As the Members of this Committee are well aware, ECPA plays a crucial role in a diverse range of criminal investigations conducted by law enforcement officers from the Department of Justice (DOJ), including officers and agents from the Federal Bureau of Investigation (FBI), the Drug Enforcement Agency (DEA), and the United States Marshals Service (USMS), among others. These officers and agents work alongside other federal and state law enforcement officers and Assistant United States Attorneys (AUSAs) from across the country, as well as with prosecutors from Main Justice. These dedicated career professionals – many of whom I had the opportunity to serve with

[1] Jamil N. Jaffer is an attorney at a Washington, D.C. trial litigation firm. Mr. Jaffer previously served in the White House as an Associate Counsel to the President (2008-2009) and in the United States Department of Justice's National Security Division as Counsel to the Assistant Attorney General (2007-2008), Senior Counsel for National Security Law & Policy (2007), and in the Department of Justice's Office of Legal Policy as Counsel (2005-2006). Mr. Jaffer also served as a law clerk to Judge Edith H. Jones of the United States Court of Appeals for the Fifth Circuit (2003-2004) and Judge Neil M. Gorsuch of the United States Court of Appeals for the Tenth Circuit (2006-2007). Mr. Jaffer is a graduate of the University of Chicago Law School (J.D., *with honors*, 2003), the United States Naval War College (M.A., *with distinction*, 2006), and the University of California, Los Angeles (B.A., *cum laude*, Phi Beta Kappa, 1998).

during my time at DOJ's National Security Division (NSD) – spend countless hours working on crucial investigations to protect the safety and security of the American public.

They are assisted in this effort by tools provided by Congress, including the authorities provided in ECPA, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended (Title III), and the Foreign Intelligence Surveillance Act of 1978, as amended (FISA), among others. In particular, the authorities provided under ECPA are often used by these career professionals to obtain and assemble the critical building blocks in cybercrime, child pornography, and national security investigations, including those related to international terrorism and espionage. In the modern era, criminals regularly use electronic devices, ranging from mobile phones to networked computers and servers to assist in their criminal enterprises, whether as the means of committing the crime itself (for example, in the transmission of digital images of minors being sexually exploited) or as a means of perpetuating the criminal activity (for example, the gang leader who keeps his hit list stored in a file on his online email account).[2]

One of the primary reasons cited in favor of substantively amending ECPA to alter the standards for the collection of certain types of communications information is the dramatic change in technology that has taken place since ECPA was first enacted. As the Members of this Committee know, ECPA was enacted in 1986 against a backdrop of emerging, innovative technologies, including electronic mail. This was, of course, well

[2] *See* United States Department of Justice, Computer Crimes and Intellectual Property Section, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE ix (3d Ed. 2009), available online at <http://www.justice.gov/criminal/cybercrime/ssmanual/ssmanual2009.pdf> (visited Sept. 18, 2010) ("CCIPS Manual").

before the development of the World Wide Web by Tim Berners-Lee at CERN in 1991, and it significantly pre-dated the massive expansion in the public use of the Internet since then, to say nothing of the concurrent evolution in the use of digital technology toward the widespread deployment and use of Internet-enabled mobile devices and "cloud computing." But simply because ECPA was first enacted long ago, in an era when the use of the Internet and networked mobile devices was dramatically less prevalent, does not mean that the principles underlying that statute and the balance that it carefully struck between the privacy interests of individuals, on one hand, and the legitimate public benefits provided by law enforcement access to certain types of communications information, on the other, is any less valid today. Indeed, what is often forgotten in the debate about ECPA is that most of the protections afforded to the public under ECPA are *not required* by the United States Constitution, including the Fourth Amendment, but rather are a matter of legislative will, enacted by Congress to protect privacy with respect to certain types of information that it believed warranted such protection.[3] As a result, while ECPA's provisions are undoubtedly complex (perhaps at times unnecessarily so), and often draw lines that at first blush may seem arbitrary, the reality is that ECPA's text and structure – including some of its most criticized provisions – are the result of nothing more and nothing less than robust debate (and ultimately a compromise) between the interests represented here today.

In striking this balance when enacting ECPA (and making subsequent amendments) – contrary to the press coverage regarding the reform proposals being

[3] As Professor Orin Kerr has noted, while the Fourth Amendment has been interpreted by the courts to provide fairly strong privacy protection for homes in the physical world, standing alone, it offers fairly weak privacy protection online. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1211-12 (2004)

discussed today – Congress set the initial bar fairly high for broad government access to communications information. Indeed, as DOJ's Office of Legal Counsel noted in 2008, ECPA establishes a broad "background rule of privacy…generally bar[ring] a provider from giving the Government a record or other information pertaining to a subscriber or customer." *See* Requests for Information Under the Electronic Communications Privacy Act, Memorandum Opinion for the General Counsel of the Federal Bureau of Investigation (Nov. 5, 2008), available online at <http://www.justice.gov/olc/2008/fbi-ecpa-opinion.pdf> (visited on Sept. 18, 2010) (discussing the general bar on disclosure contained in 18 U.S.C. § 2702(a)). Indeed, OLC relied on this fact about ECPA in part to buttress its conclusion that the national security letter (NSL) provision of ECPA did not afford the FBI access to certain data that it sought to compel from communications providers. *Id.* (noting that the provisions of ECPA granting government access to communications records constitute specific exceptions to the broad, general rule of privacy set forth in the statute and holding that, as such, additional exceptions would not be implied). Thus, it is clear that in enacting ECPA, Congress acted to ensure that the tools available to the government in this new and emerging space were carefully regulated in order to protect the interest of individuals in the privacy of their communications while preserving the ability of the government to obtain the information necessary when appropriate.

While ECPA provides rules for government access to both content and non-content information, it makes sense to focus first on the non-content information that the government might obtain, because it is this information, in particular, that is perhaps most important to investigators in the early stages of their work. Such non-content information

is comprised of, among other things, the metadata associated with a communication, including the information use to route and transmit a communication from end-to-end, as well as the subscriber information and other records associated with a given user account or identifier. Access to communications metadata and subscriber information can help investigators determine, among other things, what email address or phone number a particular individual is using, what communications provider supports the account, as well as identifiers associated with other suspects the individual is in communication with, when such communications took place, how long the communications lasted, and various other details of the target's communications activities, other than the content itself. Such records can also provide information about the location of a given individual, both on a historical and on a going-forward basis.

Not surprisingly, such information can be crucially important to investigators at the outset of an investigation, in part, because such information serves a sifting function, permitting law enforcement to determine whether a particular individual is properly the subject of investigation and whether the use of additional techniques might be warranted, as well as providing the factual support for any such additional investigative authority the government might seek, whether through court authorization or otherwise. At the same time, of course, these building block investigative techniques – seeking non-content information in the hands of third parties – also allow the government to determine that a given individual is *not* properly the focus of an investigation, that they have no connection to the activities the government is investigating, and therefore that they can appropriately be excluded from any further investigation. Such information thus can serve a privacy enhancing function, by ensuring that a given individual is only subject to

the minimal investigative techniques necessary. Thus, the tools provided in ECPA and other statutes permitting the government to obtain non-content communications information in the hands of third parties serves both law enforcement and privacy interests, conserving limited investigative resources and helping ensure that the government conducts only the minimum intrusion necessary into an individual's communications activities at the outset of an investigation.

And ECPA already limits the way in which the government may obtain these crucial investigative building blocks, by permitting particular types of data to be obtained only in certain circumstances and then only through certain processes, with a sliding scale of increasing authorizations and predication for more invasive techniques. Indeed, it is critical to note here that in creating a general bar prohibiting government access to certain non-content communications information in the hands of third-parties and providing a specific set of exceptions to this general bar in ECPA, Congress effectively limited the government's ability to obtain information that it would typically obtain, in other contexts, through a subpoena. Indeed, the background rule generally applicable here, is that an individual typically does not retain an objectively reasonable expectation of privacy in information voluntarily conveyed to a third party, even when is conveyed with the expectation that it will remain confidential. *See, e.g., Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."); *see also, e.g., SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) ("[W]hen a person communicates to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities."); *United*

States v. Miller, 425 U.S. 435, 443 (1976) ("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."). And, while there are a number of important exceptions to this general background rule, including those potentially applicable to the content of communications, for example, while they are in transit, *see, e.g., United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) (analogizing the expectation of privacy of in the contents of email to that in letters transmitted via regular mail), most of these exceptions do not apply to the non-content information that forms the critical building blocks of an investigation and which may be obtained, under certain circumstances, with less than a warrant under ECPA, *see Smith*, 442 U.S. 744-45 (holding that telephone customers have no legitimate expectation of privacy in dialing, routing, addressing, and signaling information transmitted to telephone companies); *United States v. Forrester*, 512 F.3d 500, 510-11 (9th Cir. 2008) (no reasonable expectation of privacy in information used to transmit Internet communications to and from users); *see also, e.g., United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) ("Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation."); *Guest v. Leis*, 255 F.3d 325, 356 (6th Cir. 2001).

Of course, the non-content data held by communications service providers comes in different varieties, and it is not unreasonable to argue that Congress ought provide stronger statutory protection for certain kinds of information versus others. For example, one might think that subscriber records ought generally be accessible to law enforcement

through, among other things, an administrative subpoena or a subpoena issued in the course of a grand jury investigation. *See, e.g.*, 18 U.S.C. § 2703(c)(2). At the same time, one might think that transactional records or account logs ought generally be accessible to the government not simply with a subpoena, but typically with some measure of direct judicial supervision, albeit perhaps on a showing less than probable cause. *See, e.g.*, 18 U.S.C. § 2703(c)(1)(B).[4] Of course, as the preceding citations demonstrate, ECPA make just such distinctions, generally requiring providers to disclose such non-content data to the government only under particular circumstances and, where appropriate, with judicial oversight.

And it is no different with content. ECPA already places stringent restrictions on government access to data stored by third parties on behalf of their customers. *See, e.g.*, 18 U.S.C. § 2703(a)-(b). Now, it is true that many of the rules applicable to stored communications seem archaic and appear to be a product of an era when the Internet involved the use of dial-up connections, where communications were only stored for short periods of time on servers maintained by internet service providers (ISPs), and where cloud computing was not the norm. For example, critics have pointed to the statutory rule in ECPA that treats stored communications differently depending on the length of time they are stored by a particular type of provider. *See* 18 U.S.C. 2703(a). Similarly, critics have also pointed to the fact that the Department of Justice has (often successfully) taken the position that a warrant is not required to obtain the content of communications stored by a third party once the communications have been retrieved by the putative recipient, even if they have been in storage only for a short period of time.

[4] Of course, ECPA also permits law enforcement access to such data without a court order under other circumstances, such as with the consent of the customer or subscriber, *see* 18 U.S.C. § 2703(c)(1)(C).

See CCIPS Manual at 129 (noting that in jurisdictions other than the Ninth Circuit, as a general matter, "[a]gents...can [] obtain [opened and sent] email...using a subpoena.").

The very fact that ECPA draws certain lines with respect to certain types of communications information based, in part, on the type of third-party entity stores them, how long they are held by the third party, and the like, reflects a measured legislative judgment of the appropriate balance between privacy and security. This is not to suggest that this legislative judgment cannot be revisited; it certainly can, and perhaps, as discussed below, should be revisited in certain areas. However, what it is important to note is that the lines drawn in ECPA are less the result of technological developments that the law has failed to keep up with, and are more the result of compromises made in the legislative process regarding where the appropriate lines ought to be. As such, it is important that any major change in the level of authorization required for government access to certain types of communications information or in the type of showing the government must make, ought carefully be considered, and always with an eye towards balancing individual privacy and law enforcement interests.

Indeed, the notion that ECPA is stuck in the past and can't adequately deal with or account for modern technology is simply a canard. In point of fact, ECPA has been amended more than dozen times since its enactment in 1986, including as recently as last year. These amendments, which have varied from the substantive to the technical, have consistently sought to balance the interests of law enforcement with Congress's legitimate desire to protect the personal privacy interests of Americans. At the same time, the government's use of ECPA has kept pace with developments in technology, as the government now regularly uses ECPA to obtain categories of information that hardly

even existed when ECPA was first enacted in 1986, including, for example, cell-site locational information. These facts reflect the continued vitality of this statute in the modern technological environment. And while some have argued that ECPA does not account for the development of the new cloud computing environment, the fact is that cloud computing as it is currently conceptualized is somewhat analogous to what ECPA refers to as remote computing services, where service providers host customer data and run the primary applications on their own servers, rather than the customer running the applications locally. While advocates of cloud computing may reasonably be concerned that the protections provided to customer data stored with a provider of remote computing services are not commensurate with their understanding of the appropriate level of privacy due to their customers files (and perhaps may not even be commensurate the customer's own views as to the appropriate level of privacy for his or her files), this is less a product of the change in technology and perhaps more a reflection of a change in public perceptions about where the balance between privacy and security ought be struck.

Another canard present in the ongoing public debate is that law enforcement is run amok in the cyber realm, collecting reams upon reams of data about ordinary Americans. The fact of the matter is that there is little, if any, data to support the claim that there have been extensive abuses of the authority granted law enforcement under any of the provisions of ECPA that are under discussion today. To the contrary, at a time when the Justice Department's Inspector General has taken a close look at many of the statutory tools provided to law enforcement and intelligence officers, including the authorities provided under FISA and the USA PATRIOT Act, the DOJ IG has put forward no report that I am aware of indicating a broad-based abuse of any of the ECPA

authorities that are the subject of the existing reform proposals. And, moreover, where concerns have arisen – for example, with respect to national security letters (including those issued under ECPA) – DOJ has moved swiftly to implement substantive reforms. Having served as part of the initial effort organized by the Office of the Attorney General and the National Security Division to respond to the concerns raised by the IG's first report on NSLs, I can attest to the utter seriousness with which the Department's senior leadership tackled these issues and the aggressiveness with which the Department implemented broad, sweeping reforms, including the creation of an unit within NSD's Office of Intelligence dedicated solely to oversight, and the institution of regular, consistent reviews of the FBI's use of national security investigative tools, even beyond NSLs.

All of this is not to say that some measure of ECPA reform is unwarranted, or that Congress should simply let the matter drop. To the contrary, I think there is substantial room for improvement in the existing statute and I firmly sympathize with the complaints from industry and others regarding the statutory ambiguities that exist in ECPA, as well as the often confusing (indeed, bewildering) array of standards, authorities, and definitions set forth in the statute, to say nothing of the diversity of the judicial decisions interpreting ECPA and the background constitutional rules. To pick just one example of many, one need only look to the Third Circuit's decision issued earlier this month, where that court held ECPA provides magistrate judges with the discretion to require the government to meet a higher standard (and even perhaps to obtain a warrant) in order to obtain information – in that case, historical cell site data – that the court determined would otherwise be available (without a warrant) under ECPA's court order provision.

See In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communications Service to Disclose Records to the Government, __ F. 3d __, slip op. at 21-29 (3d Cir. Sept. 7, 2010). This decision, standing on its own – not to mention the multitude of opinions across the country regarding the standards the government must meet in order to obtain historical or prospective cell site data – demonstrates that there is, in fact, a need for a close look at ECPA and that there may be room for some useful clarification of the existing statutory language.

At the same time, it is hard to understate the importance of ensuring that law enforcement has consistent, ready access to much (if not more) of the communications information that it has today. This is so because we live in an era of increasing, not decreasing cyber threats, ranging from transnational criminal gangs, to hackers, to national security threat actors, including hostile governments and increasingly sophisticated terrorist groups. Moreover, government access to communications information is perhaps most critical in protecting the most vulnerable amongst us: our children. There is a growing body anecdotal evidence from investigators (and some literature) to support the notion that pedophiles find substantive encouragement of their activities in online communities, and that this encouragement often results in increasing rates of illegal image sharing, as well as in these individuals taking further illegal action in the real world. These fora also often provide information on how these criminals might best hide their tracks on the Internet, directing them to providers and resources that make law enforcement's efforts to protect our children that much more difficult. In this way, child predators are much like potential terrorists online, finding encouragement,

support, and training over the Internet. Indeed, in many ways, these communities on the Internet can serve as a network of virtual caves and hideouts for child pornographers, cybercriminals, and foreign operatives alike, much like the Tora Bora complex in Afghanistan or the terrorist safe houses that dot the landscape of the Northern Areas of Pakistan. To limit the ability of our law enforcement personnel to ferret out these virtual hideouts and to track down their inhabitants in an era when the threat is growing and is more imminent raises obvious concerns. Indeed, in the absence of any substantive evidence of abuse or misuse of these authorities by law enforcement personnel, one may reasonably question the wisdom of substantially limiting (and essentially disarming) our frontline personal in the fight against these cyber predators.

My strong recommendation, as a result, is that Congress proceed quite cautiously and with deliberation in considering amendments to ECPA. Substantive changes to the statutory standards for accessing communications information covered by ECPA could have a dramatic and detrimental impact on law enforcement and the public safety. Thus, I recommend a three-step process for Congress's consideration of ECPA reform:

First, in my view, there are a number of somewhat modest amendments that Congress can make now to ECPA that would usefully clarify the statute, make it easier for industry to comply, and address existing issues created by outlier judicial decisions. For example, Congress could consider how to harmonize the existing definitions describing providers under ECPA, which currently make little sense, given that they differentiate between services that have largely merged in recent years, with communications services providers often providing both electronic communications services and remote computing services in the course of a given communications event.

See, e.g., CCIPS Manual at 117-20, 125-26. Similarly, Congress could likely easily address statutory ambiguities, like those that led to the Third Circuit decision described above, as well as the Ninth Circuit's outlier opinion in *Theofel v. Farey-Jones*, 359 F.3d 1006 (9th Cir. 2004), regarding the definition of electronic storage. These changes can likely be made through a consensus process and can almost certainly be completed in the next session of Congress.

Second, Congress should hold hearings over the next few months, and perhaps into the next session, specifically focused on each authority that it is considering substantively modifying. These hearings should focus on four issues with respect to each such authority: (1) how the government uses the current authority provided by statute and the tangible benefits to the public of the use of such authority; (2) whether the public's objectively reasonable expectation of privacy in the information sought by the government has substantively changed since the authority was provided; (3) whether there is any tangible, clear evidence of abuse or misuse of the authority by the government and whether such abuse, if any, is the result of procedures and processes that might be addressed through internal controls and reforms, rather than through legislative changes that would make the authority harder to obtain or use; and (4) the impact of any substantive change on the ability of law enforcement to protect the public.

Third, having determined what authorities ought be changed based on a careful balancing of the various interests at stake, Congress ought further consider whether additional provisions are necessary to counterbalance the impact of any such changes on public safety. So, for example, if Congress determines that it is in the public interest to raise the statutory standard for obtaining certain types of information from say a

subpoena to a court order, or from a court order to say a warrant, Congress may also consider requiring communications service providers to retain the covered information for longer periods of time. Such a provision could serve to ameliorate the additional burdens placed upon the government, including but not limited to the inevitable delays associated with a more onerous (but rigorous) authorization process.[5]

In sum, the message I hope to have conveyed today is as follows: (1) ECPA plays an important role in today's increasingly cyber-connected world, both in terms of protecting individual privacy interests, as well as ensuring public safety by providing government access to certain types of communications information in the hands of third-party service providers; (2) ECPA can (and should) be improved and made more consistent and clearer, particularly with an eye towards making the compliance process less onerous on providers; (3) any substantive changes to the authorization or predication levels contained in ECPA should be approached with great caution and a due regard for the implications of such changes on law enforcement investigations; and (4) where appropriate, Congress ought consider offsetting any substantive changes made to the authorities contained in ECPA by ensuring that the government has access to the relevant data once the appropriate requirements are met.

Thank you very much for the opportunity to present my view today.

---

[5] As the Committee may be aware, the Department of Justice has long considered the issue of data retention and, having served as the coordinator of one such working group led by the Assistant Attorney General for Legal Policy back in 2006, I can attest to the value of such a provision for the government's law enforcement efforts, in particular in child exploitation investigations. Of course, there are significant issues that would need to be addressed including cost and liability issues for industry, as well as the privacy and security implications of large amounts of data being retained by providers.

Testimony of Cameron F. Kerry
General Counsel
United States Department of Commerce

Before the
Committee on the Judiciary
United States Senate

The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age

I. Introduction

Chairman Leahy, Ranking Member Sessions, and Members of the Committee, thank you for this invitation to testify on behalf of the U.S. Department of Commerce concerning reform of the Electronic Communications Privacy Act of 1986 (ECPA). In the 25 years since ECPA was enacted, the communications and information landscape has been transformed. Although the authors of the law, including yourself, Mr. Chairman, recognized that the communications environment would be in a state of continual evolution, I doubt that anyone foresaw the scale and scope of the revolution to be fueled by mobile communications, the global Internet, and ever smaller, more powerful communications and computing devices.

I welcome the Committee's decision to hold this hearing and to begin another of its periodic reviews of ECPA. The goal of this effort, as always, should be to ensure that, as technology and market conditions change, ECPA continues to serve the original purpose articulated by this Committee -- to establish "a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement" to gather the information it needs to keep us safe.[1]

---

[1] S. Rep. No. 99-508, 99th Cong., 2d Sess. 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

I am especially pleased to be appearing jointly with our colleagues from the Department of Justice. The Administration has just recently launched an inter-agency effort to develop views on both commercial data privacy and a range of issues related to new information and communications technologies. While our effort is still in its early phases, we are guided by our shared belief that any legislative review of ECPA must be undertaken carefully and in a way that: (1) adequately protects privacy and builds consumer confidence; (2) addresses concerns raised by U.S. commercial firms about innovation, competition, and other challenges they face in a global marketplace; and (3) allows the government to protect the public in timely and effective ways.

I would like to talk today about the importance of digital communications innovation to the U.S. economy and society and the contribution ECPA's privacy framework has made to that innovation, and to reflect on some of the technology and market developments that may affect this privacy framework.

II. Commerce Department Initiatives to Address Internet Privacy and Innovation Challenges

President Obama has long recognized the importance of a modern communications infrastructure – including a robust, open Internet – to economic development, job creation, social interaction, and participatory democracy.[2] The President has also emphasized the need for "sensible safeguards that protect privacy in this dynamic new world."[3] That is why he has supported legislation directing the Federal Communications Commission (FCC) to develop a

---

[2] *See, e.g.*, "Barack Obama: Connecting and Empowering All Americans through Technology and Innovation," at 1-2, http://www.barackobama.com/pdf/issues/technology/Fact_Sheet_Innovation_and_Technology.pdf (Obama Technology Policy).
[3] *Id.* at 3.

National Broadband Plan.[4] It is why the President directed his Administration to develop an action plan for cybersecurity. It is why the entire Administration is moving forward to translate the values of openness into lasting improvements in the way government makes decisions, solves problems, and addresses national challenges.[5]

Because an open, innovative Internet is critical to the Nation's economic health, promoting its growth is a vital part of the Department of Commerce mission. To this end, Secretary Locke has established a Department-wide Internet Policy Task Force charged with identifying and developing a privacy and cybersecurity framework for Internet-based communications that meets the needs of the 21st Century information economy. This task force will also identify trade barriers around the world that may impede the free flow of information and commerce over the Internet. The Department's National Telecommunications and Information Administration (NTIA), with its statutory mission to advise the President on telecommunications and information policy, plays a leading role in the Task Force. The Task Force also draws on the expertise of the Department's International Trade Administration in international markets, the National Institute of Standards and Technology in innovation and technology, and the Patent and Trademark Office as, by statute, the Administration's advisor on intellectual property.

The Task Force's work on privacy began with a series of listening sessions with officials from major U.S. technology companies, advocacy groups, academic experts and businesses across the country. On April 23, 2010, it released a Notice of Inquiry on "Information Privacy

---

[4] *See Connecting America: The National Broadband Plan* (Mar. 2010), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-296935A1.pdf (*National Broadband Plan*).
[5] *See* Department of Commerce Secretary Gary Locke, "Our Open Government Plan" (Apr. 7, 2010), *available at* http://open.commerce.gov/.

and Innovation in the Internet Economy," which prompted more than seventy comments.[6] On May 7, 2010, the Task Force held a symposium on "Privacy and Innovation," in which a broad cross-section of industry, consumer groups, and privacy advocates participated. This fall, the Commerce Department will release a report with findings and recommendations on commercial data privacy issues and data breach. The Task Force is working closely with the Department of Justice, as well as other departments and agencies, in these activities.

It is worth noting that, although our Notice of Inquiry did not mention ECPA, multiple commenters volunteered the importance of reexamining the statute.[7] I would be happy to provide the Committee with an abstract of the commenters' views on this issue. Those comments, the information gathered in our listening sessions, and the Department's efforts over the past year to identify key Internet policy challenges, including privacy, inform my testimony today.

---

[6] *Information Privacy and Innovation in the Internet Economy*, Docket No. 100402174-0175-01, at 34 (filed June 14, 2010), *available at* http://www.ntia.doc.gov/frnotices/2010/FR_PrivacyNOI_04232010.pdf. For convenience, all subsequent citations in this document to "Comments" shall refer to pleadings filed in Docket No. 100402174-0175-01.

[7] *See* Google Comments, at 4, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Google%20Comments%2Epdf; Microsoft Comments, at 3, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Microsoft%20Comments.pdf; Digital Due Process Coalition Comments , at 1-9, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Digital%20Due%20Process%20Coalition%20Comments.pdf; AT&T, Incorporated Comments, at 15-16, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/ATT%20Inc%20Comments.pdf (AT&T Comments); American Civil Liberties Union Comments, at 1-9, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/ACLU%20Comments.pdf (ACLU Comments); Center for Democracy and Technology, at 5-6, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/CDT%20DOC%20NOI%20comments.pdf (CDT Comments); Computer and Communications Industry Association Comments, at 3-7, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Computer%20and%20Communications%20Industry%20Association%20Comments%2Epdf; Diedre K. Mulligan Comments, at 3, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Deirdre%20K%2E%20Mulligan%20Comments%2Epdf; Information Technology and Innovation Foundation, at 6, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/ITIF%20Comments%2Epdf.

III. ECPA's Balance and the Growth in Electronic Communications

Over the past several decades, the explosion of electronic communications – notably the proliferation of broadband Internet service and Internet-based services and applications, as well as the expansion of wireless communications – has created enormous benefits for our nation. By some estimates, for example, the Internet contributes $2 trillion to the Nation's annual Gross Domestic Product (GDP) and supports some three million jobs.[8] The contribution of wireless services to overall GDP increased by more than 16 percent annually between 1992 and 2007, as compared with less than 3 percent annual growth for the rest of the economy.[9] These measures capture only part of the sweeping changes to ways of doing business and of communicating in our society.

ECPA has contributed to this growth. As Congress recognized in 1986, the absence of sound privacy protections for electronic communications "may unnecessarily discourage potential customers from using innovative communications systems" and "American businesses from developing innovative forms of telecommunications and computer technology."[10] In establishing a privacy framework for electronic communications, ECPA has created clear and predictable rules under which service providers could operate as well as a protected, trusted environment for consumers and businesses. It also ensured that law enforcement and national security personnel can get access to electronic communications, subject to judicial oversight and consistent with the Fourth Amendment and American principles. As Mr. Baker points out in his testimony, one of the values served by law enforcement use of this information is to protect

---

[8] *See* Executive Office of the President, National Economic Council and Office of Science and Technology Policy, *A Strategy for American Innovation: Driving Towards Sustainable Growth and Quality Jobs*, at 5 (Sept. 2009), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/innovation-whitepaper.pdf; J. Deighton, J. Quelch, Hamilton Consultants, Inc., "Economic Value of the Advertising-Supported Internet Ecosystem, at 4 (June 2009), http://www.iab.net/media/file/Economic-Value-Report.pdf.

[9] *See National Broadband Plan*, at 75.

[10] S. Rep. No. 99-541, at 5, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

individual privacy from cybercriminals and other malicious actors. In this way, as Congress foresaw, ECPA helped stimulate the development of the electronic communications industry and the many economic and social benefits that it has produced in the intervening quarter century.

Congress recognized in 1986 that the law should not remain static as technology, businesses practices, and consumer behavior changes: privacy protections "must advance with technology" or privacy will "gradually erode as technology advances."[11] ECPA modernized the federal wiretap statute, also known as Title III, to take into account the rise of new communications services – such as electronic mail – that barely existed when Title III was enacted in 1968. As Mr. Baker points out, Congress has amended ECPA on several occasions to ensure that changed circumstances did not disrupt the intended balance between individual privacy and law enforcement needs.

As the Committee begins its work of examining the ECPA's ongoing role in the digital communications environment, you face the question whether changes in that environment since 1986 warrant changes in the statute to preserve the balance Congress struck – and has maintained over time – between the privacy expectations of citizens and the legitimate needs of law enforcement.

At the fulcrum of that balance is a clear distinction between "content" and "non-content" information. ECPA recognizes the different privacy interests in these two categories, and allows the government access to non-content information through a less rigorous legal process. ECPA's drafters have worked to maintain this distinction, consistent with the overall balance between law enforcement and privacy interests. ECPA defines "contents;"[12] "non-content" is described in

---

[11] *See id.*
[12] *See* 18 U.S.C. § 2510(8) (contents include "any information concerning the substance, purport, or meaning of" a communications).

terms of a "record" or "other information" pertaining to a customer.[13] Congress has recognized that "transactional records from on-line communication systems reveal more than telephone toll records or mail covers."[14] Data not imagined by ECPA's original drafters, such as information created during websurfing, may currently be treated by ECPA as non-content information.

Based on the Department's public outreach, I believe that the results have generally been in accord with most users' reasonable expectations. As Mr. Baker amply documents in his testimony, moreover, reasonable and timely access to non-content information, such as a calling record, is critical to effective law enforcement. In seeking such access, the Department of Justice has hewn closely to the lines Congress has drawn between content and non-content information.

The Commerce Department is working with the Justice Department and other interested Executive Branch departments and agencies to consider whether substantive changes to ECPA are warranted to ensure that the balance struck in 1986 remains fair and appropriate under current technology and market conditions, as well as consumer and business practices. Once this process is completed, the Administration will be happy to work with the Committee and Congress on ECPA reform initiatives and offer views.

What I can do today is focus on what the Commerce Internet Policy Task Force and our agencies have identified as some of the most significant ways that changes in technology, shifts on societal use of communications, and the growth of the digital economy have altered the communications environment. ECPA must continue to provide a clear and well-marked road map for providers, law enforcement, and citizens and to enable further innovation and growth in technology, society, and the digital economy.

---

[13] *See id.* §§ 2702(c), 2703(c) (1).
[14] H. Rep. No. 103-827, 103rd Cong., 2d Sess., at 31 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3511.

IV. The Changing Technologies of Electronic Communications

Growth of the Internet and Cloud Computing

In less than two decades, the Internet has evolved from a research network to a global communications platform that has transformed the way in which Americans gather and disseminate information, revolutionized the ways in which businesses develop, produce and market their products, and allowed virtually anyone with a good idea or an interesting point of view to find and build a following.[15] According to the NTIA-commissioned survey of Internet usage conducted by the Census Bureau, in October 2009, nearly 69 percent of U.S. households were connected to the Internet, as compared to 41.5 percent in August 2000.[16] The greatest transformation over the same period has been the growth of household use of broadband Internet service from 4.4 percent to 63.5 percent of households.[17] Worldwide, the FCC reports there are now 1.7 billion Internet users.[18]

As the number of Internet users has grown and the speed and capacity of transmissions pathways has multiplied, there has been a vast increase in the number and variety of online services, information, and applications. As a result, there has been a fundamental expansion in "the scope and magnitude of online data being collected and used in a wide variety of contexts" and "consumers are choosing to share an unprecedented amount of personal information with trusted parties and each other."[19]

---

[15] *See* Letter from Lawrence E. Strickling, NTIA, to FCC Chairman Julius Genachowski, in GN Docket No. 09-51, at 1-2 (Jan. 4, 2010), *available at* http://www.ntia.doc.gov/filings/2009/FCCLetter_Docket09-51_20100104.pdf.
[16] NTIA, *Digital Nation: 21st Century America's Progress toward Universal Broadband Internet Access*, at 4 (Feb. 2010), *available at* http://www.ntia.doc.gov/reports/2010/NTIA_internet_use_report_Feb2010.pdf.
[17] *Id.*
[18] *National Broadband Plan*, at 60.
[19] AT&T Comments, at 3-4, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/ATT%20Inc%20Comments.pdf.

The global growth of cloud computing services – the ability to store data in the Internet "cloud" or to access and engage Internet-based data processing applications – is a prominent example of this phenomenon that is changing the ways we use and store information. The range of cloud-based services and applications available today and the pervasiveness of their use by consumers and businesses far exceed the levels that existed in remote computing 25 years ago. According to one projection, cloud computing revenues will grow from $46 billion in 2009 to $150 billion in 2012 and, next year, 25 percent of new software deployments will be cloud-based applications.[20] According to one 2008 survey, "at least 40% of American Internet consumers, and at least 59% of such consumers in the 18-29 age range, have engaged in some form of cloud computing activity."[21]

This growth is fueled by benefits for individuals and businesses, including the United States Government. The core value proposition of cloud computing services is the ability to replace local computing and storage capability (in either enterprise or home settings) with more flexible, affordable, reliable, on demand resource pooling from remotely-hosted services with equal or greater privacy and security properties compared to what is available through local services.[22] Users of cloud-based email services, such as Gmail and Hotmail, can access their messages from any computer anywhere in the world. A cloud user never has to worry about having left a file at the office when he or she wants to work on it from home or on the road.

---

[20] Salesforce.com Comments, at 1, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Salesforce%20Comments%2Epdf.

[21] American Civil Liberties Union of Northern California Comments, at 2, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/ACLU%20Appendix%20A%20-%20Cloud%20Computing%20Issue%20Paper.pdf.

[22] The Commerce Department's National Institute of Standards and Technology (NIST) defines cloud computing as "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." Mell and Grance, The NIST Definition of Cloud Computing, *available at* http://csrc.nist.gov/groups/SNS/cloud-computing/.

Cloud-based services enable small and medium-sized businesses to perform essential management and administrative functions without having to keep up with investment in on-site hardware and software.[23]

Despite the benefits of cloud computing, there is evidence that concerns about the privacy and security of remotely-stored content have made both the public and private sectors wary about fully migrating to using cloud computing services. A December 2009 survey conducted for Microsoft revealed that more than 60 percent of the consumers and more than 75 percent of senior business leaders questioned cited data safety, security, and privacy as the chief concerns about cloud computing. More than 90 percent of those surveyed expressed reservations about the security and privacy of personal data stored in the cloud.[24] That finding is confirmed by a 2010 Harris Interactive Poll, which indicated that of those Americans who are not interested in using cloud computing, 81 percent are reluctant, at least in part, because they are concerned about the security of their information in the cloud.[25] These early surveys reveal that users are sensitive about whether their data is secure and private, and that they are more somewhat concerned about the actions of criminals or by service providers, than about government access.[26]

Similar concerns about the securing of data become apparent in skepticism about US-based cloud computing services by foreign customers. Even some of our closest trading partners are considering limiting the cross-border flow of data to the United States in response to

---

[23] *See* Jeffrey Rayport and Andrew Heyward, *Envisioning the Cloud: the Next Computing Paradigm*, at 14-24 (Mar. 2010), *available at* http://www.marketspaceadvisory.com/cloud/Envisioning-the-Cloud.pdf.
[24] Penn, Schoen, and Berland, *Cloud Computing Flash Poll – Fact Sheet*, Microsoft, *available at* http://www.microsoft.com/presspass/presskits/cloudpolicy/docs/PollFS.doc.
[25] ACLU Comments, at 3.
[26] *See* Penn, Schoen, and Berland, *Cloud Computing Flash Poll*, at slide 19, available at www.microsoft.com/presspass/presskits/cloudpolicy/docs/CCTopline.ppt.

perceived weaknesses in the U.S. legal regime for data privacy, including protections against government surveillance.[27] The Commerce Department believes that American common law, our Constitution, and the body of laws – of which ECPA is one part – have erected a set of protections for the privacy of individual electronic information that is second to none. The stability and certainty provided by U.S. law in this area is evident in the growth of the digital economy. The Administration places a priority on ensuring that individual users and enterprise customers develop well-founded trust in the safety, security, and privacy of evolving cloud services, and we are confident in the due process and transparency of U.S. law. At the Department of Commerce, we are committed to working with our colleagues at Justice and members of this committee to address any misperceptions the global marketplace may have in this area.

The Growth of Online Storage of Electronic Messages and Attached Content

When an electronic message (and any attached document) arrives at the recipient's online mailbox, ECPA affords it substantial privacy protection; government may compel disclosure of the contents of that message only pursuant to a warrant issued by an independent judicial authority upon a showing of probable cause.[28] The legal status of the document changes (at least in most federal circuits)[29] on the 181st day or, more commonly, as soon as the recipient opens the message. Once either of these events occurs, the contents become a stored document

---

[27] AT&T Comments, at 18; CDT Comments, at 34-35; Salesforce.com Comments, at 2; Comments of the United States Council for International Business, at 3 (filed June 14, 2010), *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/United%20States%20Council%20for%20International%20Business%20Comments.pdf. *See also* Mayer Brown, "Cloud Computing May Violate German Data Privacy Laws" (July 20, 2010), *available at* http://www.mayerbrown.com/publications/article.asp?id=9363&nid=6.

[28] Providers may voluntarily disclose content to a government entity in certain limited circumstances such as emergency situations and when evidence of a crime is inadvertently obtained.

[29] *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1075-77 (9th Cir. 2003), *cert. Den.*, 543 U.S. 863 (2004) (ECPA provides warrant protection for opened emails under many conditions).

that – like content held on behalf of a subscriber by a provider of remote storage or data processing – the government can access via a court order issued upon a documented showing of relevance or by a subpoena.[30]

These varying levels of privacy protection were the product of careful legislative deliberation in 1986, when the notion of remote computing (as a precursor of today's cloud computing) was anticipated by the drafters of the 1986 Act. In the new world of cloud computing, and the exponential increase in the use of email, texts, tweets, and Facebook postings, attitudes and practices may have evolved.[31] These changing business and consumer practices raise questions about what privacy expectations are reasonable and whether additional protections should be mandated by law.[32] In this regard, I agree with Mr. Baker: Technology has evolved and it is natural to ask whether changes to ECPA are appropriate.

Furthermore, as communications networks and digital information systems become more sophisticated, they not only store more content – including voice, text, video -- but also they record in greater and greater detail records of the interaction between individual users and that content. This realm of 'transactional records' was originally defined by telephone calling records and simple logs of emails sent and received. Today, the volume and complexity of those records has grown with the diversity and granularity of new service offerings available through the Internet, mobile phone networks, and the cloud. These records play a critical role in enabling innovation in the digital environment. Records of web search terms enable those providing

---

[30] When the government seeks to obtain a document without a warrant, it must give notice to the affected user. That notice, however, can be delayed, under certain conditions, for as many as 180 days.
[31] *See* Google Comments, at 4 (advent of cloud computing "is leading to a vast migration of data from personal computers, filing cabinets, and offices to remote third-party servers"); J. Beckwith Burr, "The Electronic Communications Privacy Act of 1986: Principles for Reform," at 8-9 (Mar. 2010) , *available at* http://www.digitaldueprocess.org/files/DDP_Burr_Memo.pdf.
[32] CDT Comments, at 35.

Internet search services to increase the relevance of search results returned to individual users based on their prior browsing history. Data on the location of a given mobile device help network and applications providers to offer more customized service. And logs of our interactions with files and data in the cloud help to troubleshoot bugs in the operation of cloud services. These same transactional records can help both commercial service operators and law enforcement agencies to detect security breaches based on noticing anomalies in patterns of information usage and access recorded in these logs.[33]

Growth of Wireless and Location Services

The Federal Communications Commission issued its first group of cellular radio licensees only a few years before ECPA's enactment and few anticipated then the future of wireless communications. According to the FCC, today there are some 4.6 billion mobile phone subscribers worldwide.[34] In the U.S. alone, roughly 91 percent of the population has a wireless phone.[35] The use of smart phones in the United States grew by roughly 50 percent from 2008 and 2009, with sales expected to eclipse traditional cellular phone sales in 2011, shifting the balance toward these more powerful devices.[36] The FCC has concluded that mobile networks will be the next generation of Internet users, as smart phones enable those with mobile access to experience the benefits of Internet connectivity.[37] This will expand both penetration and usage of the multiplying range of services and communications available online.

The expansion of advanced mobile phone usage also provides unique new data streams. When turned on, cell phones and other wireless communications devices are in nearly constant

---

[33] Weitzner, Abelson, Berners-Lee, Feigenbaum, Hendler, Sussman, Information Accountability, *Communications of the ACM*, Jun. 2008, 82-87.
[34] *National Broadband Plan*, at 60.
[35] CTIA Quick Facts: Year End 2009, http://www.ctia.org/media/industry_info/index.cfm/AID/10323.
[36] *See* Roger Entner, Smartphones to Overtake Feature Phones in U.S. by 2011, Nielsenwire, *available at* http://http://blog.nielsen.com/nielsenwire/consumer/smartphones-to-overtake-feature-phones-in-u-s-by-2011/.
[37] *See* National *Broadband Plan*, at 60.

communications with nearby cell towers. In areas where there are multiple towers, a device may communicate with several towers at the same time. Notably, information about a wireless phone's general whereabouts is essential to providing cellular service. In many cases, such general location information may be supplemented by precise Global Positioning Satellite (GPS) data. Many third-party applications providers are developing innovative services based on the increased availability of real-time location data from carriers and devices themselves. Clarity of rules in this emerging area is critical for the successful development, deployment, and adoption of location-based services. Just as some of today's technologies were unanticipated 25 years ago, I am sure new developments will emerge that we cannot foresee today.

V. **Conclusion**

Thank you again for inviting the Department of Commerce to testify on this important issue. Over the last 25 years, there have been wholesale changes in the ways Americans use electronic communications, as well as a pervasive shift in the amount of sensitive information that we entrust to third parties. I applaud this Committee's decision to examine ECPA once again to ensure that the fair balance of reasonable law enforcement access, individual privacy protection, and clarity for service providers and customers first established in 1986 is preserved in the face of changing technology. The Department stands ready to work with this Committee as your process goes forward.

That concludes my remarks. I would be happy to answer questions from you and other members of the Committee.

Statement of

The Honorable Patrick Leahy

United States Senator
Vermont
September 22, 2010

Statement Of Senator Patrick Leahy (D-Vt.),
Chairman, Senate Committee On The Judiciary,
Hearing On "The Electronic Communications Privacy Act:
Promoting Security And Protecting Privacy In The Digital Age
September 22, 2010

Today, the Committee holds an important hearing on the Electronic Communications Privacy Act (ECPA) -- one of the Nation's premier digital privacy laws. Four decades ago, Chief Justice Earl Warren wrote that "the fantastic advances in the field of electronic communication constitute a greater danger to the privacy of the individual." These words are as relevant today as they were then. For many years, ECPA has provided vital tools to law enforcement to investigate crime and to keep us safe, while at the same time protecting individual privacy online. As the country continues to grapple with the urgent need to develop a comprehensive national cybersecurity strategy, determining how best to bring this privacy law into the Digital Age will be one of Congress's greatest challenges.

American Innovation Has Outpaced Our Digital Privacy Laws

When Congress enacted ECPA in 1986, we wanted to ensure that all Americans would enjoy the same privacy protections in their online communications as they did in the offline world, while ensuring that law enforcement had access to information needed to combat crime. The result was a careful, bipartisan law designed in part to protect electronic communications from real-time monitoring or interception by the Government, as emails were being delivered and from searches when these communications were stored electronically. At the time, ECPA was a cutting-edge piece of legislation. But, the many advances in communication technologies since have outpaced the privacy protections that Congress put in place.

Today, ECPA is a law that is often hampered by conflicting privacy standards that create uncertainty and confusion for law enforcement, the business community and American consumers.

For example, the content of a single e-mail could be subject to as many as four different levels of privacy protections under ECPA, depending on where it is stored, and when it is sent. There are also no clear standards under that law for how and under what circumstances the Government

can access cell phone, or other mobile location information when investigating crime or national security matters. In addition, the growing popularity of social networking sites, such as Facebook and MySpace, present new privacy challenges that were not envisioned when ECPA was passed.

Simply put, the times have changed, and so ECPA must be updated to keep up with the times. Today's hearing is an opportunity for this Committee to begin to examine this important issue.

Principles For ECPA Reform

While no one would quibble with the notion that ECPA is outdated, the question of how best to update this law has no simple answer. In fact, there are many different -- and at times competing -- views about how best to update this law. This Committee will carefully examine each of these proposals. But, I believe that there are a few core principles that should guide our work.

First, privacy, public safety and security are not mutually exclusive goals. Meaningful ECPA reform can, and should, carefully balance and accomplish each.

Second, reforms to ECPA must not only protect Americans' privacy, but also encourage American innovation. America is the birthplace of the Internet and we should continue to lead in developing policies that address digital privacy. This not only leads to greater confidence in our laws, but encourages greater investment in new communications technologies.

Lastly, updates to ECPA must instill confidence in American consumers. If citizens are confident that their privacy rights will be protected online, they will be more comfortable using American communications technologies at home and at work.

I am pleased that we will hear from the General Counsel of the Department of Commerce, who has unique insights into the impact of ECPA on American innovation. I am pleased that we will also get the views of the Department of Justice, which relies upon ECPA to carry out its vital law enforcement and national security duties.

We also have an outstanding panel of expert witnesses to advise the Committee on the role of technology in protecting privacy in the 21st Century. I applaud the work of the Center for Democracy & Technology, Microsoft and other stakeholders in helping to build industry consensus on a core set of proposals to update ECPA.

I thank all of our witnesses for appearing today. I look forward to a good discussion.

# # # # #

Concurring opinion, Lopez v. United States, 373 U.S. 427, 441 (1963)

ECPA Reform and the Revolution in Cloud Computing

Statement of David Schellhase

Executive Vice President and General Counsel

Salesforce.com

Submitted to

The U.S. Senate

Committee on the Judiciary

September 27, 2010

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 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

[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.

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 pertain to them. In this respect, multi-tenant cloud computing is like online banking – it

[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.

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

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

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.

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

- 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.

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.

STATEMENT OF BRAD SMITH
GENERAL COUNSEL
MICROSOFT CORPORATION

BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

HEARING ON ELECTRONIC COMMUNICATIONS PRIVACY ACT REFORM

"THE NEED FOR ECPA REFORM AND ADVANCING CLOUD COMPUTING"

SEPTEMBER 22, 2010

Chairman Leahy, Ranking Member Sessions, and honorable Members of the Committee, my name is Brad Smith, and I am the general counsel and senior vice president for Legal and Corporate Affairs at Microsoft Corporation. In this capacity, I am responsible for the company's overall legal function, along with its government affairs and philanthropic work.

Thank you very much for this opportunity to discuss Microsoft's perspectives on the Electronic Communications Privacy Act (ECPA) and how the reform of this law can help promote security and protect privacy in the digital age. At Microsoft, we consider an updated ECPA to be key to realizing the full potential of exciting new computing technologies that allow users to collect, digitize, and store unprecedented amount of information online. These technologies, which are often grouped together under the heading of "cloud computing," are helping to reinvigorate our economy by enhancing productivity, empowering small businesses and enterprises of all sizes, and creating jobs. They are also generating whole new forms of social interaction and unleashing the power of information in rich new ways.

At the same time, these advances raise important and sometimes even profound new questions about the privacy and security of data stored in online services. As an industry, we recognize that enterprises and individual consumers will use new technologies only if they have confidence that their information will be reasonably protected. As companies, we see that the economic benefits of investment and potential for innovation will be fully realized only if clear and up-to-date privacy laws protect confidential information. And as individuals, we want to ensure that one of the most valued benefits of the PC era – that computing truly was *personal* in nature – will continue to flourish as information moves from the desktop to data centers.

ECPA was passed by Congress in 1986 -- almost 25 years ago -- to establish rules to address these issues and to strike an appropriate balance among the legitimate needs of law

enforcement, the burdens on service providers, and the public's reasonable expectations of privacy. Over this period, technology has enabled individuals and businesses to move data from the desk drawer to the desktop, to networks, to the Web, and now, in greater volumes than ever before, to the cloud, but ECPA and the balance it struck have not kept pace. We urge Congress to modernize ECPA in light of advances in technology and to ensure that, once again, the law strikes the appropriate balance among these important interests.

Microsoft supports the reform principles advanced by the Digital Due Process Coalition and further urges that Congress consider these as the pillars of ECPA reform. The Digital Due Process Coalition principles will enable citizens to trust that their data will be subject to reasonable privacy protections and preserve the ability of law enforcement to develop the fundamental building blocks of their investigations. The recommended changes also will provide greater clarity for service providers who must comply with ECPA.

ECPA reform is not the only area in which legislative action is warranted in order to advance the development and benefits of these technologies. In our view, legislation also is needed to address other emerging issues relating to privacy and security holistically, and not solely in the context of law enforcement access to user data. Users have reasonable interests in maintaining the security and privacy of their data in relation to their service providers and private third parties, and the importance of data privacy and security extends beyond the United States to include information that crosses national borders. To address these concerns, we urge Congress to consider comprehensive legislation to address issues of privacy and security relating to cloud computing. This, in turn, will help ensure that consumers and enterprises fully realize the exciting benefits of new computing technologies.

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

We live in an era in which unprecedented amounts of personal information are being collected, digitized, and stored online. New computing technologies are creating new benefits for consumers and enterprises, but they also are presenting important new questions for the protection of personal privacy. The computing industry, no less than consumers, needs clear and up-to-date privacy laws in order to continue to realize the benefits of new computing innovation.

With each passing year, more and more information is being collected, digitized, and stored online. This information is being harnessed with increasing computing power in new and beneficial ways that were not imagined when ECPA was first enacted almost 25 years ago. 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, expanded access to computational capabilities previously available only to the very largest companies, better collaboration through "anytime, anywhere" access to IT for users located around the world, and new opportunities for innovation as developers move to this new computing paradigm.

For example, a Microsoft product called Health Vault is helping doctors and patients at the Cleveland Clinic manage chronic health conditions such as diabetes and heart disease, by digitizing patient data, storing it online, and making it easily accessible to patents and health care providers. Using at-home medical devices such as heart rate monitors, glucometers, scales and blood pressure monitors, patients can track their own conditions and the effectiveness of their treatments. These medical devices can then upload the patient's data into Health Vault, which incorporates the data into the patient's personal health record at the Cleveland Clinic.

Another benefit of this new "cloud" computing is scalability, or the ability of businesses to quickly increase their computing capacity to meet peaks in demand. Everyone is familiar with

Domino's Pizza. Domino's Pizza's busiest day of the year by a wide margin is Super Bowl Sunday. Orders on Super Bowl Sunday are 50 percent above Domino's next-highest peak, a typical Friday night. Rather than buy a huge amount of IT hardware and software to handle its Super Bowl demands—which would go unused the rest of the year—Domino's Pizza turned to Windows Azure to handle the excess IT needs on that day. One of the interesting parts of this story is that the application Domino's is hosting on Windows Azure is based on Apache Tomcat, an open-source implementation of various Java technologies.

Microsoft is well-positioned to comment on this technological evolution and its impact on the need for ECPA reform. We have offered Internet-based services for almost 15 years, dating back to MSN's dialup Internet service and followed by our web-based Hotmail email service. These were the early forms of so-called cloud computing: convenient, on-demand online services. Today, we offer a full array of cloud computing services to individuals as well as to enterprises, including our hosted messaging and online collaboration solutions known as Microsoft Business Productivity Online Suite and our cloud-based storage and computing resources offered via Microsoft Azure. From our vantage point, we have seen the full arc of how the technologies governed by ECPA have evolved in the years since the law was enacted.

We believe that the technological advancements driving cloud computing are tremendously exciting, but also that they raise important questions about the privacy and security of individuals' information. Even as users begin to focus less on whether their data and communications are stored locally or, instead, are accessed remotely via the Internet, they continue to care deeply about how their information is protected and kept private. 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.

Given these widely-shared concerns about privacy, it is important that as we move from the era of the desktop PC to the era of Internet-based technologies such as cloud computing, we ensure that users are not forced to relinquish their privacy rights or control over their data to enjoy the benefits and efficiencies that Internet-based technologies make possible.

II. MICROSOFT'S SUPPORT FOR ECPA REFORM: RESTORING THE BALANCE CONGRESS STRUCK IN 1986

Congressional action is needed to update and preserve the privacy protections established in the Constitution and reinforced by federal statutes passed in the 1980s. Technological change increasingly calls into question the efficacy of the provisions enacted in the Electronic Communications Privacy Act. New legislation is needed both to modernize the law and to preserve the historical balance established between the rights of the individual and the needs of the state.

It is not surprising that issues relating to privacy have been at the forefront of public discussion about the new computing technologies that facilitate the digitization and online storage of unprecedented amounts of information. After all, the protection of privacy is an important American value. It is enshrined in the Fourth Amendment to the Constitution which, over the years, has guaranteed that we can send a letter or make a call and be secure in the knowledge that our communications will be kept private.

However, as a result of a series of court decisions, there is uncertainty about whether the Fourth Amendment applies to information that is transferred to a third party for storage or use. On the one hand, the Supreme Court has held that the Fourth Amendment is not triggered when the government inspects documents that an individual hands over to a third party for storage or

processing.[1] On the other, the Supreme Court also has held that the Fourth Amendment can protect the contents of communications, even when those communications traverse systems that are owned and operated by third parties, because users have a reasonable expectation that their communications will remain private.[2] The constitutional ambiguity for cloud computing is created by the fact that cloud technologies appear to implicate both lines of cases.

To address such uncertainties, Congress previously has stepped in and reinforced our privacy rights, including in 1986 when 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. ECPA grants certain protections to user data when it is stored online, and it establishes rules that law enforcement must follow before they can access that data. Depending on the type of customer information involved and the type of service being provided, the authorization law enforcement must obtain in order to require disclosure by service providers will range from a search warrant based upon probable cause (which requires the prior authorization of an independent magistrate) to a subpoena (which does not).

While this law has served us well for many years, continual advances in technology—most particularly the advent of low cost Internet-based computing and storage services—have called into question whether ECPA is adequate to meet our needs as a society today and into the future. For example, under ECPA, emails stored for less than 180 days receive greater privacy protections than emails stored for a longer period. And while information stored on a hard drive

[1] *See United States v. Miller*, 425 U.S. 435 (1976) (holding that the Fourth Amendment does not apply to an individual's personal records that are held by a bank).

[2] *See Katz v. United States*, 389 U.S. 347 (1967) (holding that the contents of telephone communications are protected by the Fourth Amendment).

would be fully protected by the Fourth Amendment, under ECPA a single email might be subject to multiple legal standards, depending upon whether it is stored and waiting to be read or whether it has been opened. While treating emails differently in these circumstances might have made sense in 1986, it is no longer justified in light of unprecedented digitization and indefinite storage of personal information online.

Another example involves the addition of online services to traditional desktop software – such as Microsoft Office. In Office 2010, when a user creates a Word document or an Excel spreadsheet, she may choose to save it locally or in the "cloud" via Office Web Apps. Increasingly, users think less and less about these distinctions – they simply expect that they can access their documents when they need to – at any time and on any device. It would come as a surprise to these users that the level of privacy afforded to those documents differs depending on where the document happens to be stored. Their reasonable expectation of privacy does not hinge on these distinctions.

To restore the balance struck in 1986, we urge Congress to revisit ECPA in light of these technological advancements. Microsoft supports changes that will ensure that users do not 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 (copy at the end of this statement) will enable citizens to trust that their data will be subject to reasonable privacy protections—no different from 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. The DDP Coalition principles will also provide greater clarity for providers who must comply with ECPA.

The example of stored email can help illustrate the effect of these principles. Rather than apply a range of legal standards to emails, depending on how old they are and whether they have been opened, the DDP Coalition principles would establish a uniform rule for all emails stored online: law enforcement must secure a warrant based upon a showing of probable cause. This uniform application of the warrant standard for online emails has two advantages. First, because individuals' data at home is typically accessible to law enforcement only through a search warrant, the application of a warrant standard for emails stored online accomplishes the goal of making online and locally-stored data subject to equal privacy protections. Second, because the warrant standard would be simple and applicable across the board, it provides clarity both for cloud service providers that must comply with the warrant and for users who store their data with cloud computing services.

In advocating for these changes, Microsoft is in no way seeking to minimize the legitimate needs of law enforcement investigators in obtaining access to data in the cloud. Every year, we dedicate significant resources to working with and training law enforcement officers, agents, and prosecutors at the federal, state, and local government levels. We see and understand how important electronic information is for law enforcement, and emphasize that it is our goal to ensure reasonable privacy protections for online data that do not interfere with law enforcement's legitimate needs. While we believe that the DDP Coalition principles accomplish this goal, we view them as a beginning, not the end, of the discussion. We look forward to engaging with the Committee, other Members of Congress and all stakeholders in the effort to restore the balance among the rights of individuals, the obligations of service providers, and the needs of law enforcement that was the underpinning of ECPA in 1986.

III. ECPA Reform in the Broader Context

ECPA reform is not the only area in which legislative action is warranted. Legislation is also needed to address other emerging issues relating to privacy and security as parts of a cohesive whole, and we need to consider them not only with respect to data in the United States but with respect to information that crosses national borders.

As Congress considers reforming ECPA, it is important to recognize that the new computing technologies that are driving the need for ECPA reform also implicate other policy issues. Accordingly, it is important to situate ECPA reform in the context of a broader policy agenda that should be advanced to ensure that the full benefits of cloud computing are realized. Such an agenda would encompass not only user privacy interests in relation to parties other than the government (such as the cloud provider itself and private third parties), but also other interests that are inextricably linked with privacy, including security, transparency, and national sovereignty.

1. ***Security***. Although the cloud is being built with powerful and unprecedented security safeguards, the aggregation of data in cloud datacenters presents new and rich targets for hackers and thieves. All stakeholders must work together to protect the security of the cloud. At the same time, Congress should ensure that the penalties for launching an attack on cloud computing infrastructure are sufficiently severe to help deter would-be criminals.

2. ***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 so that cloud computing users can make informed decisions about the services that best fit their needs.

3. ***National Sovereignty***. In recent years, there has emerged a global thicket of competing and sometimes conflicting laws impacting 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. This situation needs to be remedied.

Microsoft believes that these issues are interrelated and thus are best addressed in concert. That is why we have advocated for consideration of legislation that would:

- require transparency around cloud service providers' security and privacy practices, including by requiring 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;

- ensure greater rigor in the federal government's procurement of cloud services by requiring federal agencies to evaluate and select providers based in part on an assessment of their information security programs;

- 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; and

- encourage the federal government to engage in international efforts to promote consistency in national laws governing privacy, security and government access to cloud data.

With the benefit of a modernized regulatory framework, including an updated ECPA and these complementary reforms, industry will have the solid grounding to deliver on the promise of cloud computing for both individuals and organizations.

IV. Conclusion

One of the principal benefits of the personal computing revolution has been that it truly has made computing more personal in nature. It has empowered individuals to use technology in the way they choose. It has allowed them to store their information where they choose. And, critically, it has given individuals the freedom to share information when they choose and with whom they choose. With this freedom, users embraced the PC and moved their personal information—documents, photographs, and communications—from their desk drawer to their desktop PC.

Now, thanks to a new revolution in computing technology, users are able to collect, digitize, and store unprecedented amounts of personal information online. Given these trends, updating America's privacy laws as they apply to the online environment is a timely and crucial objective. Microsoft believes that ECPA can be reformed in such a way that consumers will feel

confident in the privacy of their data stored in the cloud without compromising the legitimate interests of law enforcement in obtaining the information necessary to carry out its responsibilities. By responsibly reforming ECPA, we can restore the balance between the rights of individuals, the obligations of service providers, and the needs of law enforcement that motivated Congress to pass ECPA in 1986.

We also believe that ECPA reform should be one aspect – albeit an important one – of a broader policy agenda that more comprehensively addresses new issues relating to privacy and security of data in the cloud computing environment. For this reason, we support consideration of legislation that would improve transparency around security and privacy practices to ensure that users can make informed decisions on the use of cloud computing services.

Thank you for providing Microsoft the opportunity to testify today. We appreciate the Committee's leadership on these important issues, and we look forward to working with you to promote security and protect privacy in the digital age.

DIGITAL DUE PROCESS COALITION PRINCIPLES

Overarching goal and guiding principle: To simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public.

These principles would not change, and are subject to, the current definitions, exceptions, immunities and permissions in ECPA.

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

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

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

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

Source: http://www.digitalddueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163